kaspersky

Kaspersky Anti Targeted Attack Platform

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 6.0.2.11

Уважаемый пользователь!

Спасибо, что доверяете нам. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Внимание! Права на этот документ являются собственностью АО "Лаборатория Касперского" (далее также "Лаборатория Касперского") и защищены законодательством Российской Федерации об авторском праве и международными договорами. За незаконное копирование и распространение документа и его отдельных частей нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с применимым законодательством.

Копирование в любой форме, распространение, в том числе в переводе, любых материалов возможны только с письменного разрешения "Лаборатории Касперского".

Документ и связанные с ним графические изображения могут быть использованы только в информационных, некоммерческих или личных целях.

Документ может быть изменен без предварительного уведомления.

За содержание, качество, актуальность и достоверность используемых в документе материалов, права на которые принадлежат другим правообладателям, а также за возможный ущерб, связанный с использованием этих материалов, "Лаборатория Касперского" ответственности не несет.

В этом документе используются зарегистрированные товарные знаки и знаки обслуживания, которые являются собственностью соответствующих правообладателей.

Дата редакции документа: 26.03.2024

© 2024 АО "Лаборатория Касперского"

https://www.kaspersky.ru
https://support.kaspersky.ru

О "Лаборатории Касперского" https://www.kaspersky.ru/about/company

kaspersky

Содержание

Об этом документе 22
Источники информации о приложении 23
О приложении 24
О Kaspersky Threat Intelligence Portal 26
Требования 27
Аппаратные и программные требования 27
Совместимость версий Kaspersky Endpoint Agent для Windows с версиями Kaspersky Anti Targeted Attack Platform 28
Совместимость версий Kaspersky Endpoint Agent для Windows с приложениями EPP 30
Совместимость версий Kaspersky Endpoint Security для Windows с версиями Kaspersky Anti Targeted Attack Platform 33
Совместимость версий Kaspersky Endpoint Security для Linux с версиями Kaspersky Anti Targeted Attack Platform 34
Совместимость Kaspersky Endpoint Security для Mac с версиями Kaspersky Anti Targeted Attack Platform 35
Совместимость версий KUMA с версиями Kaspersky Anti Targeted Attack Platform 36
Совместимость версий XDR с версиями Kaspersky Anti Targeted Attack Platform 36
Совместимость версий KPSN с версиями Kaspersky Anti Targeted Attack Platform 37
Совместимость Kaspersky Anti Targeted Attack Platform с VK Cloud 37
Указания по эксплуатации и требования к среде 38
Предоставление данных 39
Служебные данные приложения 40
Данные компонентов Central Node и Sensor 45
Данные трафика компонента Sensor 45
Данные в обнаружениях 46
Данные в событиях 49
Данные в отчетах 50
Данные об объектах в Хранилище и на карантине 51
Данные компонента Sandbox 52
Данные, пересылаемые между компонентами приложения 54
Данные в файлах трассировки приложения 60
Данные Kaspersky Endpoint Agent для Windows 60
Данные, получаемые от компонента Central Node 60
Данные в обнаружениях и событиях 62
Данные в отчетах о выполнении задач 63
Данные в журнале установки 64
Данные о файлах, запрещенных к запуску 64
Данные, связанные с выполнением задач 64
Данные Kaspersky Endpoint Security для Windows 65

Данные Kaspersky Endpoint Security для Linux 65
Данные Kaspersky Endpoint Security для Mac 65
Архитектура приложения 66
Компонент Sensor 66
Компонент Central Node 67
Компонент Sandbox 68
Компонент Endpoint Agent 68
Принцип работы приложения 69
Распределенное решение и мультитенантность 75
Сценарий перехода в режим распределенного решения и мультитенантности 77
Изменения в параметрах приложения при переходе в режим распределенного решения и мультитенантности 78
Назначение серверу роли PCN 80
Назначение серверу роли SCN 81
Обработка запросов на подключение SCN к PCN 82
Просмотр информации о тенантах, серверах PCN и SCN 83
Добавление тенанта на сервере PCN 83
Удаление тенанта на сервере PCN 84
Изменение названия тенанта на сервере PCN 84
Отключение SCN от PCN 85
Изменения в параметрах приложения при отключении SCN от PCN 86
Вывод сервера SCN из эксплуатации 87
Руководство по масштабированию 88
Типовые схемы развертывания и установки компонентов приложения 88
Схема развертывания на два сервера 91
Схема развертывания на три сервера 91
Схема развертывания на четыре и более сервера 92
Схема развертывания функциональности KEDR с компонентом Sandbox 92
Схема развертывания функциональности KEDR без компонента Sandbox 93
Калькулятор масштабирования 94
Расчеты для компонента Sensor 95
Расчеты для компонента Central Node 97
Расчеты для компонента Sandbox 103
Расчеты для компонента Central Node, развернутого на платформе виртуализации KVM 106
Оптимизация настроек сетевых интерфейсов для компонента Sensor 108
Установка и первоначальная настройка приложения 110
Подготовка к установке компонентов приложения 110
Подготовка IT-инфраструктуры к установке компонентов приложения 111
Подготовка IT-инфраструктуры к интеграции с почтовым сервером для приема сообщений по протоколу POP3 113

Подготовка IT-инфраструктуры к интеграции с почтовым сервером для отправки сообщений по протоколу SMTP 113
Подготовка виртуальной машины к установке компонента Sandbox 114
Подготовка установочного образа диска с компонентами Central Node, Sensor и Sandbox 114
Порядок установки и настройки компонентов приложения 116
Установка компонента Sandbox 119
Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности 120
Шаг 2. Выбор диска для установки компонента Sandbox 121
Шаг 3. Назначение имени хоста 121
Шаг 4. Выбор управляющего сетевого интерфейса в списке 121
Шаг 5. Назначение адреса и маски сети управляющего интерфейса 122
Шаг 6. Добавление адресов DNS-серверов 122
Шаг 7. Настройка статического сетевого маршрута 122
Шаг 8. Настройка минимальной длины пароля администратора Sandbox 123
Шаг 9. Создание учетной записи администратора Sandbox 123
Развертывание компонентов Central Node и Sensor в виде кластера 124
Развертывание сервера хранения данных 124
Шаг 1. Выбор роли сервера 125
Шаг 2. Выбор режима развертывания 125
Шаг 3. Выбор диска для установки компонента 126
Шаг 4. Просмотр Лицензионного соглашения и Политики конфиденциальности 126
Шаг 5. Выбор маски сети для адресации серверов кластера 126
Шаг 6. Выбор маски сети для адресации компонентов приложения 127
Шаг 7. Выбор кластерного сетевого интерфейса 127
Шаг 8. Выбор внешнего сетевого интерфейса 127
Шаг 9. Выбор способа получения IP-адресов для сетевых интерфейсов 128
Шаг 10. Создание учетной записи администратора и аутентификация сервера в кластере 128
Шаг 11. Добавление адресов DNS-серверов 130
Шаг 12. Выбор дисков для Ceph-хранилища 130
Развертывание обрабатывающего сервера 131
Шаг 1. Выбор роли сервера 131
Шаг 2. Выбор режима развертывания 132
Шаг 3. Выбор диска для установки компонента 132
Шаг 4. Просмотр Лицензионного соглашения и Политики конфиденциальности 132
Шаг 5. Выбор маски сети для адресации серверов кластера 133
Шаг 6. Выбор маски сети для адресации компонентов приложения 133
Шаг 7. Выбор кластерного сетевого интерфейса 134
Шаг 8. Выбор внешнего сетевого интерфейса 134
Шаг 9. Выбор способа получения IP-адресов для сетевых интерфейсов 134
Шаг 10. Аутентификация сервера в кластере 135
Шаг 11. Настройка получения зеркалированного трафика со SPAN-портов 135

Шаг 12. Добавление адресов DNS-серверов 135
Установка компонентов Central Node и Sensor на сервере 136
Шаг 1. Выбор роли сервера 137
Шаг 2. Просмотр Лицензионного соглашения и Политики конфиденциальности 138
Шаг 3. Выбор диска для установки компонента 138
Шаг 4. Выделение диска для базы данных компонента Targeted Attack Analyzer 138
Шаг 5. Выбор маски сети для адресации серверов кластера 139
Шаг 6. Выбор внешнего сетевого интерфейса 139
Шаг 7. Выбор способа получения IP-адресов для сетевых интерфейсов 140
Шаг 8. Создание учетной записи администратора 140
Шаг 9. Добавление адресов DNS-серверов 140
Шаг 10. Настройка получения зеркалированного трафика со SPAN-портов 141
Шаг 11. Настройка синхронизации времени с NTP-сервером 141
Установка компонента Sensor на отдельном сервере 142
Шаг 1. Выбор роли сервера 142
Шаг 2. Просмотр Лицензионного соглашения и Политики конфиденциальности 143
Шаг 3. Выбор диска для установки компонента 143
Шаг 4. Выбор внешнего сетевого интерфейса 143
Шаг 5. Подключение к серверу с компонентом Central Node 144
Шаг 6. Создание учетной записи администратора 144
Настройка Kaspersky Anti Targeted Attack Platform на базе операционной системы Astra Linux 144
Установка пакета обновления приложения до версии 6.0.2 146
Подключение и настройка внешнего хранилища для компонента Sensor 147
Процедура приемки 150
Безопасное состояние 150
Проверка целостности файлов Kaspersky Anti Targeted Attack Platform 151
Проверка безопасности и работоспособности Kaspersky Anti Targeted Attack Platform 153
О журналах Kaspersky Anti Targeted Attack Platform 153
Просмотр журнала работоспособности сервера с компонентом Central Node 154
Просмотр журнала работоспособности сервера с компонентом Sandbox 154
Просмотр журнала аудита безопасности сервера с компонентом Central Node 154
Просмотр журнала аудита безопасности сервера с компонентом Sandbox 155
Лицензирование приложения 156
О Лицензионном соглашении 156
О лицензии 157
О лицензионном сертификате 157
О ключе 158
О файле ключа 158
Просмотр информации о лицензии и добавленных ключах в веб-интерфейсе Central Node 158
Просмотр текста Лицензионного соглашения в веб-интерфейсе Central Node 159

Просмотр текста Политики конфиденциальности в веб-интерфейсе Central Node 159
Просмотр информации о стороннем коде, используемом в приложении 160
Просмотр текста Лицензионного соглашения в веб-интерфейсе Sandbox 160
Просмотр текста Лицензионного соглашения компонента Endpoint Agent 160
Добавление ключа 161
Замена ключа 161
Удаление ключа 161
Режимы работы приложения в соответствии с лицензией 162
Настройка интеграции Kaspersky Anti Targeted Attack Platform с компонентом Endpoint Agent 163
Настройка доверенного соединения Kaspersky Anti Targeted Attack Platform с приложением Kaspersky Endpoint Agent 164
Настройка соединения с сервером Central Node без проверки TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform 166
Настройка соединения с сервером Central Node с проверкой TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform 166
Настройка соединения с сервером Sensor без проверки TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform 167
Настройка соединения с сервером Sensor с проверкой TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform 168
Скачивание TLS-сертификата сервера Central Node на компьютер 169
Генерация TLS-сертификата сервера Central Node в веб-интерфейсе Kaspersky Anti Targeted Attack Platform 169
Загрузка самостоятельно подготовленного TLS-сертификата сервера Central Node через веб-интерфейс Kaspersky Anti Targeted Attack Platform 170
Загрузка TLS-сертификата сервера Central Node или Sensor в Kaspersky Endpoint Agent 171
Включение проверки TLS-сертификата Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform 172
Генерация TLS-сертификата Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform и скачивание крипто-контейнера 173
Загрузка самостоятельно подготовленного TLS-сертификата Kaspersky Endpoint Agent через веб-интерфейс Kaspersky Anti Targeted Attack Platform 173
Просмотр таблицы TLS-сертификатов Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform 174
Фильтрация и поиск TLS-сертификатов Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform 175
Удаление TLS-сертификатов Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform 176
Настройка проверки TLS-сертификата Kaspersky Endpoint Agent сервером Central Node и загрузка крипто-контейнера в Kaspersky Endpoint Agent 176
Настройка перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor 177
Включение и отключение перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor 178
Авторизация компонента Sensor на сервере Central Node 178
Генерация TLS-сертификата сервера Sensor в меню администратора сервера Sensor 179

Загрузка самостоятельно подготовленного TLS-сертификата сервера Sensor через меню администратора сервера Sensor 180
Скачивание TLS-сертификата сервера Sensor на компьютер 181
Настройка интеграции и доверенного соединения с Kaspersky Anti Targeted Attack Platform на стороне Kaspersky Endpoint Agent 181
Разделение доступа к функциям приложения по пользовательским ролям 184
Начало работы с приложением 186
Начало работы в веб-интерфейсе приложения под учетной записью локального администратора 186
Начало работы в веб-интерфейсе для управления масштабированием 187
Начало работы в меню администратора приложения 188
Начало работы с приложением в режиме Technical Support Mode 189
Управление учетными записями администраторов и пользователей приложения 191
Создание учетной записи администратора веб-интерфейса приложения 194
Создание учетной записи пользователя веб-интерфейса приложения 196
Настройка отображения таблицы учетных записей пользователей 197
Просмотр таблицы учетных записей пользователей 198
Фильтрация учетных записей 199
Сброс фильтра учетных записей 199
Изменение прав доступа учетной записи пользователя веб-интерфейса приложения 200
Включение и отключение учетной записи администратора или пользователя веб-интерфейса приложения 200
Изменение пароля учетной записи администратора или пользователя приложения 201
Изменение пароля своей учетной записи 202
Аутентификация с помощью доменных учетных записей 203
Создание keytab-файла 203
Настройка интеграции с Active Directory 206
Отключение интеграции с Active Directory 207
Участие в Kaspersky Security Network и использование Kaspersky Private Security Network 209
Просмотр Положения о KSN и настройка участия в KSN 210
Включение использования KPSN 210
Настройка подключения к локальной репутационной базе KPSN 211
Настройка сохранения информации в локальную репутационную базу KPSN 211
Отказ от участия в KSN и использования KPSN 212
Работа с компонентом Sandbox через веб-интерфейс 213
Обновление баз компонента Sandbox 214
Запуск обновления баз вручную 215
Выбор источника обновления баз 215
Включение и отключение использования прокси-сервера для обновления баз 216
Настройка параметров соединения с прокси-сервером для обновления баз 216
Настройка соединения компонентов Sandbox и Central Node 216
Обработка запросов на подключение от серверов Central Node в веб-интерфейсе Sandbox 217

Настройка сетевых интерфейсов компонента Sandbox 218
Настройка параметров DNS 218
Настройка параметров управляющего сетевого интерфейса 218
Настройка параметров сетевого интерфейса для доступа обрабатываемых объектов в интернет 219
Добавление, изменение и удаление статических сетевых маршрутов 220
Установка даты и времени системы Sandbox 221
Установка и настройка образов операционных систем и приложений для работы компонента Sandbox 221
Работа с образами операционных систем и приложений в Хранилище Sandbox 223
Просмотр таблицы образов операционных систем и приложений в Хранилище Sandbox 223
Загрузка образов операционных систем и приложений в Хранилище 224
Активация образов операционных систем и приложений в Хранилище Sandbox 224
Удаление образов операционных систем и приложений из Хранилища Sandbox 226
Работа с шаблонами виртуальных машин 226
Создание шаблона виртуальной машины 226
Просмотр таблицы шаблонов 227
Включение и выключение шаблона 228
Редактирование шаблона 229
Настройка операционной системы и программного обеспечения 229
Экспорт шаблона 230
Импорт шаблона 231
Удаление шаблона 231
Управление виртуальными машинами 232
Создание виртуальной машины 232
Создание виртуальной машины в разделе Виртуальные машины 233
Создание виртуальной машины в таблице шаблонов 234
Создание виртуальной машины в окне просмотра шаблона 235
Просмотр таблицы виртуальных машин с преднастроенными операционными системами 236
Просмотр таблицы виртуальных машин с пользовательскими операционными системами 236
Установка виртуальной машины 236
Удаление виртуальной машины 237
Загрузка отладочных символов 238
Установка максимального количества одновременно запускаемых виртуальных машин 239
Изменение количества лицензионных ключей для виртуальной машины с пользовательским образом операционной системы 239
Загрузка журнала системы Sandbox на жесткий диск 240
Экспорт параметров Sandbox 240
Импорт параметров Sandbox 241
Перезагрузка сервера Sandbox 242
Выключение сервера Sandbox 242
Изменение пароля учетной записи администратора Sandbox 242

Администратору: работа в веб-интерфейсе приложения 243
Интерфейс Kaspersky Anti Targeted Attack Platform 243
Мониторинг работы приложения 244
О виджетах и схемах расположения виджетов 245
Выбор тенанта и сервера для работы в разделе Мониторинг 246
Добавление виджета на текущую схему расположения виджетов 246
Перемещение виджета на текущей схеме расположения виджетов 246
Удаление виджета с текущей схемы расположения виджетов 247
Сохранение схемы расположения виджетов в PDF 247
Настройка периода отображения данных на виджетах 247
Мониторинг приема и обработки входящих данных 248
Мониторинг очередей обработки данных модулями и компонентами приложения 250
Мониторинг обработки данных компонентом Sandbox 251
Просмотр состояния работоспособности модулей и компонентов приложения 251
Управление серверами Central Node, PCN или SCN с помощью веб-интерфейса приложения 253
Настройка даты и времени сервера 254
Генерация или загрузка TLS-сертификата сервера 254
Скачивание TLS-сертификата сервера на компьютер 256
Назначение DNS-имени сервера 256
Настройка параметров DNS 257
Настройка параметров сетевого интерфейса 257
Настройка сетевого маршрута для использования по умолчанию 258
Настройка параметров соединения с прокси-сервером 258
Настройка параметров соединения с почтовым сервером 258
Выбор операционных систем для проверки объектов в Sandbox 259
Управление компонентом Sensor 260
Просмотр таблицы серверов с компонентом Sensor 261
Обработка запроса на подключение от компонента Sensor 262
Настройка максимального размера проверяемого файла 262
Настройка получения зеркалированного трафика со SPAN-портов 263
Выбор сетевых протоколов для получения зеркалированного трафика со SPAN-портов 263
Настройка интеграции с почтовым сервером по протоколу SMTP 265
Настройка TLS-шифрования соединений с почтовым сервером по протоколу SMTP 266
Настройка интеграции с прокси-сервером по протоколу ICAP 267
Включение и отключение интеграции с прокси-сервером по протоколу ICAP 267
Включение и отключение проверки ICAP-трафика в режиме реального времени 269
Настройка параметров проверки ICAP-трафика в режиме реального времени 271
Настройка отображения страниц уведомлений 272
Настройка записи сырого сетевого трафика 273
Включение и настройка параметров записи сырого сетевого трафика на сервере с установленными компонентами Sensor и Central Node 273

Включение и настройка параметров записи сырого сетевого трафика на отдельном сервере с компонентом Sensor 274
Настройка интеграции с почтовым сервером по протоколу POP3 275
Управление кластером 277
Просмотр таблицы серверов кластера 277
Добавление сервера в кластер 278
Увеличение дискового пространства сервера хранения 278
Вывод серверов из эксплуатации 278
Удаление сервера из кластера 279
Включение и выключение кластера 279
Уведомления о максимальной загрузке центрального процессора и оперативной памяти серверов Central Node и Sensor 280
Настройка максимального допустимого значения загрузки центрального процессора и оперативной памяти серверов Central Node и Sensor 281
Настройка соединения с протоколом SNMP 282
Описание объектов MIB Kaspersky Anti Targeted Attack Platform 283
Работа с информацией о хостах с компонентом Endpoint Agent 284
Выбор тенанта для работы в разделе Endpoint Agents 286
Просмотр таблицы хостов с компонентом Endpoint Agent на отдельном сервере Central Node 286
Просмотр информации о хосте 287
Фильтрация и поиск хостов с компонентом Endpoint Agent по имени хоста 287
Фильтрация и поиск хостов с компонентом Endpoint Agent, изолированных от сети 288
Фильтрация и поиск хостов с компонентом Endpoint Agent по именам серверов PCN и SCN 289
Фильтрация и поиск хостов с компонентом Endpoint Agent по IP-адресу компьютера 289
Фильтрация и поиск хостов с компонентом Endpoint Agent по версии операционной системы на компьютере 290
Фильтрация и поиск хостов с компонентом Endpoint Agent по версии компонента 290
Фильтрация и поиск хостов с компонентом Endpoint Agent по их активности 291
Быстрое создание фильтра хостов с компонентом Endpoint Agent 292
Сброс фильтра хостов с компонентом Endpoint Agent 292
Настройка показателей активности компонента Endpoint Agent 293
Удаление хостов с компонентом Endpoint Agent 293
Автоматическое удаление неактивных хостов 294
Поддерживаемые интерпретаторы и процессы 295
Настройка интеграции с компонентом Sandbox 297
Просмотр таблицы серверов с компонентом Sandbox 298
Создание запроса на подключение к серверу с компонентом Sandbox 299
Включение и отключение соединения с компонентом Sandbox 299
Удаление соединения с компонентом Sandbox 300
Настройка интеграции с внешними системами 300
Просмотр таблицы внешних систем 301
Обработка запроса от внешней системы 301

Удаление внешней системы из списка разрешенных к интеграции 302
Настройка приоритета обработки трафика от почтовых сенсоров 302
Настройка интеграции с Kaspersky Managed Detection and Response 302
Включение интеграции с MDR 303
Отключение интеграции с MDR 304
Замена конфигурационного файла MDR 304
Настройка интеграции с SIEM-системой 304
Включение и отключение записи информации в удаленный журнал 305
Настройка основных параметров интеграции с SIEM-системой 306
Загрузка TLS-сертификата 306
Включение и отключение TLS-шифрования соединения с SIEM-системой 307
Содержание и свойства syslog-сообщений об обнаружениях 307
Управление журналом активности 312
Включение и отключение записи информации в журнал активности 313
Скачивание файлов журнала активности 313
Содержание и свойства CEF-сообщений о действиях пользователей в веб-интерфейсе 314
Обновление баз приложения 317
Выбор источника обновления баз 318
Запуск обновления баз вручную 319
Создание списка паролей для архивов 319
Сотруднику службы безопасности: работа в веб-интерфейсе приложения 320
Интерфейс Kaspersky Anti Targeted Attack Platform 322
Выбор тенанта для работы в веб-интерфейсе приложения 323
Мониторинг работы приложения 323
О виджетах и схемах расположения виджетов 324
Добавление виджета на текущую схему расположения виджетов 325
Перемещение виджета на текущей схеме расположения виджетов 325
Удаление виджета с текущей схемы расположения виджетов 326
Сохранение схемы расположения виджетов в PDF 326
Настройка периода отображения данных на виджетах 326
Настройка масштаба отображения виджетов 327
Основные принципы работы с виджетами типа "Обнаружения" 328
Просмотр состояния работоспособности модулей и компонентов приложения 329
Просмотр таблицы обнаружений 331
Настройка отображения таблицы обнаружений 334
Фильтрация, сортировка и поиск обнаружений 334
Фильтрация обнаружений по наличию статуса VIP 335
Фильтрация и поиск обнаружений по времени 336
Фильтрация обнаружений по степени важности 336
Фильтрация и поиск обнаружений по категориям обнаруженных объектов 337

Фильтрация и поиск обнаружений по полученной информации 338
Фильтрация и поиск обнаружений по адресу источника 339
Фильтрация и поиск обнаружений по адресу назначения 339
Фильтрация и поиск обнаружений по имени сервера 340
Фильтрация и поиск обнаружений по названию технологии 340
Фильтрация и поиск обнаружений по состоянию их обработки пользователем 341
Сортировка обнаружений в таблице 342
Быстрое создание фильтра обнаружений 343
Сброс фильтра обнаружений 343
Рекомендации по обработке обнаружений 343
Рекомендации по обработке AM-обнаружений 344
Рекомендации по обработке TAA-обнаружений 345
Рекомендации по обработке SB-обнаружений 346
Рекомендации по обработке IOC-обнаружений 347
Рекомендации по обработке YARA-обнаружений 348
Рекомендации по обработке IDS-обнаружений 349
Просмотр обнаружений 350
Просмотр информации об обнаружении 351
Общая информация об обнаружении любого типа 351
Информация в блоке Информация об объекте 352
Информация в блоке Информация об обнаружении 353
Информация в блоке Результаты проверки 354
Информация в блоке Правило IDS 356
Информация в блоке Сетевое событие 356
Результаты проверки в Sandbox 357
Результаты IOC-проверки 359
Информация в блоке Хосты 361
Информация в блоке Журнал изменений 361
Отправка данных об обнаружении 361
Действия пользователей над обнаружениями 362
Назначение обнаружений определенному пользователю 363
Отметка о завершении обработки одного обнаружения 364
Отметка о завершении обработки обнаружений 365
Изменение статуса VIP обнаружений 365
Добавление комментария к обнаружению 366
Поиск угроз по базе событий 366
Поиск событий в режиме конструктора 367
Критерии для поиска событий 368
Операторы 371
Поиск событий в режиме исходного кода 371

Сортировка событий в таблице ... 373
Изменение условий поиска событий ... 374
Поиск событий по результатам их обработки в приложениях EPP ... 374
Загрузка IOC-файла и поиск событий по условиям, заданным в IOC-файле ... 376
Создание правила TAA (IOA) на основе условий поиска событий ... 377
Информация о событиях ... 378
Рекомендации по обработке событий ... 379
Выполнение рекомендации по изоляции хоста ... 381
Выполнение рекомендации по запрету запуска файла ... 382
Выполнение рекомендации по созданию задачи ... 383
Информация о событиях в дереве событий ... 384
Просмотр информации о родительском процессе в дереве событий ... 385
Просмотр информации о событиях, инициированных родительским процессом, в дереве событий ... 385
Просмотр информации о хосте в дереве событий ... 386
Просмотр таблицы событий ... 387
Настройка отображения таблицы событий ... 389
Просмотр информации о событии ... 390
Информация о событии Запущен процесс ... 390
Информация о событии Завершен процесс ... 394
Информация о событии Загружен модуль ... 397
Информация о событии Удаленное соединение ... 400
Информация о событии Правило запрета ... 402
Информация о событии Заблокирован документ ... 405
Информация о событии Изменен файл ... 407
Информация о событии Журнал событий ОС ... 412
Информация о событии Изменение в реестре ... 414
Информация о событии Прослушан порт ... 416
Информация о событии Загружен драйвер ... 418
Информация о событии Обнаружение ... 421
Информация о событии Результат обработки обнаружения ... 423
Информация о событии Интерпретированный запуск файла ... 426
Информация о событии AMSI-проверка ... 428
Информация о событии Интерактивный ввод команд в консоли ... 431
Работа с информацией о хостах с компонентом Endpoint Agent ... 433
Просмотр таблицы хостов с компонентом Endpoint Agent ... 435
Настройка отображения таблицы хостов с компонентом Endpoint Agent ... 437
Просмотр информации о хосте ... 437
Фильтрация и поиск хостов с компонентом Endpoint Agent по имени хоста ... 439
Фильтрация и поиск хостов с компонентом Endpoint Agent, изолированных от сети ... 440
Фильтрация и поиск хостов с компонентом Endpoint Agent по именам серверов PCN и SCN ... 440

Фильтрация и поиск хостов с компонентом Endpoint Agent по IP-адресу компьютера 441
Фильтрация и поиск хостов с компонентом Endpoint Agent по версии операционной системы на компьютере 442
Фильтрация и поиск хостов с компонентом Endpoint Agent по версии компонента 442
Фильтрация и поиск хостов с компонентом Endpoint Agent по их активности 443
Быстрое создание фильтра хостов с компонентом Endpoint Agent 444
Сброс фильтра хостов с компонентом Endpoint Agent 444
Удаление хостов с компонентом Endpoint Agent 444
Настройка показателей активности компонента Endpoint Agent 445
Поддерживаемые интерпретаторы и процессы 446
Сетевая изоляция хостов с компонентом Endpoint Agent 448
Создание правила сетевой изоляции 449
Добавление исключения из правила сетевой изоляции 450
Удаление правила сетевой изоляции 451
Ограничения, действующие при сетевой изоляции 451
Автоматическая отправка файлов с хостов с компонентом Endpoint Agent на проверку в Sandbox по правилам TAA (IOA) "Лаборатории Касперского" 451
Включение и отключение автоматической отправки файлов с хостов с компонентом Endpoint Agent на проверку компоненту Sandbox 453
Выбор операционных систем для проверки объектов в Sandbox 454
Просмотр таблицы серверов с компонентом Sandbox 454
Выбор операционных систем для проверки объектов в Sandbox 455
Работа с задачами 456
Просмотр таблицы задач 457
Просмотр информации о задаче 459
Создание задачи получения файла 460
Создание задачи сбора форензики 461
Создание задачи получения ключа реестра 463
Создание задачи получения метафайлов NTFS 464
Создание задачи получения дампа памяти процесса 465
Создание задачи получения образа диска 466
Конвертация файла из формата RAW в формат EWF 467
Создание задачи получения дампа оперативной памяти 469
Создание задачи завершения процесса 469
Создание задачи проверки хостов с помощью правил YARA 470
Создание задачи управления службами 473
Создание задачи выполнения приложения 476
Создание задачи удаления файла 477
Создание задачи помещения файла на карантин 478
Создание задачи восстановления файла из карантина 479
Создание копии задачи 480

Удаление задач ... 480
Фильтрация задач по времени создания ... 481
Фильтрация задач по типу ... 482
Фильтрация задач по имени ... 483
Фильтрация задач по имени и пути к файлу ... 483
Фильтрация задач по описанию ... 484
Фильтрация задач по имени сервера ... 485
Фильтрация задач по имени пользователя, создавшего задачу ... 485
Фильтрация задач по состоянию обработки ... 486
Сброс фильтра задач ... 486
Работа с политиками (правилами запрета) ... 486
Просмотр таблицы правил запрета ... 488
Настройка отображения таблицы правил запрета ... 489
Просмотр правила запрета ... 490
Создание правила запрета ... 491
Импорт правил запрета ... 492
Включение и отключение правила запрета ... 493
Включение и отключение предустановок ... 494
Удаление правил запрета ... 494
Фильтрация правил запрета по имени ... 495
Фильтрация правил запрета по типу ... 495
Фильтрация правил запрета по хешу файла ... 496
Фильтрация правил запрета по имени сервера ... 496
Сброс фильтра правил запрета ... 497
Работа с пользовательскими правилами ... 497
Об использовании индикаторов компрометации (IOC) и атаки (IOA) для поиска угроз ... 499
Работа с пользовательскими правилами ТАА (IOA) ... 500
Просмотр таблицы правил ТАА (IOA) ... 503
Создание правила ТАА (IOA) на основе условий поиска событий ... 504
Импорт правила ТАА (IOA) ... 505
Просмотр информации о правиле ТАА (IOA) ... 506
Поиск обнаружений и событий, в которых сработали правила ТАА (IOA) ... 507
Фильтрация и поиск правил ТАА (IOA) ... 508
Сброс фильтра правил ТАА (IOA) ... 510
Включение и отключение использования правил ТАА (IOA) ... 510
Изменение правила ТАА (IOA) ... 511
Удаление правил ТАА (IOA) ... 511
Работа с пользовательскими правилами IOC ... 512
Просмотр таблицы IOC-файлов ... 514
Просмотр информации об IOC-файле ... 515

Загрузка IOC-файла 516
Скачивание IOC-файла на компьютер 516
Включение и отключение автоматического использования IOC-файла при проверке хостов 517
Удаление IOC-файла 517
Поиск обнаружений по результатам IOC-проверки 518
Поиск событий по IOC-файлу 518
Фильтрация и поиск IOC-файлов 518
Сброс фильтра IOC-файлов 519
Настройка расписания IOC-проверки 519
Работа с пользовательскими правилами IDS 520
Импорт пользовательского правила IDS 521
Просмотр информации о пользовательском правиле IDS 522
Включение и отключение использования правила IDS при проверке событий 522
Настройка важности обнаружений, выполненных по пользовательскому правилу IDS 522
Замена пользовательского правила IDS 523
Экспорт файла пользовательского правила IDS на компьютер 523
Удаление пользовательского правила IDS 524
Работа с пользовательскими правилами YARA 524
Просмотр таблицы правил YARA 525
Настройка отображения таблицы правил YARA 526
Импорт правил YARA 526
Просмотр информации о правиле YARA 527
Фильтрация и поиск правил YARA 528
Сброс фильтра правил YARA 529
Включение и отключение использования правил YARA 530
Удаление правил YARA 531
Работа с объектами в Хранилище и на карантине 531
Просмотр таблицы объектов, помещенных в Хранилище 533
Просмотр информации об объекте, загруженном в Хранилище через веб-интерфейс 535
Просмотр информации об объекте, помещенном в Хранилище по задаче получения файла 536
Просмотр информации об объекте, помещенном в Хранилище по задаче получения данных 538
Скачивание объектов из Хранилища 539
Загрузка объектов в Хранилище 539
Отправка объектов из Хранилища на проверку 540
Удаление объектов из Хранилища 541
Фильтрация объектов в Хранилище по типу объекта 541
Фильтрация объектов в Хранилище по описанию объекта 542
Фильтрация объектов в Хранилище по результатам проверки 543
Фильтрация объектов в Хранилище по имени сервера Central Node, PCN или SCN 543
Фильтрация объектов в Хранилище по источнику объекта 544

Фильтрация объектов по времени помещения в Хранилище 544
Сброс фильтра объектов в Хранилище....545
Просмотр таблицы объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent 545
Просмотр информации об объекте на карантине 546
Восстановление объекта из карантина 547
Получение копии объекта на карантине на сервер Kaspersky Anti Targeted Attack Platform....548
Удаление информации об объекте, помещенном на карантин, из таблицы 549
Фильтрация информации об объектах, помещенных на карантин, по типу объекта....549
Фильтрация информации об объектах, помещенных на карантин, по описанию объекта....550
Фильтрация информации об объектах, помещенных на карантин, по имени хоста 550
Фильтрация информации об объектах, помещенных на карантин, по времени 551
Сброс фильтра информации об объектах на карантине 552
Работа с отчетами 552
Просмотр таблицы шаблонов и отчетов 553
Создание шаблона 554
Создание отчета по шаблону 556
Просмотр отчета 556
Скачивание отчета на локальный компьютер....557
Изменение шаблона....557
Фильтрация шаблонов по имени....558
Фильтрация шаблонов по имени пользователя, создавшего шаблон 559
Фильтрация шаблонов по времени создания 559
Сброс фильтра шаблонов....560
Удаление шаблона 560
Фильтрация отчетов по времени создания 560
Фильтрация отчетов по имени....561
Фильтрация отчетов по имени сервера с компонентом Central Node 561
Фильтрация отчетов по имени пользователя, создавшего отчет 562
Сброс фильтра отчетов 562
Удаление отчета 562
Работа с правилами присвоения обнаружениям статуса VIP 563
Просмотр таблицы правил присвоения статуса VIP 563
Создание правила присвоения статуса VIP 564
Удаление правила присвоения статуса VIP....564
Изменение правила присвоения статуса VIP....565
Импорт списка правил присвоения статуса VIP 565
Экспорт списка данных, исключенных из проверки....566
Фильтрация и поиск по типу правила присвоения статуса VIP 566
Фильтрация и поиск по значению правила присвоения статуса VIP 566
Фильтрация и поиск по описанию правила присвоения статуса VIP 567

Сброс фильтра правил присвоения статуса VIP 567
Работа со списком исключений из проверки 568
Просмотр таблицы данных, исключенных из проверки 568
Добавление правила исключения из проверки 569
Удаление правила исключения из проверки 570
Изменение правила, добавленного в исключения из проверки 571
Экспорт списка данных, исключенных из проверки 571
Фильтрация правил в списке исключений из проверки по критерию 572
Поиск правил в списке исключений из проверки по значению 572
Сброс фильтра правил в списке исключений из проверки 573
Работа с IDS-исключениями 573
Просмотр таблицы правил IDS, добавленных в исключения 574
Добавление правила IDS в исключения 574
Редактирование описания правила IDS, добавленного в исключения 575
Удаление правил IDS из исключений 576
Работа с TAA-исключениями 577
Просмотр таблицы правил TAA (IOA), добавленных в исключения 578
Добавление правила TAA (IOA) в исключения 579
Просмотр правила TAA (IOA), добавленного в исключения 582
Удаление правил TAA (IOA) из исключений 583
Работа с ICAP-исключениями 584
Просмотр таблицы ICAP-исключений 585
Добавление правила в ICAP-исключения 585
Удаление правил из ICAP-исключений 587
Изменение и выключение правила в списке ICAP-исключений 587
Фильтрация правил в списке ICAP-исключений по критерию 588
Фильтрация правил в списке ICAP-исключений по значению 588
Фильтрация правил в списке ICAP-исключений по состоянию 589
Сброс условий фильтрации правил в списке ICAP-исключений 589
Создание списка паролей для архивов 589
Просмотр параметров сервера 590
Просмотр таблицы серверов с компонентом Sandbox 591
Просмотр параметров набора операционных систем для проверки объектов в Sandbox 592
Просмотр таблицы серверов с компонентом Sensor 592
Работа с сырым сетевым трафиком 593
Выгрузка сырого сетевого трафика, захваченного с сетевых интерфейсов 594
Просмотр таблицы внешних систем 595
Отправка уведомлений 597
Просмотр таблицы правил для отправки уведомлений 597
Создание правила для отправки уведомлений об обнаружениях 598

Создание правила для отправки уведомлений о работе компонентов приложения 599
Включение и отключение правила для отправки уведомлений 600
Изменение правила для отправки уведомлений 600
Удаление правила для отправки уведомлений 600
Фильтрация и поиск правил отправки уведомлений по типу правила 601
Фильтрация и поиск правил отправки уведомлений по теме уведомлений 601
Фильтрация и поиск правил отправки уведомлений по адресу электронной почты 602
Фильтрация и поиск правил отправки уведомлений по их состоянию 602
Сброс фильтра правил отправки уведомлений 603
Управление приложением Kaspersky Endpoint Agent для Windows 604
Управление приложением Kaspersky Endpoint Security для Windows 606
Управление приложением Kaspersky Endpoint Security для Linux 607
Управление приложением Kaspersky Endpoint Security для Mac 608
Создание резервной копии и восстановление приложения 609
Создание резервной копии параметров сервера Central Node из меню администратора приложения612
Загрузка файла с резервной копией параметров сервера с сервера Central Node или PCN на жесткий диск компьютера 612
Загрузка файла с резервной копией параметров сервера с вашего компьютера на сервер Central Node 613
Восстановление параметров сервера из резервной копии через меню администратора приложения613
Создание резервной копии приложения в режиме Technical Support Mode 615
Восстановление приложения из резервной копии в режиме Technical Support Mode 616
Взаимодействие с внешними системами по API 618
Интеграция внешней системы с Kaspersky Anti Targeted Attack Platform 619
API для проверки объектов внешних систем 619
Запрос на проверку объектов 620
Запрос на получение результатов проверки 621
Запрос на удаление результатов проверки 623
Запрос на вывод ограничений приложения на проверку объектов 624
API для получения внешними системами информации об обнаружениях приложения 625
Запрос на вывод информации об обнаружениях 626
Состав передаваемых данных 628
Данные об обнаруженных объектах 630
Данные о найденных угрозах 630
Данные об окружении обнаруженных объектов 631
API для получения внешними системами информации о событиях приложения 633
Запрос на вывод информации о событиях 633
Язык запросов для фильтрации событий 637
Поля для фильтрации событий 638
API для управления действиями по реагированию на угрозы 645
Запрос на получение списка хостов с компонентом Endpoint Agent 645

Запрос на получение информации о сетевой изоляции и наличии правил запрета для хостов с компонентом Endpoint Agent 647
Управление сетевой изоляцией хостов 649
Запрос на включение сетевой изоляции 649
Запрос на отключение сетевой изоляции 651
Запрос на добавление исключения в правило сетевой изоляции 652
Управление правилами запрета 656
Запрос на создание правила запрета 658
Запрос на удаление правила запрета 660
Управление задачей запуска приложения 662
Запрос на получение информации о задаче 662
Запрос на создание задачи 664
Запрос на удаление задачи 666
Действия после сбоя или неустранимой ошибки в работе программы 668
Устранение уязвимостей и установка критических обновлений 669
Обращение в Службу технической поддержки 670
Способы получения технической поддержки 670
Техническая поддержка через Kaspersky CompanyAccount 670
Информация о стороннем коде 672
Уведомления о товарных знаках 673
Приложение. Значения параметров приложения в сертифицированной конфигурации 674

Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия "Kaspersky Anti Targeted Attack Platform" (далее также "Kaspersky Anti Targeted Attack Platform", "приложение").

Подготовительные процедуры изложены в разделах "Подготовка к установке компонентов приложения", "Установка приложения", "Подготовка приложения к работе" и "Процедура приемки" и содержат процедуры безопасной установки и первоначальной настройки приложения, которые необходимы для получения безопасной (сертифицированной) конфигурации. В разделе "Требования" приведены минимально необходимые системные требования для безопасной установки приложения.

Остальные разделы этого документа представляют собой руководство по эксплуатации. Руководство по эксплуатации содержит сведения о том, как осуществлять безопасное администрирование приложения, а также инструкции и указания по безопасному использованию приложения.

В документе также содержатся разделы с дополнительной информацией о приложении.

Документ адресован техническим специалистам, в обязанности которых входит установка, эксплуатация и администрирование Kaspersky Anti Targeted Attack Platform, а также поддержка организаций, использующих Kaspersky Anti Targeted Attack Platform.

Источники информации о приложении

Указанные источники информации о приложении созданы для удобства пользователя и не являются полноценным эквивалентом этого документа.

Страница Kaspersky Anti Targeted Attack Platform на веб-сайте "Лаборатории Касперского"

На странице (https://support.kaspersky.ru/kata/about_kata) Kaspersky Anti Targeted Attack Platform вы можете получить общую информацию о приложении, его возможностях и особенностях работы.

Страница Kaspersky Anti Targeted Attack Platform в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице (https://support.kaspersky.ru/kata/about_kata) Kaspersky Anti Targeted Attack Platform в Базе знаний вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании приложения.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Anti Targeted Attack Platform, но и к другим приложениям "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Обсуждение программ "Лаборатории Касперского" в сообществе пользователей

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями в нашем сообществе (https://community.kaspersky.com).

В сообществе вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

О приложении

Программное изделие Kaspersky Anti Targeted Attack Platform поставляется в двух исполнениях:

1. Network – система обнаружения вторжений уровня сети четвертого класса защиты (лицензия KATA).
2. XDR – система обнаружения вторжений многоуровневого типа для защиты от целевых атак (лицензии KATA и KEDR).

Объект оценки представляет собой программное средство, реализующее функции автоматизированного обнаружения в ИС угроз нового поколения, таких как *атаки «нулевого дня»* и *целевые атаки* (advanced persistent threat), направленных на преднамеренный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней. Обнаружение производится при помощи анализа сетевой активности в ИС и исследования поведения потенциально вредоносных объектов в контролируемой среде выполнения.

В приложении реализованы следующие функции безопасности:

1. Аудит безопасности:
   - возможность генерации записей аудита для событий, потенциально подвергаемых аудиту;
   - возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего (если возможно);
   - возможность предоставлять чтение информации из записей аудита;
   - ограничение доступа к чтению записей аудита по обнаруженным нарушениям безопасности (признакам проведения атак);
   - сортировка, поиск и фильтрация данных аудита об обнаруженных нарушениях безопасности.
2. Идентификация и аутентификация:
   - возможность идентификации пользователей;
   - возможность аутентификации пользователей.
3. Управление безопасностью:
   - возможность администрирования СОВ;
   - поддержка определенных ролей для СОВ и их ассоциации с конкретными администраторами СОВ и пользователями ИС;
   - возможность со стороны уполномоченных администраторов (ролей) управлять данными СОВ;
   - возможность со стороны уполномоченных администраторов (ролей) управлять режимом выполнения функций безопасности СОВ.
4. Защита ФБО:
   - возможность тестирования (самотестирования) функций безопасности СОВ;
   - возможность верификации целостности обновлений баз решающих правил и баз данных ПКВ, а также программного кода ОО.
5. Анализ собранных данных:
   - возможность анализа собранных данных СОВ о сетевом трафике в режиме, близком к реальному масштабу времени и по результатам анализа фиксировать информацию о дате и времени, результате анализа, идентификаторе источника данных, протоколе, используемом для проведения вторжения;

- возможность обнаружения вторжений на основе анализа служебной информации протоколов сетевого, транспортного и прикладного уровней базовой эталонной модели взаимосвязи открытых систем;
- возможность выполнения анализа собранных данных с целью обнаружения вторжений с использованием сигнатурного и эвристических методов.
- возможность выполнения анализа собранных данных с целью обнаружения вторжений с использованием эвристических методов, основанных на методах выявления аномалий сетевого трафика на заданном уровне эвристического анализа; а также путем оценки репутационных данных адресатов сетевых соединений и анализа данных, полученных путем выполнения объектов в контролируемой среде.
- возможность анализа собранных объектов сетевого трафика:
  - сканирование с целью выявления известных КВ сигнатурными и эвристическими методами;
  - анализ объекта на потенциально опасные действия путем запуска в контролируемой среде исполнения;
  - статический анализ исполняемого кода на признаки принадлежности к проведению атак, на основе настраиваемых правил, заданных администратором безопасности.

6. Сбор данных о событиях и активности в контролируемой информационной системе:
   - возможность сбора информации о сетевом трафике:
     - с сетевых шлюзов;
     - (только в исполнении XDR) с объектов локальной сети;
     - с почтовых сервисов.
   - (только в исполнении XDR) с АРМ в ИС при помощи датчиков.
7. Реагирование ОО:
   - возможность фиксации факта обнаружения вторжений или нарушений безопасности в журналах аудита;
   - уведомление администратора СОВ об обнаруженных вторжениях по отношению к контролируемым узлам ИС и нарушениях безопасности с помощью отображения соответствующего сообщения на консоли управления;
   - (только в исполнении XDR) возможность автоматизированного выполнения действий реагирования на узлах сети.
8. Управление обновлением базы решающих правил и базы данных признаков вредоносных компьютерных программ (вирусов) (БД ПКВ) ОО:
   - возможность автоматического обновления баз решающих правил и баз данных ПКВ;
   - возможность обновления баз решающих правил и баз данных ПКВ по команде администратора сервера.

В этом разделе

О Kaspersky Threat Intelligence Portal 26

О Kaspersky Threat Intelligence Portal

Для получения дополнительной информации о файлах, которые вы считаете подозрительными, вы можете перейти на веб-сайт приложения "Лаборатории Касперского" Kaspersky Threat Intelligence Portal, которая анализирует каждый файл на содержание в нем вредоносного кода и отображает информацию о репутации этого файла.

Доступ к приложению Kaspersky Threat Intelligence предоставляется на платной основе. Для авторизации на веб-сайте приложения на вашем компьютере в хранилище сертификатов должен быть установлен сертификат доступа к приложению. Кроме того, у вас должны быть имя пользователя и пароль доступа к приложению.
Подробнее о приложении Kaspersky Threat Intelligence Portal см. веб-сайт "Лаборатории Касперского".

kaspersky

Требования

Этот раздел содержит аппаратные и программные требования для установки и работы приложения, а также указания по эксплуатации и требования к среде.

В этом разделе

Аппаратные и программные требования.....27

Указания по эксплуатации и требования к среде 38

Аппаратные и программные требования

Аппаратные и программные требования к серверам для установки Kaspersky Anti Targeted Attack Platform

Для развертывания приложения на виртуальной платформе должен быть установлен гипервизор VMware ESXi™ версии 6.7.0 или 7.0.

> Для корректной работы приложения в виртуальной среде необходимо установить для гипервизора актуальный пакет обновления.

Аппаратные требования к компонентам Central Node, Sensor и Sandbox приведены в Руководстве по масштабированию (см. раздел "Руководство по масштабированию" на стр. 88).

Аппаратные требования к компьютерам для установки компонента Endpoint Agent

Компонент Endpoint Agent может быть представлен следующими приложениями:

- Kaspersky Endpoint Agent для Windows.
- Kaspersky Endpoint Security для Windows.
- Kaspersky Endpoint Security для Linux.
- Kaspersky Endpoint Security для Mac

Аппаратные требования к компьютерам для установки приложений см. в справке соответствующего приложения: Kaspersky Endpoint Agent для Windows, Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux, Kaspersky Endpoint Security для Mac.

Аппаратные и программные требования к компьютерам для работы в веб-интерфейсе Kaspersky Anti Targeted Attack Platform

Для настройки и работы с приложением через веб-интерфейс на компьютерах должен быть установлен один из следующих браузеров:

- Mozilla™ Firefox™ для Linux.
- Mozilla Firefox для Windows.
- Google™ Chrome™ для Windows.

- Google Chrome для Linux.
- Edge (Windows).
- Safari (Mac).

Минимально возможное разрешение экрана для работы в веб-интерфейсе: 1366x768 пикселей.

В этом разделе

Совместимость версий Kaspersky Endpoint Agent для Windows с версиями Kaspersky Anti Targeted Attack Platform 28

Совместимость версий Kaspersky Endpoint Agent для Windows с приложениями EPP 30

Совместимость версий Kaspersky Endpoint Security для Windows с версиями Kaspersky Anti Targeted Attack Platform 33

Совместимость версий Kaspersky Endpoint Security для Linux с версиями Kaspersky Anti Targeted Attack Platform 34

Совместимость Kaspersky Endpoint Security для Mac с версиями Kaspersky Anti Targeted Attack Platform....35

Совместимость версий KUMA с версиями Kaspersky Anti Targeted Attack Platform 36

Совместимость версий XDR с версиями Kaspersky Anti Targeted Attack Platform 36

Совместимость версий KPSN с версиями Kaspersky Anti Targeted Attack Platform....37

Совместимость Kaspersky Anti Targeted Attack Platform с VK Cloud 37

Совместимость версий Kaspersky Endpoint Agent для Windows с версиями Kaspersky Anti Targeted Attack Platform

Приложение Kaspersky Endpoint Agent использует предустановленные параметры, которые определяют его влияние на производительность локального компьютера в сценариях получения информации и взаимодействия с компонентом Central Node.

Если версия приложения Kaspersky Anti Targeted Attack Platform, установленного на серверах Central Node, несовместима с версией приложения Kaspersky Endpoint Agent, установленного на компьютерах локальной сети вашей организации, возможны ограничения в работе Kaspersky Anti Targeted Attack Platform.

Информация о совместимости версий Kaspersky Endpoint Agent с версиями Kaspersky Anti Targeted Attack Platform приведена в таблице ниже.

Таблица 1. Совместимость версий Kaspersky Endpoint Agent для Windows с версиями Kaspersky Anti Targeted Attack Platform

Версия Kaspersky Endpoint Agent	Тип Kaspersky Endpoint Agent	Совместимость с KATA 3.7	Совместимость с KATA 3.7.1	Совместимость с KATA 3.7.2	Совместимость с KATA 4.0	Совместимость с KATA 4.1	Совместимость с KATA 5.0	Совместимость с KATA 5.1	Совместимость с KATA 6.0
Endpoint Agent 3.7	Устанавливается отдельно или в составе KES версий 11.2 и 11.3	Нет	Нет	Нет	Нет	Нет	Нет	Нет	Нет
Endpoint Agent 3.8	Устанавливается отдельно	Да	Да	Есть ограничения	Есть ограничения	Есть ограничения	Есть ограничения	Нет	Нет
Endpoint Agent 3.9	Устанавливается отдельно или в составе приложений EPP	Да	Да	Есть ограничения	Есть ограничения	Есть ограничения	Есть ограничения	Нет	Нет
Endpoint Agent 3.10	Устанавливается отдельно или в составе приложений EPP	Нет	Есть ограничения	Да	Есть ограничения	Есть ограничения	Есть ограничения	Нет	Нет
Endpoint Agent 3.11	Устанавливается отдельно или в составе KES 11.7	Нет	Есть ограничения	Да	Есть ограничения	Есть ограничения	Есть ограничения	Нет	Нет
Endpoint Agent 3.12	Устанавливается отдельно	Нет	Нет	Нет	Да	Есть ограничения	Есть ограничения	Есть ограничения	Есть ограничения
Endpoint Agent 3.13	Устанавливается отдельно	Нет	Нет	Нет	Есть ограничения	Да	Есть ограничения	Есть ограничения	Есть ограничения
Endpoint Agent 3.14	Устанавливается отдельно	Нет	Нет	Нет	Есть ограничения	Есть ограничения	Да	Да	Да
Endpoint Agent 3.15	Устанавливается отдельно	Нет	Нет	Нет	Нет	Нет	Да	Да	Да
Endpoint Agent 3.16	Устанавливается отдельно	Нет	Нет	Нет	Нет	Нет	Нет	Нет	Да

Совместимость версий Kaspersky Endpoint Agent для Windows с приложениями EPP

Если в качестве компонента Endpoint Agent (см. раздел "Компонент Endpoint Agent" на стр. 68) вы хотите использовать приложение Kaspersky Endpoint Agent, вы можете установить только Kaspersky Endpoint Agent или настроить интеграцию Kaspersky Endpoint Agent с приложениями защиты рабочих станций (Endpoint Protection Platform, далее также "EPP") Kaspersky Endpoint Security для Windows, Kaspersky Security для Windows Server и Kaspersky Security для виртуальных сред Легкий агент. Если интеграция между приложениями настроена, Kaspersky Endpoint Agent будет также передавать на сервер Central Node данные об угрозах, обнаруженных приложениями EPP, и о результатах их обработки.

Описанные сценарии интеграции не работают при установке приложения Kaspersky Endpoint Agent на виртуальный рабочий стол в инфраструктуре Virtual Desktop Infrastructure.

Для интеграции Kaspersky Endpoint Agent с Kaspersky Endpoint Security для Windows и Kaspersky Security для Windows Server требуется установить Kaspersky Endpoint Agent в составе этих приложений.

Совместимость Kaspersky Endpoint Agent для Windows с версиями Kaspersky Security для Windows Server

Вы можете установить в составе Kaspersky Security для Windows Server следующие версии Kaspersky Endpoint Agent:

- Kaspersky Endpoint Agent 3.9 в составе Kaspersky Security 11 для Windows Server.
- Kaspersky Endpoint Agent 3.10 в составе Kaspersky Security 11.0.1 для Windows Server.

При установке Kaspersky Endpoint Agent в составе Kaspersky Security для Windows Server отдельно установленное ранее приложение Kaspersky Endpoint Agent той же или более ранних версий удаляется. Если версия Kaspersky Endpoint Agent в составе Kaspersky Security для Windows Server более ранняя, приложение не будет установлено. В этом случае вам требуется предварительно удалить отдельно установленное приложение Kaspersky Endpoint Agent.

При необходимости вы можете обновить приложение Kaspersky Endpoint Agent, уже установленное в составе Kaspersky Security для Windows Server. Интеграция между совместимыми версиями приложений сохранится как при обновлении Kaspersky Endpoint Agent, так и при обновлении Kaspersky Security для Windows Server.

Информация о совместимости версий приложений Kaspersky Endpoint Agent и Kaspersky Security для Windows Server приведена в таблице ниже.

Таблица 2. Совместимость версий Kaspersky Endpoint Agent и Kaspersky Security для Windows Server

Версия Kaspersky Security для Windows Server	Совместимость с Endpoint Agent 3.8, 3.9, 3.10	Совместимость с Endpoint Agent 3.11, 3.12	Совместимость с Endpoint Agent 3.13, 3.14, 3.15, 3.16
• KSWS 10.1.2	Да	Нет	Нет
• KSWS 11	Да	Да	Нет
• KSWS 11.0.1	Нет	Да	Есть ограничения

Подробнее об установке Kaspersky Security для Windows Server см. в справке Kaspersky Security для Windows Server.

Совместимость Kaspersky Endpoint Agent для Windows с версиями Kaspersky Endpoint Security для Windows

Вы можете установить в составе Kaspersky Endpoint Security для Windows следующие версии Kaspersky Endpoint Agent (Endpoint Sensors):

- Kaspersky Endpoint Agent 3.7 или Kaspersky Endpoint Agent (Endpoint Sensors) 3.6.1 в составе Kaspersky Endpoint Security 11.2, 11.3 для Windows.

  Приложение Kaspersky Endpoint Agent (Endpoint Sensors) 3.6.1 несовместимо с Kaspersky Anti Targeted Attack Platform 4.1 и выше.
  Приложение Kaspersky Endpoint Agent 3.7 несовместимо со всеми версиями Kaspersky Anti Targeted Attack Platform.

- Kaspersky Endpoint Agent 3.9 в составе Kaspersky Endpoint Security 11.4, 11.5.
- Kaspersky Endpoint Agent 3.10 в составе Kaspersky Endpoint Security 11.6.
- Kaspersky Endpoint Agent 3.11 в составе Kaspersky Endpoint Security 11.7, 11.8.

При установке Kaspersky Endpoint Agent версии 3.10 и выше в составе Kaspersky Endpoint Security для Windows отдельно установленное ранее приложение Kaspersky Endpoint Agent той же или более ранних версий удаляется. Если отдельно установленное приложение Kaspersky Endpoint Agent более поздних версий, приложение в составе Kaspersky Endpoint Security для Windows не будет установлено. В этом случае вам требуется предварительно удалить отдельно установленное приложение Kaspersky Endpoint Agent.

При необходимости вы можете обновить приложение Kaspersky Endpoint Agent, уже установленное в составе Kaspersky Endpoint Security для Windows. Интеграция между совместимыми версиями приложений сохранится как при обновлении приложения Kaspersky Endpoint Agent, так и при обновлении приложения Kaspersky Endpoint Security для Windows. Обновление с предыдущей версии Kaspersky Endpoint Agent до версии 3.14 доступно для Kaspersky Endpoint Agent версии 3.7 и выше.

Информация о совместимости версий Kaspersky Endpoint Agent и Kaspersky Endpoint Security для Windows приведена в таблице ниже.

Таблица 3. Совместимость версий Kaspersky Endpoint Agent и Kaspersky Endpoint Security для Windows

Версия Kaspersky Endpoint Security	Совместимость с Endpoint Agent 3.8, 3.9	Совместимость с Endpoint Agent 3.10, 3.12	Совместимость с Endpoint Agent 3.11	Совместимость с Endpoint Agent 3.13, 3.14, 3.15, 3.16
• KES 10 SP2 MR2	Нет	Нет	Нет	Нет
• KES 10 SP2 MR3/MR4	Да	Нет	Нет	Нет
• KES 11.0.0	Нет	Нет	Нет	Нет
• KES 11.0.1	Да	Нет	Нет	Нет
• KES 11.1 • KES 11.1.1	Да	Да	Нет	Нет
• KES 11.2 • KES 11.3	Да	Да	Да	Нет
• KES 11.4 • KES 11.5	Да	Да	Да	Нет
• KES 11.6 • KES 11.7 • KES 11.8	Да	Да	Да	Да
• KES 12.1 • KES 12.2 • KES 12.3	Нет	Нет	Нет	Нет

Подробнее об установке Kaspersky Endpoint Security см. в справке Kaspersky Endpoint Security для Windows.

Совместимость Kaspersky Endpoint Agent с версиями Kaspersky Security для виртуальных сред Легкий агент

Вы можете настроить интеграцию для отдельно установленных приложений Kaspersky Endpoint Agent и Kaspersky Security для виртуальных сред Легкий агент.

Информация о совместимости версий приложений Kaspersky Endpoint Agent и Kaspersky Security для виртуальных сред Легкий агент приведена в таблице ниже.

Таблица 4. Совместимость версий Kaspersky Endpoint Agent и Kaspersky Security для виртуальных сред Легкий агент

Версия Kaspersky Security для виртуальных сред Легкий агент	Совместимость с Endpoint Agent 3.8, 3.9, 3.10	Совместимость с Endpoint Agent 3.12	Совместимость с Endpoint Agent 3.11, 3.13, 3.14	Совместимость с Endpoint Agent 3.15	Совместимость с Endpoint Agent 3.16
• KSV 5.1 LA	Да	Да	Нет	Нет	Нет
• KSV 5.1.1 LA	Да	Нет	Нет	Нет	Нет
• KSV 5.2 LA	Нет	Да	Да	Да	Да

Версия Kaspersky Security для виртуальных сред Легкий агент	Совместимость с Endpoint Agent 3.8, 3.9, 3.10	Совместимость с Endpoint Agent 3.12	Совместимость с Endpoint Agent 3.11, 3.13, 3.14	Совместимость с Endpoint Agent 3.15	Совместимость с Endpoint Agent 3.16
• KSV 6.0 LA	Нет	Да	Да	Да	Нет

Kaspersky Endpoint Agent и Kaspersky Security для виртуальных сред Легкий агент, установленные на виртуальную машину, дают такую же нагрузку на сервер Central Node, как Kaspersky Endpoint Agent и Kaspersky Security для виртуальных сред Легкий агент, установленные на хост.

Подробнее о включении интеграции между Kaspersky Endpoint Agent и Kaspersky Security для виртуальных сред Легкий агент см. в справке Kaspersky Security для виртуальных сред Легкий агент.

Совместимость Kaspersky Endpoint Agent с версиями Kaspersky Industrial CyberSecurity for Nodes

Вы можете установить приложение Kaspersky Endpoint Agent на устройство с установленным приложением Kaspersky Industrial CyberSecurity for Nodes. Приложения интегрируются автоматически.

Таблица 5. Совместимость версий Kaspersky Endpoint Agent и Kaspersky Industrial CyberSecurity for Nodes

Версия Kaspersky Industrial CyberSecurity for Nodes	Совместимость с Endpoint Agent 3.11, 3.12	Совместимость с Endpoint Agent 3.13, 3.14, 3.15	Совместимость с Endpoint Agent 3.16
• KICS for Nodes 3.0	Да	Да	Да
• KICS for Nodes 3.1	Нет	Да	Да
• KICS for Nodes 3.2	Нет	Нет	Да

Для интеграции с Kaspersky Industrial CyberSecurity for Nodes в Kaspersky Endpoint Agent должен быть установлен соответствующий лицензионный ключ.

Для получения детальной информации вы можете обратиться к вашему аккаунт-менеджеру.

Совместимость версий Kaspersky Endpoint Security для Windows с версиями Kaspersky Anti Targeted Attack Platform

Вы можете использовать Kaspersky Endpoint Security в качестве компонента Endpoint Agent (см. раздел "Компонент Endpoint Agent" на стр. 68).

Информация о совместимости версий Kaspersky Endpoint Security с версиями Kaspersky Anti Targeted Attack Platform приведена в таблице ниже.

Таблица 6. Совместимость версий Kaspersky Endpoint Security для Windows с версиями Kaspersky Anti Targeted Attack Platform

Версия Kaspersky Endpoint Security	Совместимость с KATA 3.7	Совместимость с KATA 3.7.1	Совместимость с KATA 3.7.2	Совместимость с KATA 4.0	Совместимость с KATA 4.1	Совместимость с KATA 5.0	Совместимость с KATA 5.1	Совместимость с KATA 6.0
Kaspersky Endpoint Security 12.1	Нет	Нет	Нет	Нет	Да	Да	Да	Да
Kaspersky Endpoint Security 12.2	Нет	Нет	Нет	Нет	Да	Да	Да	Да
Kaspersky Endpoint Security 12.3	Нет	Нет	Нет	Нет	Да	Да	Да	Да

Для интеграции Kaspersky Endpoint Security 12.1 и выше с Kaspersky Anti Targeted Attack Platform не требуется устанавливать Kaspersky Endpoint Agent.

Совместимость версий Kaspersky Endpoint Security для Linux с версиями Kaspersky Anti Targeted Attack Platform

Вы можете использовать Kaspersky Endpoint Security в качестве компонента Endpoint Agent.

Информация о совместимости версий Kaspersky Endpoint Security с версиями Kaspersky Anti Targeted Attack Platform приведена в таблице ниже.

Таблица 7. Совместимость версий Kaspersky Endpoint Security для Linux с версиями Kaspersky Anti Targeted Attack Platform

Версия Kaspersky Endpoint Security	Совмести-мость с KATA 3.7	Совме-стимость с KATA 3.7.1	Совме-стимость с KATA 3.7.2	Совме-стимость с KATA 4.0	Совме-стимость с KATA 4.1	Совме-стимость с KATA 5.0	Совме-стимость с KATA 5.1	Совме-стимость с KATA 6.0
Kaspersky Endpoint Security 11.4	Нет	Нет	Нет	Нет	Нет	Нет	Да	Есть ограничения
Kaspersky Endpoint Security 12	Нет	Нет	Нет	Нет	Нет	Нет	Есть ограничения	Да

Для интеграции Kaspersky Endpoint Security 11.4 и 12 с Kaspersky Anti Targeted Attack Platform не требуется устанавливать Kaspersky Endpoint Agent.

Kaspersky Endpoint Security для Linux с версии 12 может использоваться в качестве компонента Легкий агент для Linux для приложения Kaspersky Security для виртуальных сред. Подробнее об интеграции см. в справке Kaspersky Security для виртуальных сред Легкий агент

При использовании приложения Kaspersky Endpoint Security для Linux в качестве компонента Легкий агент для Linux интеграция Kaspersky Endpoint Security для Linux и Kaspersky Anti Targeted Attack Platform сохраняется.

Совместимость Kaspersky Endpoint Security для Mac с версиями Kaspersky Anti Targeted Attack Platform

Вы можете использовать Kaspersky Endpoint Security для Mac в качестве компонента Endpoint Agent (см. раздел "Компонент Endpoint Agent" на стр. 68).

Информация о совместимости версий Kaspersky Endpoint Security для Mac с версиями Kaspersky Anti Targeted Attack Platform приведена в таблице ниже.

Таблица 8. Совместимость версий Kaspersky Endpoint Security для Mac с версиями Kaspersky Anti Targeted Attack Platform

Версия Kaspersky Endpoint Security	Совместимость с KATA 3.7	Совместимость с KATA 3.7.1	Совместимость с KATA 3.7.2	Совместимость с KATA 4.0	Совместимость с KATA 4.1	Совместимость с KATA 5.0	Совместимость с KATA 5.1	Совместимость с KATA 6.0
Kaspersky Endpoint Security 12	Нет	Нет	Нет	Нет	Нет	Нет	Нет	Да

Совместимость версий KUMA с версиями Kaspersky Anti Targeted Attack Platform

Вы можете использовать KUMA в качестве SIEM-системы.

Информация о совместимости версий KUMA с версиями Kaspersky Anti Targeted Attack Platform приведена в таблице ниже.

Таблица 9. Совместимость версий KUMA с версиями Kaspersky Anti Targeted Attack Platform

Версия KUMA	Совместимость с KATA 4.1	Совместимость с KATA 5.0	Совместимость с KATA 5.1	Совместимость с KATA 6.0
KUMA 2.0	Да	Да	Нет	Нет
KUMA 2.1	Нет	Да	Да	Нет
KUMA 3.0	Нет	Нет	Нет	Да

Совместимость версий XDR с версиями Kaspersky Anti Targeted Attack Platform

Вы можете использовать XDR в качестве SIEM-системы.

Информация о совместимости версий XDR с версиями Kaspersky Anti Targeted Attack Platform приведена в таблице ниже.

Таблица 10. Совместимость версий XDR с версиями Kaspersky Anti Targeted Attack Platform

Версия XDR	Совместимость с KATA 4.1	Совместимость с KATA 5.0	Совместимость с KATA 5.1	Совместимость с KATA 6.0
XDR 1.0	Нет	Нет	Да	Да

Совместимость версий KPSN с версиями Kaspersky Anti Targeted Attack Platform

Вы можете использовать Kaspersky Private Security Network (KPSN) вместо Kaspersky Security Network (KSN), чтобы не использовать отправку данных вашей организации за пределы локальной сети организации.

Информация о совместимости версий KPSN с версиями Kaspersky Anti Targeted Attack Platform приведена в таблице ниже.

Таблица 11. Совместимость версий KPSN с версиями Kaspersky Anti Targeted Attack Platform

Версия KPSN	Совместимость с KATA 4.1	Совместимость с KATA 5.0	Совместимость с KATA 5.1	Совместимость с KATA 6.0
KPSN 3.3	Да	Да	Да	Нет
KPSN 3.4	Нет	Нет	Нет	Да

Совместимость Kaspersky Anti Targeted Attack Platform с VK Cloud

Kaspersky Anti Targeted Attack Platform поддерживает развертывание на облачной платформе VK Cloud.

При развертывании приложения вы можете подключить к компоненту Central Node компоненты Sandbox.

Ограничения при развертывании Kaspersky Anti Targeted Attack Platform для работы с VK Cloud:

- Поддерживается работа только функционального блока KATA (см. раздел "Принцип работы приложения" на стр. 69).
- Поддерживается работа только сертифицированной версии приложения на базе операционной системы Astra Linux.
- Поддерживается работа только неотказоустойчивой версии приложения.
- Вы можете настроить интеграцию только с внешней системой KSMG. Подробнее об интеграции см. справку KSMG.
- Вы можете использовать режим распределенного решения, только используя интеграцию с KSMG.

Для функционирования компонента Sandbox необходимо выполнить следующие требования:

- На виртуальной машине должна быть включена вложенная виртуализация.
- Должны быть корректно настроены параметры сетевого интерфейса для доступа обрабатываемых объектов в интернет (см. раздел "Настройка параметров сетевого интерфейса для доступа обрабатываемых объектов в интернет" на стр. 219).

  Активация образов операционной системы Windows возможна только при корректной настройке сетевого интерфейса.

- Сетевой интерфейс для доступа обрабатываемых объектов в интернет должен быть изолирован от локальной сети вашей организации.
- Сетевой интерфейс для доступа обрабатываемых объектов в интернет должен быть подключен к подсети, не совпадающей с подсетью, к которой подключен управляющий интерфейс.

- Не рекомендуется использовать статический публичный IP-адрес для сетевого интерфейса, обрабатывающего доступ объектов в интернет.

Указания по эксплуатации и требования к среде

1. Установка, конфигурирование и управление приложения должны осуществляться в соответствии с эксплуатационной документацией.
2. Приложение должно эксплуатироваться на компьютерах, отвечающих минимальным требованиям, приведенным в разделе "Аппаратные и программные требования".
3. Перед установкой и началом эксплуатации приложения необходимо установить все доступные обновления для используемых версий ПО среды функционирования.
4. Должен быть обеспечен доступ приложения ко всем объектам информационной системы, которые необходимы приложению для реализации своих функциональных возможностей (к контролируемым объектам информационной системы).
5. Должна быть обеспечена совместимость приложения с контролируемыми ресурсами информационной системы.
6. Должна быть обеспечена возможность корректной совместной работы приложения со средствами антивирусной защиты других производителей в случае их совместного использования в информационной системе.
7. Должна быть обеспечена физическая защита элементов информационной системы, на которых установлено приложение.
8. Должна быть обеспечена синхронизация по времени между компонентами приложения, а также между приложением и средой его функционирования.
9. Персонал, ответственный за функционирование приложения, должен обеспечивать надлежащее функционирование приложения, руководствуясь эксплуатационной документацией.
10. Должна быть обеспечена доверенная связь между приложением и уполномоченными субъектами информационной системы (администраторами безопасности).
11. Функционирование приложения должно осуществляться в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности приложения.
12. Должен быть обеспечен доверенный канал получения обновлений БД ПКВ.
13. Должна быть обеспечена защищенная область для выполнения функций безопасности приложения.
14. Управление атрибутами безопасности, связанными с доступом к функциям и данным приложения, должно предоставляться только уполномоченным ролям (администраторам приложения и информационной системы).
15. Администратор должен установить в среде ИТ максимальное число попыток неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя с последующей блокировкой попыток аутентификации при превышении установленного значения.
16. Администратор должен задать метрику качества паролей, включающую требования к длине паролей, требования по запрещению использования определенных комбинаций символов, а также требования к категории используемых символов.

Предоставление данных

Для работы некоторых компонентов Kaspersky Anti Targeted Attack Platform необходима обработка данных на стороне "Лаборатории Касперского". Компоненты не отправляют данные без согласия администратора Kaspersky Anti Targeted Attack Platform.

Вы можете ознакомиться с перечнем данных и условиями их использования, а также дать согласие на обработку данных в следующих соглашениях между вашей организацией и "Лабораторией Касперского":

- В Лицензионном соглашении (например, при установке приложения).

  Согласно условиям Лицензионного соглашения, вы соглашаетесь в автоматическом режиме предоставлять "Лаборатории Касперского" информацию, перечисленную в Лицензионном соглашении в пункте Предоставление информации. Лицензионное соглашение входит в комплект поставки приложения.

- В Положении о KSN (например, при установке приложения или в меню администратора приложения после установки).

  При участии в Kaspersky Security Network в "Лабораторию Касперского" автоматически передается информация, полученная в результате работы Kaspersky Anti Targeted Attack Platform. Перечень передаваемых данных указан в Положении о KSN. Пользователь Kaspersky Anti Targeted Attack Platform самостоятельно принимает решение об участии в KSN. Положение о KSN входит в комплект поставки приложения.

  Перед тем, как данные KSN-статистики отправляются в "Лабораторию Касперского", они накапливаются в кеше на серверах с компонентами Kaspersky Anti Targeted Attack Platform.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского". Данные передаются по зашифрованным каналам связи.

При использовании Kaspersky Private Security Network в "Лабораторию Касперского" не передается информация о работе Kaspersky Anti Targeted Attack Platform, но данные KSN-статистики накапливаются в кеше на серверах с компонентами Kaspersky Anti Targeted Attack Platform в том же составе, что и при использовании Kaspersky Security Network. Эти накопленные данные KSN-статистики могут передаваться за пределы вашей организации в том случае, если сервер с приложением Kaspersky Private Security Network находится за пределами вашей организации. Администратору Kaspersky Private Security Network необходимо обеспечить безопасность этих данных самостоятельно.

kaspersky

В этом разделе

Служебные данные приложения 40
Данные компонентов Central Node и Sensor 45
Данные компонента Sandbox 52
Данные, пересылаемые между компонентами приложения 54
Данные в файлах трассировки приложения 60
Данные Kaspersky Endpoint Agent для Windows 60
Данные Kaspersky Endpoint Security для Windows 65
Данные Kaspersky Endpoint Security для Linux 65
Данные Kaspersky Endpoint Security для Mac 65

Служебные данные приложения

Возможность ограничить права пользователей серверов и операционных систем, на которые установлен компонент Central Node, средствами Kaspersky Anti Targeted Attack Platform не предусмотрена. Администратору рекомендуется контролировать доступ пользователей серверов и операционных систем, на которые установлено приложение, к персональным данным других пользователей любыми системными средствами на его усмотрение.

К служебным данным Kaspersky Anti Targeted Attack Platform относятся:

- Данные об учетных записях пользователей.
- Данные о подключенных к компоненту Central Node компьютерах, на которых установлен компонент Endpoint Agent.
- Данные о предустановках и правилах запрета.
- Данные о задачах, назначенных на компьютеры с компонентом Endpoint Agent.
- Данные о пользовательских правилах TAA (IOA).
- Данные о пользовательских правилах IDS.
- Данные о пользовательских правилах IOC.
- Данные о правилах сетевой изоляции.
- Данные об исключениях из проверки.
- Данные о шаблонах отчетов.
- Данные о сертификатах компонента Endpoint Agent.

  Указанные выше данные хранятся бессрочно на сервере с компонентом Central Node в директории `/data`, если компонент Central Node установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных бессрочно.

- Журнал событий ОС.

  Файлы журнала ОС хранятся бессрочно в директории `/var/log` на сервере с компонентом Central Node.

- Журнал с информацией о работе приложения.

  Файл журнала хранится бессрочно в директории `/data` на сервере с компонентом Central Node, если компонент установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных бессрочно.

- Очередь файлов на проверку.

  Файлы хранятся на сервере с компонентом Central Node в директории `/data`, если компонент установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных. Данные хранятся до выполнения проверки.

- Файлы, полученные с компьютеров с компонентом Endpoint Agent.

  Файлы хранятся на сервере с компонентом Central Node в директории `/data`, если компонент установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных. Данные ротируются при заполнении места на диске.

- Файлы с правилами YARA и IDS (пользовательские и от "Лаборатории Касперского").

  Файлы хранятся бессрочно в директории `/data` на сервере с компонентом Central Node, если компонент установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных бессрочно.

- Файлы с данными о переданных во внешние системы обнаружениях.

  Файлы хранятся бессрочно на сервере с компонентом Central Node в директории `/data`, если компонент установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных бессрочно.

- Артефакты компонента Sandbox.

  Файлы хранятся на сервере с компонентом Central Node в директории `/data`, если компонент установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных. Данные ротируются при заполнении места на диске.

- Файлы, для которых были созданы обнаружения компонентом Sandbox.

  Файлы хранятся на сервере с компонентом Central Node в директории `/data`, если компонент установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных. Данные ротируются при заполнении места на диске.

- Файлы сертификатов, которые используются для аутентификации компонентов приложения.

  Файлы хранятся бессрочно в директории `/data` на сервере с компонентом Central Node, PCN, SCN, Sensor или на компьютере с компонентом Endpoint Agent.

- Ключи шифрования, которые передаются между компонентами приложения.

  Файлы хранятся бессрочно в директории `/data` на сервере с компонентом Central Node, PCN, SCN, Sensor или на компьютере с компонентом Endpoint Agent.

- Копии сырого сетевого трафика.

  Файлы хранятся в хранилище, примонтированном к серверу с компонентом Sensor. Данные ротируются при заполнении места на диске.

- Фильтры ICAP-исключений

Файлы хранятся бессрочно на сервере с компонентом Central Node в директории `/data`, если компонент установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных бессрочно.

Приложение хранит об учетных записях пользователей следующую информацию:

- Идентификатор учетной записи.
- Имя учетной записи.
- Хеш и соль пароля учетной записи.
- Доменное имя пользователя.
- Роль учетной записи.
- Статус учетной записи.
- Права доступа к тенантам в режиме распределенного решения и мультитенантности.
- Идентификатор тенанта в режиме распределенного решения и мультитенантности.

Приложение хранит о подключенных к компоненту Central Node компьютерах, на которых установлен компонент Endpoint Agent, следующую информацию:

- Идентификатор компьютера, присвоенный Kaspersky Security Center.
- Имя компьютера.
- IP-адрес компьютера.
- Операционная система, используемая на компьютере.
- Версия приложения, которое выступает в роли компонента.
- Статус механизма самозащиты.
- Дата и время отправки первого и последнего пакета телеметрии, отправленного компоненту Central Node.
- Дата и время последней запущенной IOC-проверки.
- Результат последней запущенной IOC-проверки.
- Статус лицензии на хосте.

Приложение хранит о правилах запрета следующую информацию:

- MD5- или SHA256-хеш файла, запрещенного для запуска.
- Имя учетной записи пользователя, создавшего правило запрета.
- Имя учетной записи пользователя, изменившего правило запрета.
- Список компьютеров, на которых запрещен запуск файла.
- Журнал изменений правил запрета.
- Дата и время создания правила запрета.
- Дата и время изменения правила запрета.
- Имя правила запрета.
- Признак необходимости уведомления пользователя о блокировке запуска файла.

Приложение хранит о задачах, назначенных на компьютеры с компонентом Endpoint Agent, следующую информацию:

- Тип задачи.
- Имя компьютера.
- IP-адрес компьютера.
- Дата и время создания задачи.
- Срок действия задачи.
- Имя учетной записи пользователя, создавшего задачу.
- Данные параметров задачи.
- Данные отчета о выполнении задачи.
- Комментарий к задаче.

Приложение хранит о пользовательских правилах TAA (IOA) следующую информацию:

- Имя правила.
- Исходный код запроса, по которому осуществляется проверка.
- Идентификатор правила.
- Статус правила.
- Дата и время создания правила.
- Важность, указанная при добавлении правила.
- Уровень надежности в зависимости от вероятности ложных срабатываний, заданный при добавлении правила.

Приложение хранит о пользовательских правилах IDS следующую информацию:

- Имя учетной записи пользователя, загрузившего файл с правилами.
- Дата и время загрузки файла с правилами.
- Статус правила.
- Степень важности, указанная в файле с правилами.

Приложение хранит о пользовательских правилах IOC следующую информацию:

- Имя учетной записи пользователя, загрузившего файл с правилами.
- Имя IOC-файла.
- Содержимое IOC-файла.
- Дата и время загрузки IOC-файла.
- Статус IOC-правила.
- Степень важности, указанная в IOC-файле.
- Описание IOC-правила.

Приложение хранит о пользовательских правилах YARA следующую информацию:

- Имя учетной записи пользователя, загрузившего файл с правилами.

- Содержимое YARA-файла.
- Дата и время загрузки YARA-файла.
- Имя файла, содержащего YARA-правила.
- Степень важности.
- Статус YARA-правила.

Приложение хранит о правилах сетевой изоляции следующую информацию:

- Имя учетной записи пользователя, включившего сетевую изоляцию.
- Идентификатор изолированного компьютера.
- Имя правила.
- Статус правила.
- Список ресурсов, исключенных из сетевой изоляции.
- Дата и время изменения правила сетевой изоляции.
- Состояние правила.
- Срок действия правила сетевой изоляции.

Приложение хранит об исключениях из проверки следующую информацию:

- Имя учетной записи пользователя, добавившего исключение.
- Список объектов, исключенных из проверки.
- Идентификатор правила исключения.
- Имя исключения.
- Дата и время создания исключения.

Приложение хранит о шаблонах отчетов следующую информацию:

- Идентификатор учетной записи пользователя, создавшего или изменившего шаблон.
- Дата создания шаблона.
- Дата последнего изменения шаблона.
- Текст шаблона в виде HTML-кода.
- Имя шаблона.

Приложение хранит о сертификатах компонента Endpoint Agent следующую информацию:

- Имя учетной записи пользователя, загрузившего файл сертификата.
- Дайджест сертификата.
- Серийный номер сертификата.
- Публичный ключ.
- Срок окончания действия сертификата.

Приложение хранит о правилах проверки компонента Sandbox следующую информацию:

- Состояние правила.
- Тип правила.

- Маски включаемых объектов.
- Маски исключаемых объектов.
- Размер проверяемых файлов.
- Дата и время создания правила.
- Идентификатор виртуальной машины, на которой назначено правило.

Приложение хранит о конфигурации виртуальных машин следующую информацию:

- IP-адрес сервера с компонентом Sandbox.
- Список виртуальных машин.

Данные компонентов Central Node и Sensor

В этом разделе содержится следующая информация о данных пользователей, хранящихся на сервере с компонентом Central Node и на сервере с компонентом Sensor:

- состав хранимых данных;
- место хранения;
- срок хранения;
- доступ пользователей к данным.

В этом разделе

Данные трафика компонента Sensor 45
Данные в обнаружениях 46
Данные в событиях 49
Данные в отчетах 50
Данные об объектах в Хранилище и на карантине 51

Данные трафика компонента Sensor

Данные трафика компонента Sensor (см. раздел "Компонент Sensor" на стр. 66) хранятся на сервере с компонентом Sensor или на сервере с компонентами Sensor и Central Node, если Sensor и Central Node установлены на одном сервере или развернуты в виде кластера (см. раздел "Установка и первоначальная настройка приложения" на стр. 110).

Данные трафика записываются и хранятся в последовательно создаваемых файлах. Приложение перестает записывать данные в один файл и начинает записывать в следующий файл в следующих случаях:

- при достижении максимального размера файла (вы можете настроить этот параметр);
- по окончании заданного в настройках промежутка времени (вы можете настроить этот параметр);

- при перезагрузке службы сохранения трафика или всего приложения Kaspersky Anti Targeted Attack Platform.

По мере накопления данных трафика, Kaspersky Anti Targeted Attack Platform фильтрует данные и оставляет только следующую информацию:

- информацию, связанную с обнаружениями, выполненными технологией Targeted Attack Analyzer;
- PCAP-файлы, в которых:
  - IP-адрес источника или назначения совпадают каким-либо IP-адресом из обнаружения;
  - данные трафика относятся ко времени, отстоящему от времени обнаружения не более, чем на 15 минут.

Отфильтрованные данные трафика переносятся в отдельный раздел. Все остальные данные трафика (не отвечающие условиям фильтрации), удаляются.

Данные отфильтрованного трафика сохраняются в последовательно создаваемых файлах. Приложение перестает записывать данные в один файл и начинает записывать в следующий файл в следующих случаях:

- при достижении максимального размера файла;
- по окончании заданного в настройках промежутка времени.

Данные отфильтрованного трафика хранятся за последние сутки. Более старые данные удаляются.

Данные в обнаружениях

Данные пользователя могут содержаться в обнаружениях. Если компонент Central Node установлен на сервере, информация об обнаружениях и файлы, по результатам проверки которых возникло обнаружение, хранятся на сервере с компонентом Central Node в директории `/data/var/lib/kaspersky/storage/pgsql/10/data/`. При установке компонента Central Node на кластер информация об обнаружениях и файлы, по результатам проверки которых возникло обнаружение, хранятся на серверах хранения данных.

Возможность ограничить права пользователей серверов и операционных систем, на которые установлен компонент Central Node, средствами Kaspersky Anti Targeted Attack Platform не предусмотрена. Администратору рекомендуется контролировать доступ пользователей серверов и операционных систем, на которые установлено приложение, к персональным данным других пользователей любыми системными средствами на его усмотрение.

Во всех обнаружениях хранится следующая информация:

- Дата и время обнаружения.
- Дата и время изменения обнаружения.
- Категория обнаруженного объекта.
- Имя обнаруженного файла.
- Обнаруженный URL-адрес.
- MD5- , SHA256-хеш обнаруженного файла.

- Комментарии пользователя, добавленные в информацию об обнаружении.
- Идентификатор правила TAA(IOA), по которому было выполнено обнаружение.
- IP-адрес и имя компьютера, на котором выполнено обнаружение.
- Идентификатор компьютера, на котором выполнено обнаружение.
- User agent.
- Учетная запись пользователя, которому было назначено обнаружение.

При изменении обнаружения на сервере хранится следующая информация:

- Учетная запись пользователя, который изменил обнаружение.
- Учетная запись пользователя, которому было назначено обнаружение.
- Дата и время изменения обнаружения.
- Статус обнаружения.
- Пользовательский комментарий.

Если обнаружено сообщение электронной почты, на сервере может храниться следующая информация:

- Адреса электронной почты отправителя и получателей сообщения, копии и скрытой копии сообщения.
- Тема сообщения электронной почты.
- Дата и время поступления сообщения в Kaspersky Anti Targeted Attack Platform, с точностью до секунд.
- Все служебные заголовки сообщения (так, как они выглядят в сообщении).

Если обнаружение выполнено технологией URL Reputation, на сервере может храниться следующая информация:

- Имя компьютера, с которого были отправлены данные.
- Имя компьютера, получившего данные.
- IP-адрес компьютера, с которого были отправлены данные.
- IP-адрес компьютера, получившего данные.
- URI переданного ресурса.
- Информация о прокси-сервере.
- Уникальный идентификатор сообщения электронной почты.
- Адреса электронной почты отправителя и получателей сообщения (включая получателей копии и скрытой копии сообщения).
- Тема сообщения электронной почты.
- Дата и время поступления сообщения в Kaspersky Anti Targeted Attack Platform, с точностью до секунд.
- Список обнаруженных объектов.
- Время сетевого соединения.
- URL-адрес сетевого соединения.

- User agent.

Если обнаружение выполнено технологией Intrusion Detection System, на сервере может храниться следующая информация:

- Имя компьютера, с которого были отправлены данные.
- Имя компьютера, получившего данные.
- IP-адрес компьютера, с которого были отправлены данные.
- IP-адрес компьютера, получившего данные.
- Переданные данные.
- Время передачи данных.
- URL-адрес, извлеченный из файла с трафиком, User Agent, метод.
- Файл с трафиком, в котором произошло обнаружение.
- Категория объекта по базе IDS.
- Название пользовательского правила IDS, по которому было выполнено обнаружение.

Если обнаружение выполнено с помощью правил YARA, на сервере может храниться следующая информация:

- Версия правил YARA, с помощью которых было выполнено обнаружение.
- Категория обнаруженного объекта.
- Имя обнаруженного объекта.
- MD5-хеш обнаруженного объекта.
- Дата и время обнаружения объекта.

Если обнаружение выполнено с помощью компонента Sandbox, на сервере может храниться следующая информация:

- Версия баз приложения, с помощью которых было выполнено обнаружение.
- Категория обнаруженного объекта.
- Имена обнаруженных объектов.
- MD5-хеши обнаруженных объектов.
- Информация об обнаруженных объектах.

Если обнаружение выполнено в результате работы пользовательских правил IOC или TAA (IOA), на сервере может храниться следующая информация:

- Дата и время выполнения проверки.
- Идентификаторы компьютеров, на которых выполнено обнаружение.
- Имя правила TAA (IOA).
- Имя IOC-файла.
- Информация об обнаруженных объектах.
- Список хостов с компонентом Endpoint Agent.

Если обнаружение выполнено технологией Anti-Malware Engine, на сервере может храниться следующая

информация:

- Версии баз компонентов Kaspersky Anti Targeted Attack Platform, с помощью которых было выполнено обнаружение.
- Категория обнаруженного объекта.
- Список обнаруженных объектов.
- MD5-хеш обнаруженных объектов.
- Дополнительная информация об обнаружении.

Если обнаружение выполнено в результате повторного сканирования, на сервере может храниться следующая информация:

- Имя файла.

Если обнаружение выполнено в результате проверки файла, на сервере может храниться следующая информация:

- Полное имя обнаруженного файла.
- MD5-, SHA256-хеш обнаруженного файла.
- Размер обнаруженного файла.
- Информация о подписи файла.

Если обнаружение выполнено в результате проверки FTP-трафика, на сервере может храниться следующая информация:

- URI FTP-запроса.

Если обнаружение выполнено в результате проверки HTTP-трафика, на сервере может храниться следующая информация:

- URI HTTP-запроса.
- URI источника запроса.
- User agent.
- Информация о прокси-сервере.

Данные в событиях

Данные пользователя могут содержаться в событиях. Если компонент Central Node установлен на сервере, информация о произошедших событиях хранится на сервере с компонентом в директории `/data/var/lib/kaspersky/storage/fastsearch/elasticsearch/data/`. При установке компонента Central Node на кластер информация хранится на серверах хранения данных.

Данные ротируются по мере заполнения диска.

Возможность ограничить права пользователей серверов и операционных систем, на которые установлен компонент Central Node, средствами Kaspersky Anti Targeted Attack Platform не предусмотрена. Администратору рекомендуется контролировать доступ пользователей серверов и операционных систем, на которые установлено приложение, к персональным данным других пользователей любыми системными средствами на его усмотрение.

Данные о событиях могут содержать следующую информацию:

- Имя компьютера, на котором произошло событие.
- Уникальный идентификатор компьютера с Kaspersky Endpoint Agent.
- Имя пользователя, под учетной записью которого произошло событие.
- Имя группы, в которую входит пользователь.
- Тип события.
- Время события.
- Информация о файле, для которого записано событие: имя, путь, полное имя.
- MD5- и SHA256-хеш файла.
- Время создания файла.
- Время изменения файла.
- Флаги прав доступа к файлу.
- Переменные окружения процесса.
- Параметры командной строки.
- Текст команды, введенный в командную строку.
- Локальный IP-адрес адаптера.
- Локальный порт.
- Имя удаленного хоста.
- IP-адрес удаленного хоста.
- Порт на удаленном хосте.
- URL- и IP-адреса посещенных веб-сайтов, а также ссылки с этих веб-сайтов.
- Протокол сетевого соединения.
- Метод HTTP-запроса.
- Заголовок HTTP-запроса.
- Информация о переменных реестра Windows: путь к переменной, имя переменной, значение переменной.
- Содержание скрипта или двоичного файла, переданного на AMSI-проверку.
- Информация о событии в журнале Windows: тип события, идентификатор типа события, идентификатор события, пользователь, под учетной записью которого событие записано в журнал, полный текст события из журнала событий Windows в формате XML.

Данные в отчетах

Данные пользователя могут содержаться в отчетах. Если компонент Central Node установлен на сервере, информация о произошедших событиях хранится на сервере с компонентом в директории `/data/var/lib/kaspersky/storage/pgsql/10/data/` бессрочно. При установке компонента Central Node на кластер информация хранится на серверах хранения данных.

Возможность ограничить права пользователей серверов и операционных систем, на которые установлен компонент Central Node, средствами Kaspersky Anti Targeted Attack Platform не предусмотрена. Администратору рекомендуется контролировать доступ пользователей серверов и операционных систем, на которые установлено приложение, к персональным данным других пользователей любыми системными средствами на его усмотрение.

В отчетах может содержаться следующая информация:

- Дата создания отчета.
- Период, за который сформирован отчет.
- Идентификатор учетной записи пользователя, сформировавшего отчет.
- Статус отчета.
- Текст отчета в виде HTML-кода.
- Описание
- Имя шаблона, на основе которого создан отчет.

Данные об объектах в Хранилище и на карантине

Объекты в Хранилище и на карантине могут содержать данные пользователя. Информация об объектах в Хранилище и о копиях объектов, помещенных на карантин на компьютерах с Kaspersky Endpoint Agent, сохраненных на сервере с помощью задачи **Получить файл**, хранится на сервере с компонентом Central Node в директории `/data/var/lib/kaspersky/storage/pgsql/10/data/` бессрочно.

Возможность ограничить права пользователей серверов и операционных систем, на которые установлен компонент Central Node, средствами Kaspersky Anti Targeted Attack Platform не предусмотрена. Администратору рекомендуется контролировать доступ пользователей серверов и операционных систем, на которые установлено приложение, к персональным данным других пользователей любыми системными средствами на его усмотрение.

Данные об объектах в Хранилище и на карантине могут содержать следующую информацию:

- Имя объекта.
- Путь к объекту на компьютере с Kaspersky Endpoint Agent.
- MD5-, SHA256-хеш файла.
- Идентификатор пользователя, поместившего объект на карантин на компьютере с Kaspersky Endpoint Agent.
- Идентификатор пользователя, поместившего объект в Хранилище.
- IP-адрес компьютера, на котором хранится объект, помещенный на карантин.
- Имя компьютера, на котором хранится объект, помещенный на карантин.
- Уникальный идентификатор компьютера, на котором хранится объект, помещенный на карантин.
- Идентификатор правила TAA (IOA), по которому было выполнено обнаружение.

- Категория обнаруженного объекта.
- Результаты проверки объекта с помощью отдельных модулей и технологий приложения.
- Время загрузки файла.
- Метаинформация о проверенных файлах и источниках получения.

Данные компонента Sandbox

На время обработки тело переданного компонентом Central Node файла сохраняется в открытом виде на сервере с компонентом Sandbox. Во время обработки доступ к переданному файлу может получить администратор сервера в режиме Technical Support Mode. Проверенный файл удаляется специальным скриптом по расписанию. По умолчанию один раз в 60 минут.

Информация о данных, хранящихся на сервере с компонентом Sandbox, приведена в таблице ниже.

Таблица 12. Данные, хранящиеся на сервере с компонентом Sandbox

Состав данных	Место хранения	Срок хранения	Доступ к данным
Проверяемые файлы	`/var/opt/kaspersky/sandbox/library/`	После получения компонентом Central Node результатов проверки или до автоматического удаления, но не более 24 часов.	Доступ пользователей определяется администратором с помощью средств операционной системы.
Результат проверки файлов	• `/var/opt/kaspersky/sandbox/library/` • `/tmp/`	После получения компонентом Central Node результатов проверки или до автоматического удаления, но не более 24 часов.	Доступ пользователей определяется администратором с помощью средств операционной системы.
Параметры задач	• `/var/opt/kaspersky/sandbox/library/` • база данных компонента Sandbox	После получения компонентом Central Node результатов проверки или до автоматического удаления, но не более 24 часов в директории `/var/opt/kaspersky/sandbox/library/`. В базе данных компонента Sandbox до 90 дней.	Доступ пользователей к директории `/var/opt/kaspersky/sandbox/library/` определяется администратором с помощью средств операционной системы. Для аутентификации пользователей в базе данных требуется пароль. Доступ к файлам базы данных имеют только пользователи, от имени которых запущены процессы базы данных,

			и пользователь с правами root. Доступ осуществляется только по шифрованному каналу IPSec.
Файлы трассировки	/var/log/kaspersky/sandbox/	До 21 дня.	Доступ пользователей определяется администратором с помощью средств операционной системы. Действия с файлами трассировки доступны только для авторизованных пользователей. Информация о действиях с файлами трассировки сохраняется в журнале событий приложения.
Настройки источника обновлений	/var/opt/kaspersky/apt-updater	До изменения или удаления.	Доступ пользователей определяется администратором с помощью средств операционной системы.
Настройки минимальной длины пароля	/var/opt/kaspersky/apt-config-ram-common/validator.conf	До изменения или удаления.	Доступ пользователей определяется администратором с помощью средств операционной системы.
Виртуальные машины	/vm	До изменения или удаления.	Доступ пользователей определяется администратором с помощью средств операционной системы.
Загруженные образы операционных систем и приложений в формате iso	/var/opt/kaspersky/sandbox/custom_images/iso	До изменения или удаления.	Доступ пользователей определяется администратором с помощью средств операционной системы.

Данные, пересылаемые между компонентами приложения

Central Node, Kaspersky Endpoint Agent для Windows, Kaspersky Endpoint Security для Windows

Приложения Kaspersky Endpoint Agent для Windows и Kaspersky Endpoint Security для Windows отправляют на компонент Central Node отчеты о выполнении задач, информацию о событиях и обнаружениях, произошедших на компьютерах с этими приложениями, а также информацию о терминальных сессиях.

Если связь с компонентом Central Node отсутствует, все данные, предназначенные для отправки, накапливаются до тех пор, пока они не будут отправлены на компонент Central Node или приложение Kaspersky Endpoint Agent для Windows или Kaspersky Endpoint Security для Windows не будет удалено с компьютера, но не более 21 дня.

Если событие произошло на компьютере пользователя, приложения отправляют следующие данные в базу событий:

1. Общие сведения для всех событий:
   - Тип события.
   - Время события.
   - Учетная запись пользователя, от имени которой было совершено событие.
   - Имя хоста, на котором произошло событие.
   - IP-адрес хоста.
   - Тип операционной системы, установленной на хосте.
2. Событие создания файла.
   - Сведения о процессе, создавшем файл: имя файла процесса, MD5-, SHA256-хеш файла процесса.
   - Имя файла.
   - Путь к файлу.
   - Полное имя файла.
   - MD5-, SHA256-хеш файла.
   - Дата создания и изменения файла.
   - Размер файла.
3. Событие мониторинга реестра.
   - Сведения о процессе, изменившем реестр: ID процесса, имя файла процесса, MD5-, SHA256-хеш файла процесса.
   - Путь к ключу реестра.
   - Имя параметра реестра.
   - Значение параметра реестра.
   - Тип параметра реестра.

- Предыдущий путь к ключу реестра.
- Предыдущее значение параметра реестра.
- Предыдущий тип параметра реестра.

4. Событие загрузки драйвера.
   - Имя файла.
   - Путь к файлу.
   - Полное имя файла.
   - MD5-, SHA256-хеш файла.
   - Размер файла.
   - Дата создания и изменения файла.
5. Событие открытия порта на прослушивание.
   - Сведения о процессе, открывшем порт на прослушивание: имя файла процесса, MD5-, SHA256-хеш файла процесса.
   - Номер порта.
   - IP-адрес адаптера.
6. Событие в журнале ОС.
   - Время события, хост, на котором произошло событие, имя учетной записи пользователя.
   - ID события.
   - Имя журнала/канала.
   - ID события в журнале.
   - Имя провайдера.
   - Подтип события аутентификации.
   - Имя домена.
   - Удаленный IP-адрес.
   - Поля заголовка события: ProviderName, EventId, Version, Level, Task, Opcode, Keywords, TimeCreatedSystemTime, EventRecordId, CorellationActivityId, ExecutionProcessID, ThreadID, Channel, Computer.
   - Поля тела события: AccessList, AccessFiles mask, AccountExpires, AllowedToDelegateTo, Application, AuditPolicyChanges, AuthenticationPackageName, CategoryId, CommandLine, DisplayName, Dummy, ElevatedToken, EventCode, EventProcessingFailure, FailureReason, FilterRTID, HandleId, HomeDirectory, HomePath, ImpersonationLevel, IpAddress, IpPort, KeyLength, LayerName, LayerRTID, LmPackageName, LogonGuid, LogonHours, LogonProcessName, LogonType, MandatoryLabel, MemberName, MemberSid, NewProcessId, NewProcessName, NewUacValue, NewValue, NewValueType, ObjectName, ObjectServer, ObjectType, ObjectValueName, OldUacValue, OldValue, OldValueType, OperationType, PackageName, ParentProcessName, PasswordLastSet, PrimaryGroupId, PriviledgeList, ProcessId, ProcessName, ProfileChanged, ProfilePath, Protocol, PublisherId, ResourceAttributes, RestrictedAdminMode, SamAccountName, ScriptPath, ServiceAccount, ServiceFileName, ServiceName, ServiceStartType, ServiceType, SettingType, SettingValue, ShareLocalPath, ShareName, SidHistory, SourceAddress, SourcePort, Status, SubcategoryGuid, SubcategoryId, SubjectDomainName, SubjectLogonId, SubjectUserName, SubjectUserSid, SubStatus, TargetDomainName, TargetLinkedLogonId,

TargetLogonId, TargetOutboundDomainName, TargetOutboundUserName, TargetUserName, TargetUserSid, TaskContent, TaskName, TokenElevationType, TransmittedServices, UserAccountControl, UserParameters, UserPrincipalName, UserWorkstations, VirtualAccount, Workstation, WorkstationName.

7. Событие запуска процесса.
   - Сведения о файле процесса: имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, размер файла, дата создания и изменения файла, имя организации, выпустившей цифровой сертификат файла, результат проверки цифровой подписи файла.
   - UniquePID.
   - Параметры запуска процесса.
   - Время запуска процесса.
   - Сведения о родительском процессе: путь к файлу, UniquePID, MD5-, SHA256-хеш файла процесса, параметры запуска процесса.
8. Событие остановки процесса
   - Сведения о файле процесса: имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, размер файла, время завершения процесса.
   - UniquePID.
   - Параметры запуска процесса.
   - Сведения о родительском процессе: путь к файлу, UniquePID, MD5-, SHA256-хеш файла процесса, параметры запуска процесса.
9. Событие загрузки модуля.
   - Сведения о файле, загрузившем модуль: UniquePID, имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, размер файла.
   - Имя DLL.
   - Путь к DLL.
   - Полное имя DLL.
   - MD5-, SHA256-хеш DLL.
   - Размер DLL.
   - Дата создания и изменения DLL.
   - Имя организации, выпустившей цифровой сертификат DLL.
   - Результат проверки цифровой подписи DLL.
10. Событие блокирования запуска процесса.
    - Сведения о файле, который пытались выполнить: имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, размер файла, дата создания и изменения файла.
    - Параметры командной строки.
11. Событие блокирования запуска файла.
    - Сведения о файле, который пытались открыть: имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, тип контрольной суммы, по которой произведена блокировка, размер файла (0 – MD5, !=0 – SHA256, для поиска не используется).

- Сведения об исполняемом файле: имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, размер файла, дата создания и изменения файла.
- Сведения о родительском процессе: имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, PID, UniquePID.

12. Событие приложения Kaspersky Endpoint Security для Windows.
    - Результат проверки.
    - Название обнаруженного объекта.
    - Идентификатор записи в базах приложения.
    - Время выпуска баз приложения, с помощью которых было выполнено обнаружение.
    - Режим обработки объекта.
    - Категория обнаруженного объекта (например, название вируса).
    - MD5-хеш обнаруженного объекта.
    - SHA256-хеш обнаруженного объекта.
    - Уникальный идентификатор процесса.
    - PID процесса, отображаемый в диспетчере задач Windows.
    - Командная срока запуска процесса.
    - Причина ошибки при обработке объекта.
    - Содержание скрипта, проверенного с помощью AMSI.
13. Событие AMSI-проверки.
    - Содержание скрипта, проверенного с помощью AMSI.

Central Node, Kaspersky Endpoint Security для Linux, Kaspersky Endpoint Security для Mac

Приложения Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Mac отправляют на компонент Central Node отчеты о выполнении задач, информацию о событиях и обнаружениях, произошедших на компьютерах с этими приложениями, а также информацию о терминальных сессиях.

Если связь с компонентом Central Node отсутствует, все данные, предназначенные для отправки, накапливаются до тех пор, пока они не будут отправлены на компонент Central Node или приложение Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac не будет удалено с компьютера, но не более 21 дня.

Если событие произошло на компьютере пользователя, Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Mac отправляют следующие данные в базу событий:

1. Общие сведения для всех событий:
    - Тип события.
    - Время события.
    - Учетная запись пользователя, от имени которой было совершено событие.
    - Имя хоста, на котором произошло событие.

- IP-адрес хоста.
- Тип и версия операционной системы, установленной на хосте.
- Имя хоста, с которого был совершен удаленный вход в систему.
- Имя пользователя, назначенное при регистрации в системе.
- Группа, к которой принадлежит пользователь.
- Имя пользователя, которое использовалось для входа в систему.
- Группа, к которой принадлежит пользователь, чье имя использовалось для входа в систему.
- Имя пользователя, создавшего файл.
- Название группы, пользователи которой могут изменить или удалить файл.
- Разрешения, которые могут использоваться для доступа к файлу.
- Наследуемые привилегии файла.

Приложение Kaspersky Endpoint Security для Mac не отправляет данные о наследуемых привилегиях файла.

2. Событие запуска процесса.
   - Сведения о файле процесса: имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, размер файла.
   - UniquePID.
   - Команда, с помощью которой был запущен процесс.
   - Тип процесса.
   - Переменные окружения процесса.
   - Время запуска процесса.
   - Время завершения процесса.
   - Сведения о родительском процессе: путь к файлу, UniquePID, MD5-, SHA256-хеш файла процесса, команда, с помощью которой был запущен процесс.
3. Событие создания файла.
   - Сведения о процессе, создавшем файл: имя файла процесса, MD5-, SHA256-хеш файла процесса.
   - Имя файла.
   - Путь к файлу.
   - Полное имя файла.
   - Тип файла.
   - MD5-, SHA256-хеш файла.
   - Дата создания и изменения файла.
   - Размер файла.
4. Событие в журнале ОС.

- Время события.
- Тип события.
- Результат операции.
- Сведения о родительском процессе: путь к файлу, UniquePID, MD5-, SHA256-хеш файла процесса, команда, с помощью которой был запущен процесс.

Central Node и Sandbox

Компонент Central Node отправляет на компонент Sandbox файлы и URL-адреса, выделенные из сетевого или почтового трафика. Перед передачей файлы никак не изменяются. Компонент Sandbox отправляет компоненту Central Node результаты проверки.

Central Node и Sensor

Приложение может пересылать между компонентами Central Node и Sensor следующие данные:

- Файлы и сообщения электронной почты.
- Данные об обнаружениях, выполненных технологиями Intrusion Detection System и URL Reputation.
- Информацию о лицензии.
- Список данных, исключенных из проверки.
- Данные приложения Kaspersky Endpoint Agent, если настроена интеграция с прокси-сервером.
- Базы приложения, если настроено получение обновления баз от компонента Central Node.

Серверы с ролями PCN и SCN

Если приложение работает в режиме распределенного решения, то между PCN и подключенными SCN передаются следующие данные:

- Об обнаружениях.
- О событиях.
- О задачах.
- О политиках.
- О проверке по пользовательским правилам IOC, TAA (IOA), IDS, YARA.
- О файлах в Хранилище.
- Об учетных записях пользователей.
- О лицензии.
- Список компьютеров с компонентом Endpoint Agent.
- Объекты, помещенные в Хранилище.
- Объекты, помещенные на карантин на компьютерах с компонентом Endpoint Agent.
- Файлы, прикрепленные к обнаружениям.
- IOC- и YARA-файлы.

Данные в файлах трассировки приложения

Возможность ограничить права пользователей серверов и операционных систем, на которые установлен компонент Central Node, средствами Kaspersky Anti Targeted Attack Platform не предусмотрена. Администратору рекомендуется контролировать доступ пользователей серверов и операционных систем, на которые установлено приложение, к персональным данным других пользователей любыми системными средствами на его усмотрение.

В файлы трассировки могут попасть любые персональные данные пользователя или конфиденциальные данные вашей организации. Файлы хранятся в директории `/data/var/log/kaspersky` бессрочно.

Данные Kaspersky Endpoint Agent для Windows

Вы можете посмотреть подробную информацию о данных Kaspersky Endpoint Agent, которые хранятся и обрабатываются локально, в справке приложения:

- Данные в запросах к компоненту KATA Central Node.
- Служебные данные.
- Данные в файлах трассировки и дампов.
- Данные о принятии условий Положения о KSN.
- Данные о событиях Журнала событий Windows.

В этом разделе

Данные, получаемые от компонента Central Node 60
Данные в обнаружениях и событиях 62
Данные в отчетах о выполнении задач 63
Данные в журнале установки 64
Данные о файлах, запрещенных к запуску 64
Данные, связанные с выполнением задач 64

Данные, получаемые от компонента Central Node

Приложение Kaspersky Endpoint Agent сохраняет на жестком диске компьютера значения параметров, получаемые от компонента Central Node. Данные сохраняются в открытом незашифрованном виде в папке `C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\data`.

По умолчанию при включенной самозащите доступ к файлам на чтение имеют только пользователи с правами System и Administrator. При выключенной самозащите пользователи с правами System и Administrator могут также удалять файлы, изменять их содержимое и изменять права доступа к ним.

Приложение Kaspersky Endpoint Agent не управляет правами доступа к данной папке и ее файлам. Доступ определяет системный администратор.

Данные удаляются при удалении приложения Kaspersky Endpoint Agent.

Данные, получаемые от компонента Central Node, могут содержать следующую информацию:

- О сетевых соединениях.
- Об операционной системе, установленной на сервере с компонентом Central Node.
- Об учетных записях пользователей операционной системы.
- О пользовательских сессиях в операционной системе.
- О журнале событий Windows.
- О ресурсе типа RT_VERSION.
- О содержимом PE-файла.
- О службах операционной системы.
- Сертификат сервера с компонентом Central Node.
- URL- и IP-адреса посещенных веб-сайтов.
- Заголовки протокола HTTP.
- Имя компьютера.
- MD5-хеши файлов.
- Уникальный идентификатор компьютера с Kaspersky Endpoint Agent.
- Имена и значения ключей реестра Windows.
- Пути к ключам реестра Windows.
- Имена переменных реестра Windows.
- Имя записи локального DNS-кеша.
- Адрес из записи локального DNS-кеша в формате IPv4.
- IP-адрес или имя запрашиваемого хоста из локального DNS-кеша.
- Хост элемента локального DNS-кеша.
- Доменное имя элемента локального DNS-кеша.
- Адрес элемента ARP-кеша в формате IPv4.
- Физический адрес элемента APR-кеша.
- Серийный номер логического диска.
- Домашняя директория локального пользователя.
- Имя учетной записи пользователя, запустившего процесс.
- Путь к скрипту, запускаемому при входе пользователя в систему.
- Имя пользователя, под учетной записью которого произошло событие.
- Имя компьютера, на котором произошло событие.
- Полные пути к файлам компьютеров с Kaspersky Endpoint Agent.

- Имена файлов компьютеров с Kaspersky Endpoint Agent.
- Маски файлов компьютеров с Kaspersky Endpoint Agent.
- Полные имена папок компьютеров с Kaspersky Endpoint Agent.
- Комментарии поставщика файла.
- Маска файла-образа процесса.
- Путь к файлу-образу процесса, открывшего порт.
- Имя процесса, открывшего порт.
- Локальный IP-адрес порта.
- Доверенный публичный ключ цифровой подписи исполняемых модулей.
- Имя процесса.
- Имя сегмента процесса.
- Параметры командной строки.

Данные в обнаружениях и событиях

Данные о событиях хранятся в бинарном виде в папке `C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\kata` в открытом незашифрованном виде.

По умолчанию при включенной самозащите доступ к файлам на чтение имеют только пользователи с правами System и Administrator. При выключенной самозащите пользователи с правами System и Administrator могут также удалять файлы, изменять их содержимое и изменять права доступа к ним. Приложение Kaspersky Endpoint Agent не управляет правами доступа к данной папке и ее файлам. Доступ определяет системный администратор.

Данные о событиях могут содержать следующую информацию:

- Об исполняемых модулях.
- О сетевых соединениях.
- Об операционной системе, установленной на компьютере с Kaspersky Endpoint Agent.
- О пользовательских сессиях в операционной системе.
- Об учетных записях пользователей операционной системы.
- О журнале событий Windows.
- Об обнаружениях Kaspersky Endpoint Security для Windows.
- Об организационных подразделениях (OU) Active Directory.
- Заголовки протокола HTTP.
- Полное доменное имя компьютера.
- MD5-, SHA256-хеш файлов и их фрагментов.
- Уникальный идентификатор компьютера с Kaspersky Endpoint Agent.
- Уникальные идентификаторы сертификатов.
- Издатель сертификата.

- Субъект сертификата.
- Название алгоритма, при помощи которого выполнен отпечаток сертификата.
- Адрес и порт локального сетевого интерфейса.
- Адрес и порт удаленного сетевого интерфейса.
- Поставщик приложения.
- Название приложения.
- Имя переменной реестра Windows.
- Путь к ключу реестра Windows.
- Данные переменной реестра Windows.
- Имя обнаруженного объекта.
- Идентификатор Агента администрирования Kaspersky Security Center.
- Содержимое файла hosts.
- Командная строка запуска процесса.

Данные в отчетах о выполнении задач

Перед отправкой на компонент Central Node отчеты, а также сопутствующие файлы временно сохраняются на жестком диске компьютера с приложением Kaspersky Endpoint Agent. Отчеты о выполнении задач сохраняются в архивированном незашифрованном виде в папке C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\kata\data_queue.

По умолчанию при включенной самозащите доступ к файлам на чтение имеют только пользователи с правами System и Administrator. При выключенной самозащите пользователи с правами System и Administrator могут также удалять файлы, изменять их содержимое и изменять права доступа к ним. Приложение Kaspersky Endpoint Agent не управляет правами доступа к данной папке и ее файлам. Доступ определяет системный администратор.

Отчеты о выполнении задач содержат следующую информацию:

- О результатах выполнения задач.
- Об исполняемых модулях.
- О процессах операционной системы.
- Об учетных записях пользователей.
- О пользовательских сессиях.
- Полное доменное имя компьютера.
- Уникальный идентификатор компьютера с Kaspersky Endpoint Agent.
- Файлы компьютера с Kaspersky Endpoint Agent.
- Имена альтернативных потоков NTFS.
- Полные пути к файлам компьютера с Kaspersky Endpoint Agent.
- Полные имена папок компьютера с Kaspersky Endpoint Agent.
- Содержимое стандартного потока вывода процесса.

- Содержимое стандартного потока ошибок процесса.

Данные в журнале установки

Администратор может включить запись журнала установки приложения Kaspersky Endpoint Agent (стандартными средствами msiexec) при установке с помощью командной строки. Администратор указывает путь к файлу, в котором будет сохраняться журнал установки.

В журнал записываются шаги процесса установки, а также командная строка вызова msiexec, которая содержит адрес сервера с компонентом Central Node и путь к файлу журнала установки.

Данные о файлах, запрещенных к запуску

Данные о файлах, запрещенных к запуску, хранятся в папке C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\kata в открытом незашифрованном виде.

По умолчанию при включенной самозащите доступ к файлам на чтение имеют только пользователи с правами System и Administrator. При выключенной самозащите пользователи с правами System и Administrator могут также удалять файлы, изменять их содержимое и изменять права доступа к ним. Приложение Kaspersky Endpoint Agent не управляет правами доступа к данной папке и ее файлам. Доступ определяет системный администратор.

Данные о файлах, запрещенных к запуску, могут содержать следующую информацию:

- Полный путь к запрещенному файлу.
- MD5-хеш файла.
- SHA256-хеш файла.
- Команда запуска процесса.

Данные, связанные с выполнением задач

При выполнении задачи помещения файла на карантин архив, содержащий этот файл, временно сохраняется в незашифрованном виде в одной из следующих папок:

- для приложения Kaspersky Endpoint Agent, входящего в состав приложения Kaspersky Endpoint Security, в папке C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\kata\temp;
- для приложения Kaspersky Endpoint Agent, установленного из пакета Kaspersky Anti Targeted Attack Platform, в папке C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\data\kata\temp.

При выполнении задачи запуска программы на хосте приложение Kaspersky Endpoint Agent локально хранит содержимое стандартных потоков вывода и ошибок запущенного процесса в открытом незашифрованном виде до тех пор, пока отчет о выполнении задачи не будет отправлен на компонент Central Node. Файлы хранятся в одной из следующих папок:

- для приложения Kaspersky Endpoint Agent, входящего в состав приложения Kaspersky Endpoint Security, в папке `C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\kata\temp`;

- для приложения Kaspersky Endpoint Agent, установленного из пакета Kaspersky Anti Targeted Attack Platform, в папке `C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\data\kata\temp`.

По умолчанию при включенной самозащите доступ к файлам на чтение имеют только пользователи с правами System и Administrator. При выключенной самозащите пользователи с правами System и Administrator могут также удалять файлы, изменять их содержимое и изменять права доступа к ним. Приложение Kaspersky Endpoint Agent не управляет правами доступа к данной папке и ее файлам. Доступ определяет системный администратор.

Данные Kaspersky Endpoint Security для Windows

Вы можете посмотреть подробную информацию о передаваемых Kaspersky Endpoint Security данных в справке приложения:

- Предоставление данных в рамках Лицензионного соглашения.
- Предоставление данных при использовании Kaspersky Security Network.
- Соответствие законодательству Европейского союза (GDPR).

Данные Kaspersky Endpoint Security для Linux

Вы можете посмотреть подробную информацию о передаваемых Kaspersky Endpoint Security данных в справке приложения.

Данные Kaspersky Endpoint Security для Mac

Вы можете посмотреть подробную информацию о передаваемых Kaspersky Endpoint Security данных в справке приложения.

Архитектура приложения

В состав приложения входят следующие основные компоненты:

- *Sensor (см. раздел "Компонент Sensor" на стр. 66).* Выполняет прием и проверку данных, а также может использоваться в качестве прокси-сервера (см. раздел "Настройка перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor" на стр. 177) при обмене данными между компонентом Endpoint Agent, если он представлен приложением Kaspersky Endpoint Agent, и компонентом Central Node.
- *Central Node* (см. раздел "*Компонент Central Node*" на стр. 67). Выполняет прием и проверку данных, исследование поведения объектов, а также публикацию результатов исследования в веб-интерфейс приложения.
- *Sandbox* (см. раздел "*Компонент Sandbox*" на стр. 68). Запускает виртуальные образы операционных систем. Запускает файлы в этих операционных системах и отслеживает поведение файлов в каждой операционной системе для выявления вредоносной активности и признаков целевых атак на IT-инфраструктуру организации.
- *Endpoint Agent* (см. раздел "*Компонент Endpoint Agent*" на стр. 68). Устанавливается на рабочие станции и серверы, входящие в IT-инфраструктуру организации. Осуществляет постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами.

В этом разделе

Компонент Sensor 66

Компонент Central Node 67

Компонент Sandbox 68

Компонент Endpoint Agent 68

Компонент Sensor

На каждом сервере с компонентом Sensor работают следующие модули Kaspersky Anti Targeted Attack Platform:

- *Sensor.* Выполняет прием данных из сетевого и почтового трафика и передает их на обработку на сервер с компонентом Central Node.
- *Intrusion Detection System* (далее также *IDS*). Выполняет проверку интернет-трафика на наличие признаков вторжения в IT-инфраструктуру организации.
- *KSN.* Выполняет для Kaspersky Anti Targeted Attack Platform проверку репутации файлов и URL-адресов в базе знаний Kaspersky Security Network и предоставляет сведения о категориях веб-сайтов (например, вредоносный веб-сайт, фишинговый веб-сайт).

  *Kaspersky Security Network (*далее также *KSN)* – инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает

эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Если вы не хотите участвовать в KSN, вы можете использовать *Kaspersky Private Security Network* (далее также *KPSN*) – решение, позволяющее пользователям получать доступ к репутационным базам Kaspersky Security Network, а также другим статистическим данным, не отправляя данные в Kaspersky Security Network со своих компьютеров.

- *URL Reputation.* Обнаруживает вредоносные, фишинговые URL-адреса и URL-адреса, которые ранее использовались злоумышленниками для целевых атак и вторжений в IT-инфраструктуру организаций.

В качестве компонента Sensor также может использоваться почтовый сенсор (см. раздел "Настройка интеграции с внешними системами" на стр. 300) – сервер или виртуальная машина, на которой установлено приложение "Лаборатории Касперского" Kaspersky Secure Mail Gateway (далее также "KSMG") или Kaspersky Security для Linux Mail Server (далее также "KLMS"). Эти приложения отправляют сообщения электронной почты на обработку в Kaspersky Anti Targeted Attack Platform. По результатам обработки сообщений электронной почты в Kaspersky Anti Targeted Attack Platform KSMG и KLMS могут блокировать пересылку сообщений.

Компонент Sensor также может использоваться в качестве прокси-сервера для соединений, исходящих от приложения Kaspersky Endpoint Agent.

Если в качестве компонента Sensor используется приложение KSMG или KLMS, то правила исключений из проверки, настроенные по получателям сообщений и MD5-суммам файлов, не передаются в KSMG и KLMS и не применяются при обработке сообщений приложениями KSMG и KLMS.

Компонент Central Node

Компонент может быть развернут на одном сервере или в виде отказоустойчивого кластера, который состоит из серверов 2 ролей – серверов хранения и обрабатывающих серверов.

Отказоустойчивость достигается за счет дублирования данных между серверами хранения и избыточности вычислительных ресурсов: при выходе из строя одного сервера его функции выполняет другой сервер с аналогичной ролью. Kaspersky Anti Targeted Attack Platform при этом продолжает работать.

На каждом сервере или кластере с компонентом Central Node работают следующие модули, ядра и технологии приложения:

- *Anti-Malware Engine* (далее также *AM* и *AM Engine*). Выполняет проверку файлов и объектов на вирусы и другие программы, представляющие угрозу IT-инфраструктуре организации, с помощью антивирусных баз.
- *Mobile Attack Analyzer* (далее также *MAA*). Выполняет проверку исполняемых файлов формата APK в облачной инфраструктуре на основе технологии машинного обучения. В результате проверки Kaspersky Anti Targeted Attack Platform получает информацию об обнаруженных угрозах или их отсутствии.
- *YARA*. Выполняет проверку файлов и объектов на наличие признаков целевых атак на IT-инфраструктуру организации с помощью баз YARA-правил, создаваемых пользователями Kaspersky Anti Targeted Attack Platform.

- *Targeted Attack Analyzer* (далее также *TAA*, *TA Analyzer*). Выполняет анализ и проверку сетевой активности программного обеспечения, установленного на компьютеры локальной сети организации, на основе правил TAA (IOA). Выполняет поиск признаков сетевой активности, на которую пользователю Kaspersky Anti Targeted Attack Platform рекомендуется обратить внимание, а также признаков целевых атак на IT-инфраструктуру организации.
- *KSN*. Выполняет для Kaspersky Anti Targeted Attack Platform проверку репутации файлов и URL-адресов в базе знаний Kaspersky Security Network и предоставляет сведения о категориях веб-сайтов (например, вредоносный веб-сайт, фишинговый веб-сайт).

Компонент Sandbox

На серверах с компонентом Sandbox запускаются виртуальные машины с образами операционных систем (см. раздел «Установка и настройка образов операционных систем и приложений для работы компонента Sandbox» на стр. 221).

Компонент Sandbox запускает объекты в этих операционных системах и анализирует поведение объектов для выявления вредоносной активности, признаков целевых атак на IT-инфраструктуру организации.

По умолчанию максимальный размер проверяемого файла составляет 100 МБ. Вы можете настроить параметры проверки в меню администратора консоли управления приложением.
Максимальный уровень вложенности проверяемых архивов составляет 32.
Максимальное количество объектов, которое может находиться в очереди на проверку компонентом Sandbox за одни сутки, составляет 20 тысяч объектов. По достижении этого ограничения приложение удаляет 10% объектов, поступивших на проверку раньше остальных, и заменяет их новыми объектами, поступившими на проверку. Удаленные объекты сохраняются в приложении со статусом NOT_SCANNED (непроверенные).

Компонент Endpoint Agent

Программный компонент. Может быть представлен следующими приложениями:

- Kaspersky Endpoint Agent для Windows.
- Kaspersky Endpoint Security для Windows.
- Kaspersky Endpoint Security для Linux.
- Kaspersky Endpoint Security для Mac.

Приложения устанавливаются на рабочие станции и серверы в IT-инфраструктуре организации (далее также "компьютеры"). На этих компьютерах приложения постоянно наблюдают за процессами, открытыми сетевыми соединениями и изменяемыми файлами и отправляют данные наблюдения на сервер с компонентом Central Node.

Компьютеры, предназначенные для установки приложений, должны удовлетворять аппаратным и программным требованиям (см. раздел "Аппаратные и программные требования" на стр. 27).

Принцип работы приложения

Приложение Kaspersky Anti Targeted Attack Platform включает в себя два функциональных блока:

- Kaspersky Anti Targeted Attack (далее также "KATA"), обнаруживающий угрозы по периметру IT-инфраструктуры предприятия.
- Kaspersky Endpoint Detection and Response (далее также "KEDR"), обеспечивающий защиту компьютеров локальной сети организации.

Вы можете использовать как полную функциональность приложения (ключ KATA и ключ KEDR), так и неполную (только ключ KATA или только ключ KEDR).

Принцип работы Kaspersky Anti Targeted Attack

Kaspersky Anti Targeted Attack включает в себя следующие компоненты:

- Sensor.
- Central Node.
- Sandbox.

Компоненты Sensor, Central Node и Sandbox взаимодействуют между собой по следующему принципу:

- Компонент Sensor получает зеркалированный SPAN-, ERSPAN-, RSPAN-трафик, объекты и метаинформацию HTTP-, FTP-, SMTP- и DNS-протоколов, данные HTTP- и FTP-трафика, а также HTTPS-трафика (если администратор настроил подмену SSL-сертификата на прокси-сервере), копии сообщений электронной почты и производит с полученными данными следующие действия:
  - Проверяет интернет-трафик на наличие признаков вторжения в IT-инфраструктуру организации с помощью технологии Intrusion Detection System (далее также "IDS").

    Технология IDS позволяет распознать и обнаружить сетевую активность по 80 протоколам, в частности по 53 протоколам прикладного уровня модели TCP/IP, фиксируя подозрительный трафик и сетевые атаки. В числе поддерживаемых протоколов TCP, UDP, FTP, TFTP, SSH, SMTP, SMB, CIF, SSL, HTTP, HTTP/2, HTTPS, TLS, ICMPv4, ICMPv6, IPv4, IPv6, IRC, LDAP, NFS, DNS, RDP, DCERPC, MS-RPC, WebSocket, Citrix и другие.
  - Проверяет репутацию файлов и URL-адресов по базе знаний Kaspersky Security Network (далее также "KSN") или Kaspersky Private Security Network (далее также "KPSN").
  - Отправляет объекты и файлы на проверку компоненту Central Node.

  В качестве компонента Sensor также может использоваться *почтовый сенсор* – сервер или виртуальная машина, на которой установлено приложение "Лаборатории Касперского" Kaspersky Secure Mail Gateway (далее также "KSMG") или Kaspersky Security для Linux Mail Server (далее также "KLMS").

- Компонент Central Node проверяет файлы и объекты с помощью антивирусных баз, баз YARA-правил, создаваемых пользователями Kaspersky Anti Targeted Attack, при необходимости отправляет файлы и объекты на проверку компоненту Sandbox.

- Компонент Sandbox анализирует поведение объектов в виртуальных операционных системах для выявления вредоносной активности и признаков целевых атак на IT-инфраструктуру организации и отправляет данные о результатах проверки на сервер Central Node.

При обнаружении угроз сервер Central Node записывает информацию о них в базу обнаружений. Вы можете просмотреть таблицу обнаружений в разделе **Обнаружения** веб-интерфейса приложения или сформировав отчет об обнаружениях.

Информация об обнаружениях также может публиковаться в SIEM-систему, которая используется в вашей организации, и во внешние системы. Информация об обнаружениях компонента Sandbox может публиковаться в локальную репутационную базу Kaspersky Private Security Network.

Принцип работы Kaspersky Endpoint Detection and Response

Kaspersky Endpoint Detection and Response включает в себя следующие компоненты:

- Central Node.
- Endpoint Agent.

  Компонент может быть представлен приложениями Kaspersky Endpoint Agent для Windows, Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux, Kaspersky Endpoint Security для Mac.
- Sandbox.

  Опциональный компонент.

  > В качестве прокси-сервера для соединений, исходящих от компонента Endpoint Agent, может использоваться компонент Sensor (см. раздел "Настройка перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor" на стр. 177).

Компоненты Endpoint Agent и Central Node взаимодействуют между собой по следующему принципу:

Одно из приложений, представляющих компонент Endpoint Agent, устанавливается на отдельных компьютерах, входящих в IT-инфраструктуру организации, и осуществляет постоянное наблюдение за процессами, открытыми сетевыми соединениями и изменяемыми файлами. Данные наблюдения отправляются на сервер с компонентом Central Node. На основе этих данных формируются события.

- Kaspersky Endpoint Agent для Windows и Kaspersky Endpoint Security для Windows передают на сервер Central Node данные о следующих событиях:
  - **Запущен процесс**;
  - **Загружен модуль**;
  - **Удаленное соединение**;
  - **Правило запрета**;
  - **Заблокирован документ**;
  - **Изменен файл**;
  - **Журнал событий ОС**;
  - **Изменение в реестре**;
  - **Прослушан порт**;
  - **Загружен драйвер**;

    - **Интерпретированный запуск файла**;
    - **Интерактивный ввод команд в консоли**.
- Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Mac передает на сервер Central Node данные о следующих событиях:
    - **Запущен процесс**;
    - **Изменен файл**;
    - **Журнал событий ОС**.

Приложение Kaspersky Endpoint Agent для Windows может интегрироваться с приложениями защиты рабочих станций (Endpoint Protection Platform (далее также "EPP")) (см. раздел "Совместимость версий Kaspersky Endpoint Agent для Windows с приложениями EPP" на стр. 30):

- Kaspersky Endpoint Security для Windows.
- Kaspersky Security для Windows Server.
- Kaspersky Security для виртуальных сред Легкий Агент для Windows.

Совместимость версий приложения Kaspersky Endpoint Agent для Windows с приложениями EPP см. в разделе Совместимость версий Kaspersky Endpoint Agent для Windows с приложениями EPP (на стр. 30).

В этом случае приложение Kaspersky Endpoint Agent также передает на сервер Central Node данные об угрозах, обнаруженных приложениями EPP, и о результатах обработки угроз этими приложениями.

Приложения EPP, Kaspersky Endpoint Agent и сервер Central Node взаимодействуют между собой по следующему принципу:

- Приложения EPP передают Kaspersky Endpoint Agent данные об обнаруженных угрозах и о результате обработки угроз.

  Приложение Kaspersky Endpoint Security для Windows также может передавать Kaspersky Endpoint Agent для Windows данные об отправке сторонним приложением с поддержкой Antimalware Scan Interface (далее также "AMSI") объектов (например, скриптов PowerShell) в Kaspersky Endpoint Security для Windows для дополнительной проверки.
- Приложение Kaspersky Endpoint Agent передает данные наблюдения за процессами, открытыми сетевыми соединениями и изменяемыми файлами, а также данные, полученные от приложений EPP, на сервер Central Node.

  Сервер Central Node обрабатывает полученные данные и отображает в веб-интерфейсе приложения соответствующие события.

  В результате обработки данных приложений EPP формируются события **Обнаружение**, **Результат обработки обнаружения**, **AMSI-проверка** (при интеграции Kaspersky Endpoint Agent для Windows с Kaspersky Endpoint Security для Windows).

  События, поступающие на сервер Central Node, отмечаются правилами ТАА (IOA). В результате разметки для событий, требующих внимания пользователя, могут формироваться обнаружения. При наличии компонента Sandbox вы можете также включить автоматическую отправку файлов с хостов Kaspersky Endpoint Agent на проверку компоненту Sandbox в соответствии с правилами ТАА (IOA) "Лаборатории Касперского" (см. раздел "Автоматическая отправка файлов с хостов с компонентом Endpoint Agent на проверку в Sandbox по правилам ТАА (IOA) "Лаборатории Касперского"" на стр. 451).

При интеграции сервера Central Node с Kaspersky Endpoint Agent для Windows и Kaspersky Endpoint Security для Windows вы можете осуществлять следующие меры по реагированию на обнаруженные угрозы:

- Работать с файлами и приложениями путем выполнения задач **Завершить процесс**, **Собрать форензику**, **Запустить YARA-проверку**, **Выполнить приложение**, **Получить файл**, **Удалить файл**, **Поместить файл на карантин**, **Восстановить файл из карантина**, **Управление службами**, **Получить образ диска**, **Получить дамп памяти** на хостах.
- Настраивать политики запрета запуска файлов и процессов на выбранных хостах.
- Изолировать отдельные хосты от сети (см. раздел "Сетевая изоляция хостов с компонентом Endpoint Agent" на стр. 448).
- Работать с правилами TAA (IOA) для классификации и анализа событий.
- Работать с файлами открытого стандарта описания индикаторов компрометации OpenIOC (IOC-файлы) для поиска признаков целевых атак, зараженных и возможно зараженных объектов на хостах и в базе обнаружений.
- Выполнять действия по реагированию с помощью интерфейса API (см. раздел "API для управления действиями по реагированию на угрозы" на стр. 645).

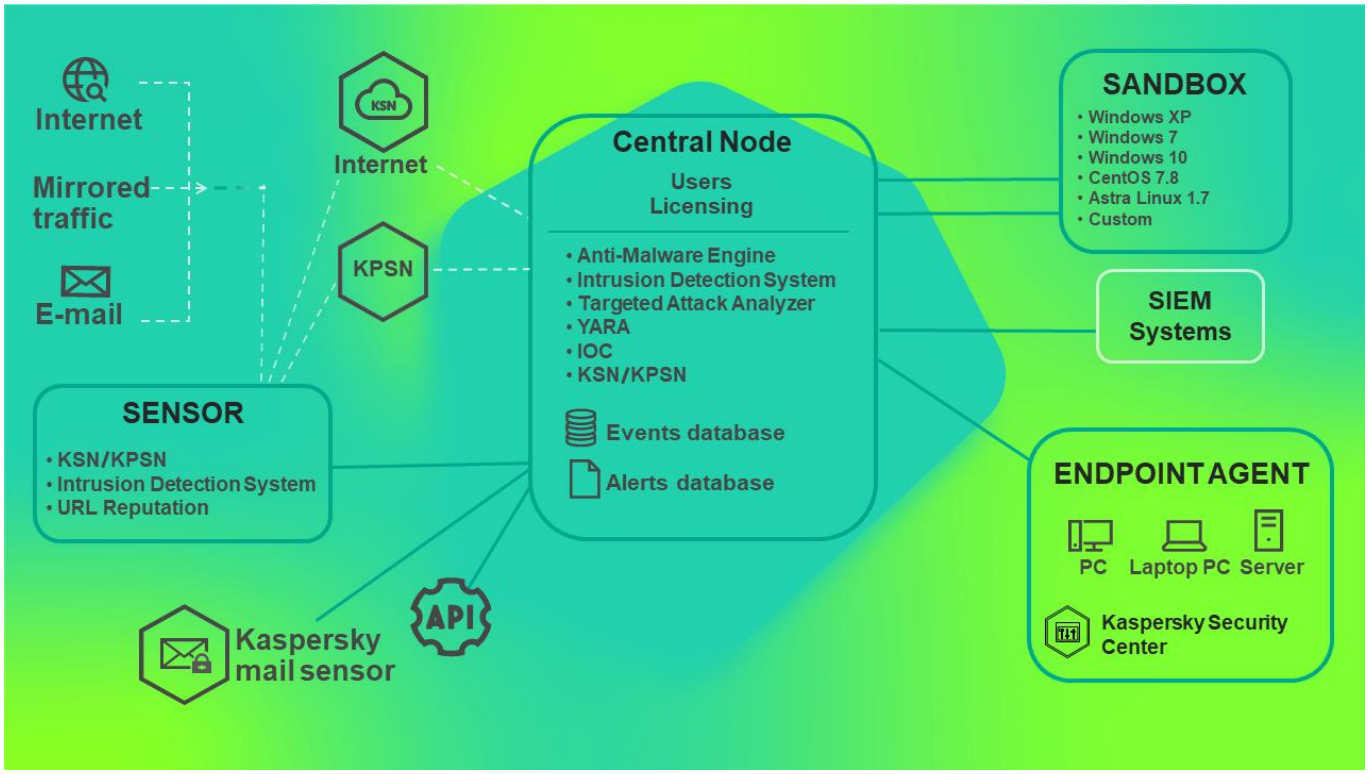
При интеграции сервера Central Node с Kaspersky Endpoint Security 11.4 для Linux и Kaspersky Endpoint Security для Mac вы можете осуществлять следующие меры по реагированию на обнаруженные угрозы:

- Работать с файлами и приложениями путем выполнения задач **Получить файл**, **Выполнить приложение**.
- Работать с правилами TAA (IOA) для классификации и анализа событий.
- Выполнять следующие действия по реагированию с помощью интерфейса API: управление задачей запуска приложений (см. раздел "Управление задачей запуска приложения" на стр. 662).

При интеграции сервера Central Node с Kaspersky Endpoint Security 12 для Linux вы можете осуществлять следующие меры по реагированию на обнаруженные угрозы:

- Работать с файлами и приложениями путем выполнения задач **Получить файл**, **Выполнить приложение**, **Удалить файл**, **Завершить процесс**.
- Изолировать отдельные хосты от сети.
- Работать с файлами открытого стандарта описания индикаторов компрометации OpenIOC (IOC-файлы) для поиска признаков целевых атак, зараженных и возможно зараженных объектов на хостах и в базе обнаружений.
- Выполнять следующие действия по реагированию с помощью интерфейса API: управление сетевой изоляцией хостов (на стр. 649), управление задачей запуска приложений (см. раздел "Управление задачей запуска приложения" на стр. 662).

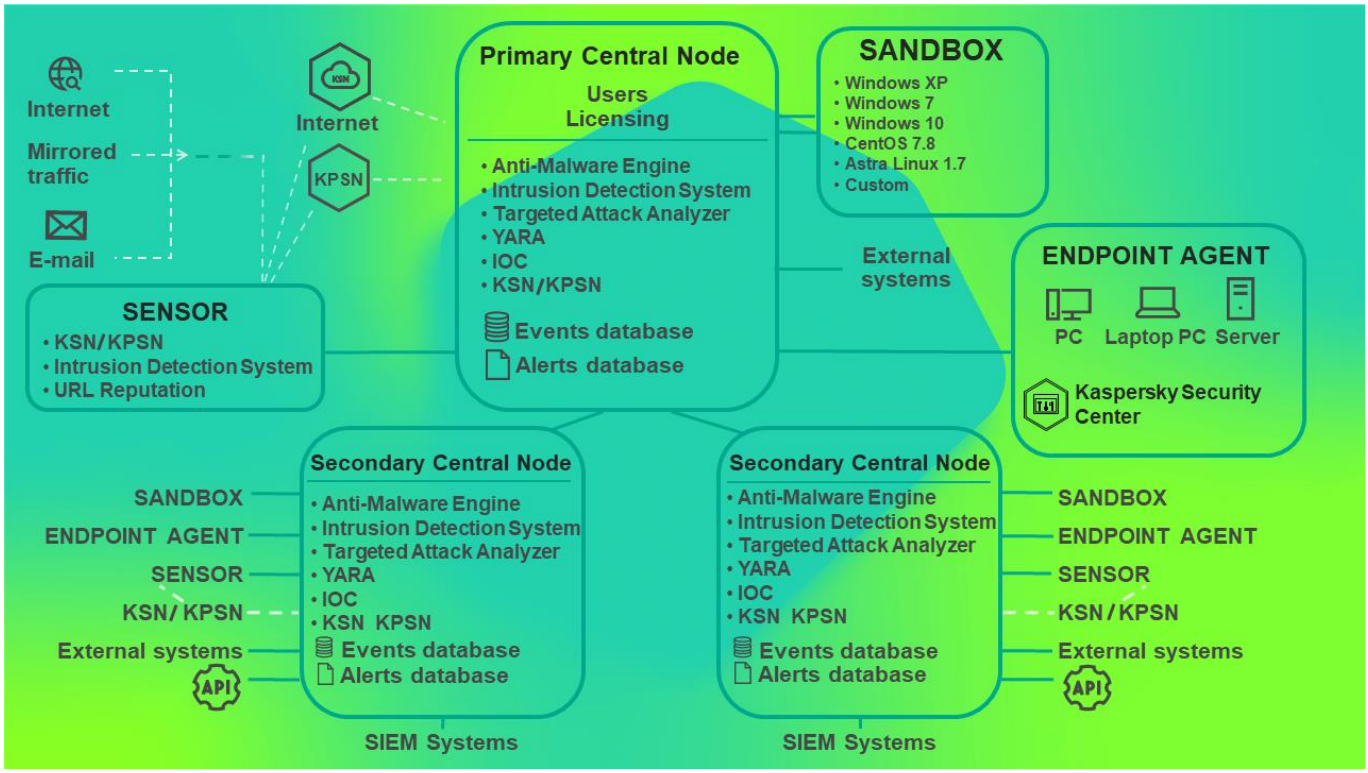
Принцип работы Kaspersky Anti Targeted Attack Platform показан на рисунке ниже.



Вы можете настраивать параметры каждого компонента Central Node отдельно или управлять несколькими компонентами централизованно в режиме распределенного решения.

Распределенное решение представляет собой двухуровневую иерархию серверов Central Node. В этой структуре выделяется главный сервер управления – Primary Central Node (PCN) и подчиненные серверы – Secondary Central Node (SCN).

Принцип работы Kaspersky Anti Targeted Attack Platform в режиме распределенного решения показан на рисунке ниже.



Распределенное решение и мультитенантность

Вы можете настраивать параметры каждого компонента Central Node отдельно или управлять несколькими компонентами централизованно в режиме распределенного решения.

Распределенное решение представляет собой двухуровневую иерархию серверов с установленными компонентами Central Node. В этой структуре выделяется главный сервер управления – *Primary Central Node (PCN)* и подчиненные серверы – *Secondary Central Node (SCN)*. Для взаимодействия серверов требуется подключить SCN к PCN.

Если вы развернули компонент Central Node в виде кластера, весь кластер выполняет роль PCN или SCN.

PCN и SCN осуществляют проверку файлов и объектов с помощью тех же технологий, что и компонент Central Node (на стр. 67), управляемый отдельно.

В распределенном решении вы можете централизованно управлять следующими функциональными областями приложения:

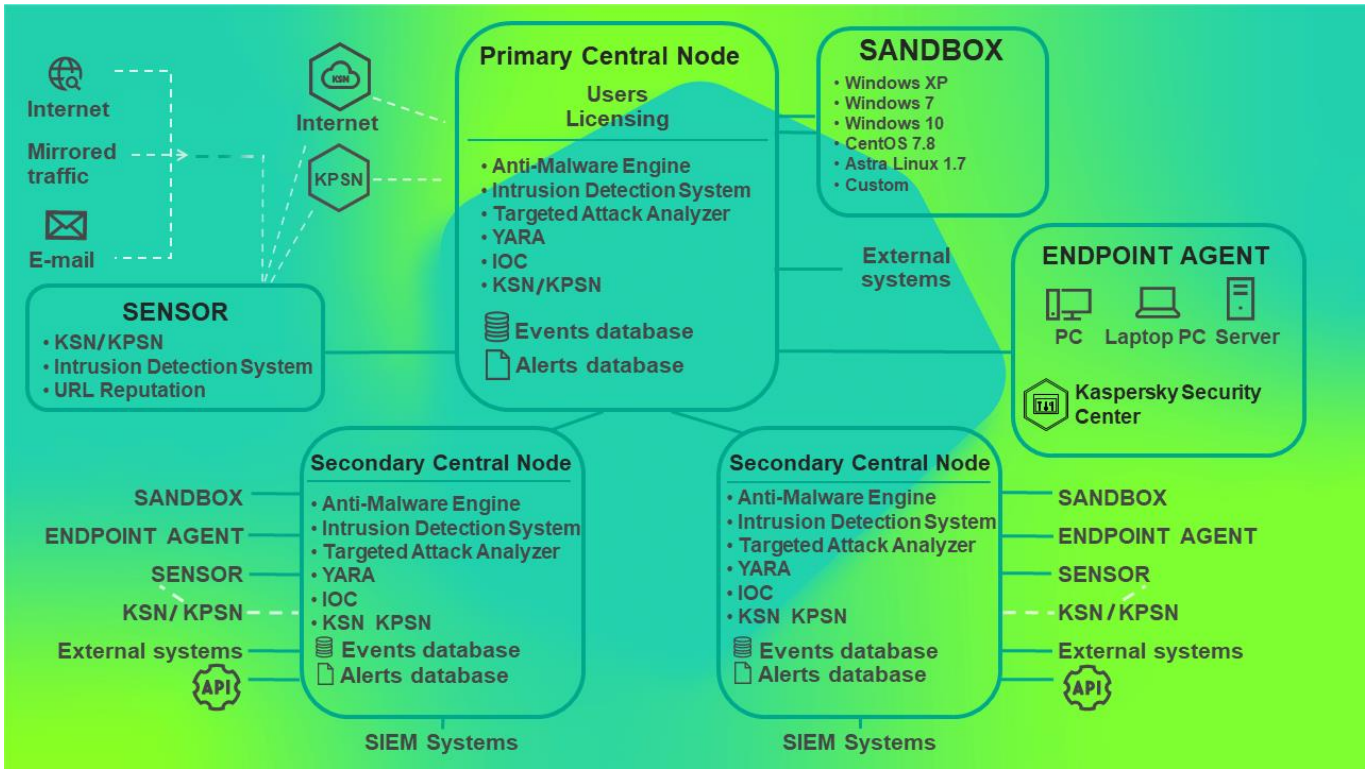
- Пользователи.
- Обнаружения.
- Поиск угроз.
- Задачи.
- Политики.
- Пользовательские правила.
- Хранилище.
- Endpoint Agents, в том числе сетевая изоляция хостов.
- Отчеты.

Если вы поддерживаете несколько организаций или филиалов одной организации, вы можете использовать приложение в режиме мультитенантности.

Мультитенантность - это режим работы, при котором приложение используется для защиты инфраструктуры нескольких организаций или филиалов одной организации (далее также "тенантов") одновременно. Вы можете установить Kaspersky Anti Targeted Attack Platform на один или несколько серверов Central Node для каждого тенанта. Каждый тенант может работать с приложением независимо от других тенантов. Поставщик услуг может работать с данными нескольких тенантов.

Количество одновременных сеансов работы с приложением под одной учетной записью ограничено одним IP-адресом. При попытке входа в приложение под этим же именем пользователя с другого IP-адреса первый сеанс работы с приложением завершается.

Если вы используете режим распределенного решения и мультитенантности, ограничение действует для каждого сервера PCN и SCN независимо друг от друга.



Вы можете использовать режим распределенного решения и мультитенантности в следующих случаях:

- для защиты более 10 000 хостов тенанта;
- для централизованного управления приложением в разных подразделениях тенантов;
- для централизованного управления приложением на серверах нескольких тенантов.

При переключении приложения в режим распределенного решения и мультитенантности на серверах с ролью SCN все ранее добавленные лицензионные ключи (см. раздел "О ключе" на стр. 158) удаляются. Каждый подключенный SCN получает ключ от PCN. Если для PCN используется полная функциональность приложения (ключ KATA и KEDR), а для SCN неполная (только ключ KATA или только ключ KEDR), в связи с увеличением объема данных возможно превышение допустимого уровня нагрузки на сервер SCN. Если для PCN используется неполная функциональность приложения (только ключ KATA или только ключ KEDR), а для SCN полная (ключ KATA и KEDR), часть функционала приложения будет недоступна.

Управление лицензионными ключами будет доступно только на PCN.

Вы можете развернуть приложение в режиме распределенного решения и мультитенантности по следующим сценариям:

- Установить компонент Central Node на новых серверах и назначить этим серверам роли PCN и SCN.
- Назначить роли PCN и SCN серверам с ранее установленным компонентом Central Node.

В этом случае вам требуется обновить компонент Central Node до версии 6.0.

Перед переключением серверов с установленными компонентами Central Node в режим распределенного решения рекомендуется ознакомиться с изменениями (см. раздел "Изменения в параметрах приложения при переходе в режим распределенного решения и мультитенантности" на стр. 78), которые произойдут в системе после смены режима работы. Назначение серверу роли PCN является необратимым.

В этом разделе

Сценарий перехода в режим распределенного решения и мультитенантности 77

Изменения в параметрах приложения при переходе в режим распределенного решения и мультитенантности 78

Назначение серверу роли PCN 80

Назначение серверу роли SCN 81

Обработка запросов на подключение SCN к PCN 82

Просмотр информации о тенантах, серверах PCN и SCN 83

Добавление тенанта на сервере PCN 83

Удаление тенанта на сервере PCN 84

Изменение названия тенанта на сервере PCN 84

Отключение SCN от PCN 85

Изменения в параметрах приложения при отключении SCN от PCN 86

Вывод сервера SCN из эксплуатации 87

Сценарий перехода в режим распределенного решения и мультитенантности

Переход приложения в режим распределенного решения и мультитенантности содержит следующие этапы:

a. **Установка компонентов Central Node (см. раздел "Установка и первоначальная настройка приложения" на стр. 110)**

b. **Назначение одному из серверов роли PCN (см. раздел "Назначение серверу роли PCN" на стр. 80)**

c. **Назначение остальным серверам роли SCN и отправка запросов на подключение к PCN (см. раздел "Назначение серверу роли SCN" на стр. 81)**

d. **Обработка запроса на подключение SCN к PCN (см. раздел "Обработка запросов на подключение SCN к PCN" на стр. 82)**

Изменения в параметрах приложения при переходе в режим распределенного решения и мультитенантности

Изменения в параметрах приложения при переключении в режим распределенного решения и мультитенантности приведены в таблице ниже.

Таблица 13. Изменения в параметрах приложения при переключении в режим распределенного решения и мультитенантности

Функциональная область	PCN	SCN
Пользователи	Пользователи и назначенные им роли сохраняются. Дополнительно пользователям PCN выдаются права на работу с PCN и всеми подключенными SCN.	Удаляются все пользователи, кроме пользователя, созданного в момент развертывания Central Node. После этого SCN запрашивает у PCN список пользователей и на основе этого списка создает локальных пользователей с такими же параметрами: • имя; • пароль; • роль; • статус. Пользователи, не имеющие прав на доступ к SCN, не отображаются в списке пользователей.
Обнаружения	В базу PCN добавляется информация об обнаружениях со всех подключенных SCN.	В информации об уже имеющихся обнаружениях перестает отображаться имя пользователя. Данные о пользователях удаляются из истории операций с обнаружением.
Мониторинг	На закладке **Обнаружения** появляется возможность выбрать SCN, информация о которых должна быть отражена на виджете. На закладке **Работоспособность системы** появляется статус соединения PCN с подключенными SCN.	На закладке **Работоспособность системы** появляется статус соединения с PCN.
Задачи	Задачи, созданные на сервере Central Node до назначения ему роли PCN, а также задачи, создаваемые на PCN после перехода в режим распределенного решения,	Отображаются задачи, созданные на PCN, а также задачи, созданные на этом SCN. Изменение параметров задач, созданных на PCN, недоступно.

	распространяются на все подключенные SCN. В списке задач также отображаются задачи, созданные на SCN. Изменение параметров этих задач на PCN недоступно.	
Отчеты	Шаблоны и отчеты, созданные до переключения в режим распределенного решения, сохраняются. В таблице отчетов появляется столбец **Серверы** с информацией о SCN, к которому относится обнаружение. После переключения в режим распределенного решения отображаются только отчеты, созданные на PCN.	Шаблоны и отчеты, созданные до переключения в режим распределенного решения, сохраняются. Информация о пользователе, создавшем отчет, сохраняется, если на PCN есть пользователь с таким же идентификатором (guid). В остальных случаях информация о пользователе удаляется. После переключения в режим распределенного решения отображаются только отчеты, созданные на SCN.
Политики	Политики, созданные на сервере Central Node до назначения ему роли PCN, а также политики, создаваемые на PCN после перехода в режим распределенного решения, распространяются на все подключенные SCN. В списке политик также отображаются политики, созданные на SCN. Изменение параметров этих политик на PCN недоступно.	Отображаются политики, созданные на PCN, а также политики, созданные на этом SCN. Изменение параметров политик, созданных на PCN, недоступно.
Хранилище	Все файлы и метаданные, которые хранились на PCN до перехода в режим распределенного решения, сохраняются. В столбце **Central Node** для них отображается имя PCN. На PCN также сохраняется содержимое Хранилища всех подключенных SCN.	Все файлы и метаданные, которые хранились на SCN до перехода в режим распределенного решения, сохраняются.
Исключение ТАА (IOA)	Изменений нет.	Изменений нет.
Статус VIP	Изменений нет.	Изменений нет.
Правила уведомлений	Изменений нет.	Изменений нет.

Интеграция с почтовыми сенсорами	Изменений нет.	Изменений нет.
Поиск угроз	При поиске угроз по базе событий PCN отправляет запрос на все подключенные SCN. В результате обработки поискового запроса отображается список событий PCN и SCN выбранного тенанта.	Изменений нет.
Пользовательские правила - TAA	IOC-файлы, добавленные на сервере Central Node до назначения ему роли PCN, распространяются на PCN. Правила TAA (IOA), добавленные на сервере Central Node до назначения ему роли PCN, распространяются на PCN.	Отображаются IOC-файлы и правила TAA (IOA), добавляемые на PCN, а также IOC-файлы и правила TAA (IOA), добавляемые на этом SCN до и после перехода в режим распределенного решения.
Резервное копирование приложения	Резервное копирование приложения доступно только на PCN, к которому не подключены SCN. Чтобы сделать резервное копирование приложения на PCN, необходимо отключить все SCN от этого PCN.	Резервное копирование приложения на SCN недоступно. Чтобы сделать резервное копирование приложения на SCN, необходимо отключить этот сервер от PCN, переведя его в режим отдельного сервера.

Назначение серверу роли PCN

Назначение серверу роли PCN необратимо. После изменения роли сервера на PCN вы не сможете изменить роль этого сервера на SCN или отдельный сервер. Если вы захотите изменить роль этого сервера снова, вам потребуется переустановить приложение.

► *Чтобы назначить серверу роль PCN:*

1. Войдите в веб-интерфейс приложения под учетной записью администратора.

   Вам нужно войти в веб-интерфейс того сервера, которому вы хотите назначить роль PCN.
2. Выберите раздел **Режим работы**.
3. Нажмите на кнопку **Распределенное решение**.
4. В раскрывающемся списке **Роль сервера** выберите **Primary Central Node**.
5. В поле **Название тенанта** введите название тенанта, к которому относится этот сервер Central Node.

6. Нажмите на кнопку **Назначить роль PCN**.

   Откроется окно подтверждения действия.

   После подтверждения действия вам потребуется снова войти в веб-интерфейс приложения.

7. Нажмите на кнопку **Да**.

Серверу будет назначена роль PCN и присвоено название тенанта.

После того, как вы снова войдете в веб-интерфейс приложения под учетной записью администратора, в окне веб-интерфейса приложения в разделе **Режим работы** отобразится следующая информация:

- **Текущий режим** – Распределенное решение.
- **Роль сервера** – Primary Central Node.
- **Отпечаток сертификата** – отпечаток сертификата сервера, необходимый для проверки подлинности при установке соединения с SCN.
- **Тенанты** – информация о тенантах, к которым относится этот сервер, и все подключенные серверы SCN:
  - **IP** – Primary Central Node для этого сервера и IP-адреса серверов SCN (после их подключения).
  - **Сервер** – имя этого сервера и имена серверов SCN (после их подключения).

    Это имя не связано с именем хоста, на котором установлено приложение. Вы можете его изменить.
  - **Отпечаток сертификата** – пустое значение для этого сервера и отпечатки сертификатов серверов SCN (после их подключения).
  - **Состояние** – состояние подключения серверов SCN (после их подключения), а также количество серверов, подключенных к тенантам.
- Таблица **Серверы, ожидающие авторизации** с информацией о подключенных SCN (см. раздел "Просмотр информации о тенантах, серверах PCN и SCN" на стр. 83).

Назначение серверу роли SCN

► *Чтобы назначить серверу роль SCN:*

1. Войдите в веб-интерфейс приложения под учетной записью администратора.

   Вам нужно войти в веб-интерфейс того сервера, которому вы хотите назначить роль SCN.
2. В окне веб-интерфейса приложения выберите раздел **Режим работы**.
3. Нажмите на кнопку **Распределенное решение**.
4. В раскрывающемся списке **Роль сервера** выберите **Secondary Central Node**.
5. В поле **IP-адрес сервера PCN** укажите IP-адрес сервера с ролью PCN, к которому вы хотите подключить SCN.
6. Нажмите на кнопку **Получить отпечаток сертификата**.

   В рабочей области отобразится отпечаток сертификата сервера с ролью PCN.

7. Свяжитесь с администратором PCN и сравните полученный отпечаток сертификата с отпечатком, указанным на PCN в разделе **Режим работы** в поле **Отпечаток сертификата**.
8. Если отпечатки сертификата на SCN и PCN совпадают, нажмите на кнопку **Отправить запрос на подключение**.

   Откроется окно подтверждения действия.
9. Нажмите на кнопку **Да**.

Серверу будет назначена роль SCN после того, как администратор PCN примет запрос на подключение. Сервер SCN будет относиться к тому тенанту, который укажет администратор PCN.

Обработка запросов на подключение SCN к PCN

► *Чтобы обработать запрос на подключение SCN к PCN:*

1. Войдите в веб-интерфейс приложения под учетной записью администратора.

   Вам нужно войти в веб-интерфейс того сервера PCN, на котором вы хотите обработать запросы на подключение от других серверов.
2. В окне веб-интерфейса приложения выберите раздел **Режим работы**.

   В рабочей области отобразится таблица **Серверы, ожидающие авторизации**.
3. Свяжитесь с администратором SCN, отправившим запрос на подключение, и проверьте отпечаток сертификата в таблице **Серверы, ожидающие авторизации**. Он должен совпадать с отпечатком, отображаемым на SCN в разделе **Режим работы** в поле **Отпечаток сертификата из запроса**.
4. Если отпечатки сертификата на PCN и SCN совпадают, выполните одно из следующих действий:
   - Если вы хотите отклонить запрос на подключение от SCN, нажмите на кнопку **Отклонить**.
   - Если вы хотите принять запрос на подключение от SCN, выполните следующие действия:
     1. Нажмите на кнопку **Принять**.

        Откроется окно **Принять запрос на подключение**.
     2. В списке **Тенант** выберите тенант, которому вы хотите назначить этот сервер SCN. Список формируется из тенантов, добавленных ранее (см. раздел "Добавление тенанта на сервере PCN" на стр. 83).
     3. Нажмите на кнопку **Принять**.

> Не рекомендуется принимать запросы на подключение при несовпадении отпечатков сертификата. Убедитесь в правильности введенных данных.

На время подключения сервера SCN к PCN все кнопки в окне **Режим работы** блокируются. После того, как подключение завершится, кнопки будут разблокированы.

Если вы отклонили запрос на подключение, SCN продолжит работу в режиме отдельного сервера Central Node.

Просмотр информации о тенантах, серверах PCN и SCN

В веб-интерфейсе сервера PCN вы можете просмотреть информацию об этом сервере, а также о всех серверах SCN, которые к нему подключены.

► *Чтобы просмотреть информацию о серверах PCN и SCN в режиме мультитенантности:*

1. Войдите в веб-интерфейс приложения под учетной записью администратора.

   Вам нужно войти в веб-интерфейс сервера PCN.

2. В окне веб-интерфейса приложения выберите раздел **Режим работы**.

В рабочей области отобразится следующая информация о серверах:

- **Текущий режим** – Распределенное решение.
- **Роль сервера** – Primary Central Node.
- **Отпечаток сертификата** – отпечаток сертификата сервера PCN.
- **Тенанты** – информация о тенантах, к которым относятся этот сервер, а также все серверы SCN, подключенные к PCN.
  - **IP** – Primary Central Node для сервера PCN и IP-адреса серверов SCN, подключенных к PCN.
  - **Сервер** – имя этого сервера и имена серверов SCN, подключенных к PCN.

    Это имя не связано с именем хоста, на котором установлено приложение. Вы можете его изменить.
  - **Отпечаток сертификата** – пустое значение для сервера PCN и отпечатки сертификатов серверов SCN, которые ожидают подключения к PCN.
  - **Состояние** – состояние подключения серверов SCN, а также количество серверов, подключенных к тенанту.
- Таблица **Серверы, ожидающие авторизации** со следующей информацией:
  - **IP** – IP-адрес или доменное имя сервера SCN.
  - **Сервер** – имя сервера SCN, которое отображается в веб-интерфейсе приложения.

    Это имя не связано с именем хоста, на котором установлено приложение. Вы можете его изменить.
  - **Отпечаток сертификата** – отпечаток сертификата сервера SCN, передаваемый на PCN вместе с запросом на подключение.
  - **Состояние** – статус подключения SCN к PCN.

Добавление тенанта на сервере PCN

► *Чтобы добавить тенант в веб-интерфейсе сервера PCN:*

1. Войдите в веб-интерфейс приложения под учетной записью администратора.

   Вам нужно войти в веб-интерфейс того сервера PCN, для которого вы хотите добавить тенант.

2. В окне веб-интерфейса приложения выберите раздел **Режим работы**.

3. В правой части рабочей области **Тенанты** нажмите на кнопку **Добавить**.
4. В поле **Имя** введите название тенанта, который вы хотите добавить.
5. Нажмите на кнопку **Добавить**.

Тенант будет добавлен и отобразится в списке.

Удаление тенанта на сервере PCN

► *Чтобы удалить тенант в веб-интерфейсе сервера PCN:*

1. Войдите в веб-интерфейс приложения под учетной записью администратора.

   Вам нужно войти в веб-интерфейс сервера PCN, для которого вы хотите удалить тенант.
2. В окне веб-интерфейса приложения выберите раздел **Режим работы**.
3. В рабочей области **Тенанты** выберите тенант, который вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

   Действие необратимо. Все глобальные объекты, а также отчеты и шаблоны отчетов, связанные с этим тенантом, будут потеряны.
5. Нажмите на кнопку **Да**.

Тенант будет удален.

Изменение названия тенанта на сервере PCN

► *Чтобы изменить название тенанта в веб-интерфейсе сервера PCN:*

1. Войдите в веб-интерфейс приложения под учетной записью администратора.

   Вам нужно войти в веб-интерфейс сервера PCN, для которого вы хотите изменить название тенанта.
2. В окне веб-интерфейса приложения выберите раздел **Режим работы**.
3. В списке **Тенанты** нажмите на значок справа от названия тенанта, которое вы хотите изменить.

   Откроется окно изменения названия тенанта.
4. В поле **Имя** измените название тенанта.
5. Нажмите на кнопку **Сохранить**.

Название тенанта будет изменено.

Отключение SCN от PCN

Отключение SCN от PCN может быть односторонним.

Если вы отключите SCN через веб-интерфейс SCN, то изменения в параметрах будут применены только на SCN. На PCN по-прежнему будет отображаться информация об этом сервере.

Если вы отключите SCN через веб-интерфейс PCN, то информация об этом сервере будет удалена на PCN. Однако сервер с ролью SCN будет пытаться подключиться к PCN для синхронизации параметров.

Для двустороннего отключения необходимо выполнить обе инструкции, приведенные ниже. В этом случае SCN продолжит работать как отдельный сервер Central Node, на PCN будет отображаться информация об отключенном SCN.

Администратор Kaspersky Anti Targeted Attack Platform несет ответственность за сохранность конфиденциальных данных на серверах PCN, SCN и Central Node. Если вы планируете передать сервер SCN от одного тенанта другому, необходимо удалить все данные, оставшиеся на сервере после использования Kaspersky Anti Targeted Attack Platform и переустановить Kaspersky Anti Targeted Attack Platform перед передачей сервера другому тенанту.

► *Чтобы отключить SCN от PCN через веб-интерфейс PCN:*

1. Войдите в веб-интерфейс приложения под учетной записью администратора.

   Войдите в веб-интерфейс того сервера PCN, от которого вы хотите отключить SCN.
2. В окне веб-интерфейса приложения выберите раздел **Режим работы**.
3. В списке серверов выберите SCN, который вы хотите отключить.
4. Нажмите на кнопку **Отключить**.

   Откроется окно подтверждения действия.
5. Нажмите на кнопку **Да**.

SCN будет пытаться подключиться к PCN для синхронизации параметров.

► *Чтобы отключить SCN от PCN через веб-интерфейс SCN:*

1. Войдите в веб-интерфейс приложения под учетной записью администратора.

   Войдите в веб-интерфейс того сервера SCN, который вы хотите отключить от PCN.
2. В окне веб-интерфейса приложения выберите раздел **Режим работы**.
3. Нажмите на кнопку **Отключить**.

   Откроется окно подтверждения действия.
4. Нажмите на кнопку **Да**.

SCN будет отключен от PCN и продолжит работать как отдельный сервер Central Node.

Изменения в параметрах приложения при отключении SCN от PCN

Изменения в параметрах приложения после отключения SCN от PCN представлены в таблице ниже.

Таблица 14. Изменения параметров приложения после отключения SCN от PCN

Функциональная область	PCN	SCN
Пользователи	Отключенный SCN не исключается из списка серверов, на которые распространяются права пользователей. Информация об изменении учетной записи пользователя, имеющего права на отключенный SCN, не передается на SCN.	Учетные записи пользователей, полученные с PCN, не удаляются. Появляется возможность создания новых учетных записей пользователей, а также отключения и смены пароля существующих учетных записей.
Обнаружения	Информация об обнаружениях на отключенном SCN удаляется.	История операций и вся информация об обнаружениях сохраняется.
Задачи	Задачи, созданные на отключенном SCN, удаляются.	Задачи, созданные на PCN, удаляются. Информация о пользователях, создавших задачи на SCN, сохраняется.
Отчеты	Все созданные ранее отчеты об отключенном SCN, а также возможность фильтровать список отчетов по этому серверу, сохраняются.	Шаблоны и отчеты не изменяются.
Политики	Политики, созданные на отключенном SCN, удаляются.	Политики, созданные на PCN, удаляются. Информация о пользователях, создавших политики на SCN, сохраняется.
Хранилище	Из Хранилища удаляются все объекты, относящиеся к отключенному SCN.	Все объекты в Хранилище сохраняются. В информации об объектах, полученных в рамках задач, созданных на PCN, перестает работать ссылка на задачу.
Исключение ТАА (IOA)	Изменений нет.	Изменений нет.
Статус VIP	Изменений нет.	Изменений нет.
Правила уведомлений	Изменений нет.	Изменений нет.
Интеграция с почтовыми сенсорами	Изменений нет.	Изменений нет.

Поиск угроз	В результате обработки поискового запроса события, связанные с отключенным SCN, не отображаются.	Изменений нет.
Пользовательские правила - TAA и IOC	IOC- и правила TAA (IOA) отключенного SCN удаляются.	IOC- и правила TAA (IOA), созданные на PCN, удаляются.
Резервное копирование приложения	Резервное копирование приложения остается недоступным.	Резервное копирование приложения становится доступным.

Вывод сервера SCN из эксплуатации

Если вы не планируете в дальнейшем использовать сервер SCN, вы можете вывести сервер SCN из эксплуатации приложением, удалив его на PCN.

Администратор Kaspersky Anti Targeted Attack Platform несет ответственность за сохранность конфиденциальных данных на серверах PCN, SCN и Central Node. Если вы планируете передать сервер SCN от одного тенанта другому, необходимо удалить все данные, оставшиеся на сервере после использования Kaspersky Anti Targeted Attack Platform и переустановить Kaspersky Anti Targeted Attack Platform перед передачей сервера другому тенанту.

Вывод сервера SCN из эксплуатации приложением состоит из следующих этапов:

a. **Удаление всех данных на SCN**

b. **Отключение SCN от PCN через веб-интерфейс PCN (см. раздел "Отключение SCN от PCN" на стр. 85)**

c. **Отключение SCN от PCN через веб-интерфейс SCN (см. раздел "Отключение SCN от PCN" на стр. 85)**

d. **Удаление SCN через веб-интерфейс PCN**

► *Чтобы удалить SCN через веб-интерфейс PCN:*

1. Войдите в веб-интерфейс приложения под учетной записью администратора.

   Войдите в веб-интерфейс того сервера PCN, на котором вы хотите удалить SCN.
2. В окне веб-интерфейса приложения выберите раздел **Режим работы**.
3. В списке серверов выберите SCN, который вы хотите удалить.
4. Нажмите на кнопку **Удалить**.
5. В окне подтверждения нажмите на кнопку **Да**.

SCN будет удален. На PCN не будут отображаться сведения об удаленном SCN.

Руководство по масштабированию

Для достижения и сохранения оптимальной производительности при различных условиях работы приложения требуется учитывать количество устройств в сети, топологию сети и необходимую вам функциональность приложения.

Выбор оптимальной конфигурации приложения состоит из следующих этапов:

a. **Выбор типовой схемы развертывания (см. раздел "Типовые схемы развертывания и установки компонентов приложения" на стр. 88)**

b. **Расчет аппаратных требований с помощью калькулятора масштабирования (см. раздел "Калькулятор масштабирования" на стр. 94)**

В этом разделе

Типовые схемы развертывания и установки компонентов приложения 88

Калькулятор масштабирования 94

Типовые схемы развертывания и установки компонентов приложения

Схема развертывания и установки компонентов приложения определяется планируемой нагрузкой на серверы приложения.

Компонент Endpoint Agent устанавливается на любых компьютерах, которые входят в IT-инфраструктуру организации и работают под управлением операционной системы Windows. На компьютерах с компонентом Endpoint Agent необходимо разрешить исходящее соединение с сервером с компонентом Central Node напрямую, без использования прокси-сервера.

Вы можете установить один или несколько компонентов Central Node. При установке нескольких компонентов Central Node вы можете использовать их независимо друг от друга или объединить для централизованного управления в режиме распределенного решения (см. раздел "Распределенное решение и мультитенантность" на стр. 75).

Выбор схемы развертывания зависит от используемой функциональности приложения (см. раздел "Режимы работы приложения в соответствии с лицензией" на стр. 162). Все приведенные в данном руководстве схемы применимы также для развертывания приложения на виртуальной платформе.

Полная функциональность (KATA и KEDR)

При использовании функциональности KATA и KEDR вы можете проверять сетевой и почтовый трафик, а также данные на компьютерах локальной сети организации.

Если в организации используется более 5000 хостов с компонентом Endpoint Agent, не рекомендуется использовать компонент Central Node для обработки трафика.

Вы можете использовать компонент Sensor в качестве прокси-сервера для соединения хостов с компонентом Endpoint Agent и Central Node. Один компонент Sensor поддерживает подключение до 1000 хостов с с компонентом Endpoint Agent.

Критерии выбора схемы развертывания при использовании функциональности KATA и KEDR представлены в таблице ниже. Алгоритм выбора следующий:

1. В каждой строке таблицы выберите ячейку со значением критерия, соответствующим вашей IT-инфраструктуре.

   Если в строке две ячейки с одинаковым значением, необходимо выбрать левую ячейку.

2. Выберите самую правую колонку, в которой есть отмеченные ячейки.

Таблица 15. Выбор схемы развертывания при использовании функциональности KATA и KEDR

Критерий	Схема на два сервера (см. раздел "Схема развертывания на два сервера" на стр. 91)	Схема на три сервера (см. раздел "Схема развертывания на три сервера" на стр. 91)	Схема на четыре и более сервера (см. раздел "Схема развертывания на четыре и более сервера" на стр. 92)	Распределенное решение (см. раздел "Распределенное решение и мультитенантность" на стр. 75)
Сетевой и почтовый трафик не может быть принят на одном устройстве	Нет	Да	Да	Да
Количество хостов с компонентом Endpoint Agent	Нет	От 5000 до 10000	От 5000 до 10000	Более 10000
Пропускная способность канала связи	1 Гбит/с	От 1 до 2 Гбит/с	Более 2 Гбит/с	Более 2 Гбит/с
Количество удаленных инфраструктур, в которых требуется анализировать трафик	Нет	Одна	Две и более	Две и более
Мощности одного компонента Sandbox недостаточно для анализа всех объектов в приемлемые сроки	Нет	Нет	Да	Да

В режиме распределенного решения каждый из компонентов приложения должен отвечать аппаратным требованиям, указанным в калькуляторе масштабирования (см. раздел "Калькулятор масштабирования" на стр. 94).

Обработка сетевого, почтового и веб-трафика (KATA)

Функциональность KATA рекомендуется использовать, если в организации нет необходимости обрабатывать данные на компьютерах локальной сети организации. В этом случае обрабатывается только сетевой и почтовый трафик.

Критерии выбора схемы развертывания при использовании функциональности KATA представлены в таблице ниже. Алгоритм выбора следующий:

1. В каждой строке таблицы выберите ячейку со значением критерия, соответствующим вашей IT-инфраструктуре.

   Если в строке две ячейки с одинаковым значением, необходимо выбрать левую ячейку.

2. Выберите самую правую колонку, в которой есть отмеченные ячейки.

Таблица 16. Выбор схемы развертывания при использовании функциональности KATA

Критерий	Схема на два сервера (см. раздел "Схема развертывания на два сервера" на стр. 91)	Схема на три сервера (см. раздел "Схема развертывания на три сервера" на стр. 91)	Схема на четыре и более серверов (см. раздел "Схема развертывания на четыре и более сервера" на стр. 92)
Сетевой и почтовый трафик не может быть принят на одном устройстве	Нет	Да	Да
Пропускная способность канала связи	1 Гбит/с	От 1 до 2 Гбит/с	Более 2 Гбит/с
Количество удаленных инфраструктур, в которых требуется анализировать трафик	Нет	Одна	Две и более
Мощности одного компонента Sandbox недостаточно для анализа всех объектов в приемлемые сроки	Нет	Нет	Да

Обработка данных с компьютеров локальной сети организации (KEDR)

Функциональность KEDR рекомендуется использовать, если в организации нет необходимости обрабатывать трафик. В этом случае обрабатываются только данные на компьютерах локальной сети организации.

В зависимости от наличия в организации стороннего решения Sandbox вы можете использовать одну из следующих схем развертывания:

- схема без компонента Sandbox (см. раздел "Схема развертывания функциональности KEDR без компонента Sandbox" на стр. 93);
- схема с компонентом Sandbox (см. раздел "Схема развертывания функциональности KEDR с компонентом Sandbox" на стр. 92).

kaspersky

В этом разделе

Схема развертывания на два сервера 91
Схема развертывания на три сервера 91
Схема развертывания на четыре и более сервера 92
Схема развертывания функциональности KEDR с компонентом Sandbox 92
Схема развертывания функциональности KEDR без компонента Sandbox 93

Схема развертывания на два сервера

При использовании функциональности KATA и KEDR вы можете установить компонент Endpoint Agent на компьютерах локальной сети организации. При использовании функциональности KATA компонент Endpoint Agent не устанавливается.

При использовании этой схемы развертывания компоненты Central Node и Sensor устанавливаются на одном сервере или кластере. Этот сервер или кластер принимает трафик, выполняет первичный анализ трафика и более глубокий анализ извлеченных файлов. По результатам проверки компоненты выявляют признаки целевых атак на IT-инфраструктуру организации.

На другом сервере устанавливается компонент Sandbox.

Схема работы приложения при развертывании на два сервера представлена на рисунке ниже.

Схема развертывания на три сервера

При использовании функциональности KATA и KEDR вы можете установить компонент Endpoint Agent на компьютерах локальной сети организации. При использовании функциональности KATA компонент Endpoint Agent не устанавливается.

При использовании этой схемы развертывания компоненты Sensor, Central Node и Sandbox устанавливаются на отдельных серверах (см. раздел "Установка и первоначальная настройка приложения" на стр. 110). Компонент Central Node также может быть развернут в виде кластера. Сервер с компонентом Sensor принимает трафик, выполняет первичный анализ, извлекает файлы и пересылает их компоненту Central Node для более глубокого анализа.

При такой схеме развертывания компонент Central Node может принимать трафик и выполнять первичный анализ данных в основной инфраструктуре. В этом случае вы можете установить компонент Sensor на сервере удаленной инфраструктуры, трафик которой требуется анализировать. Если пропускная способность канала в основной инфраструктуре составляет более 2 Гбит/с, то сервер с компонентом Sensor рекомендуется устанавливать в основной инфраструктуре.

Трафик, передаваемый между компонентами Central Node и Sensor, составляет до 20% трафика, получаемого компонентом Sensor (см. раздел "Расчеты для компонента Sensor" на стр. 95).

Схема работы приложения при развертывании на три сервера представлена на рис. ниже.

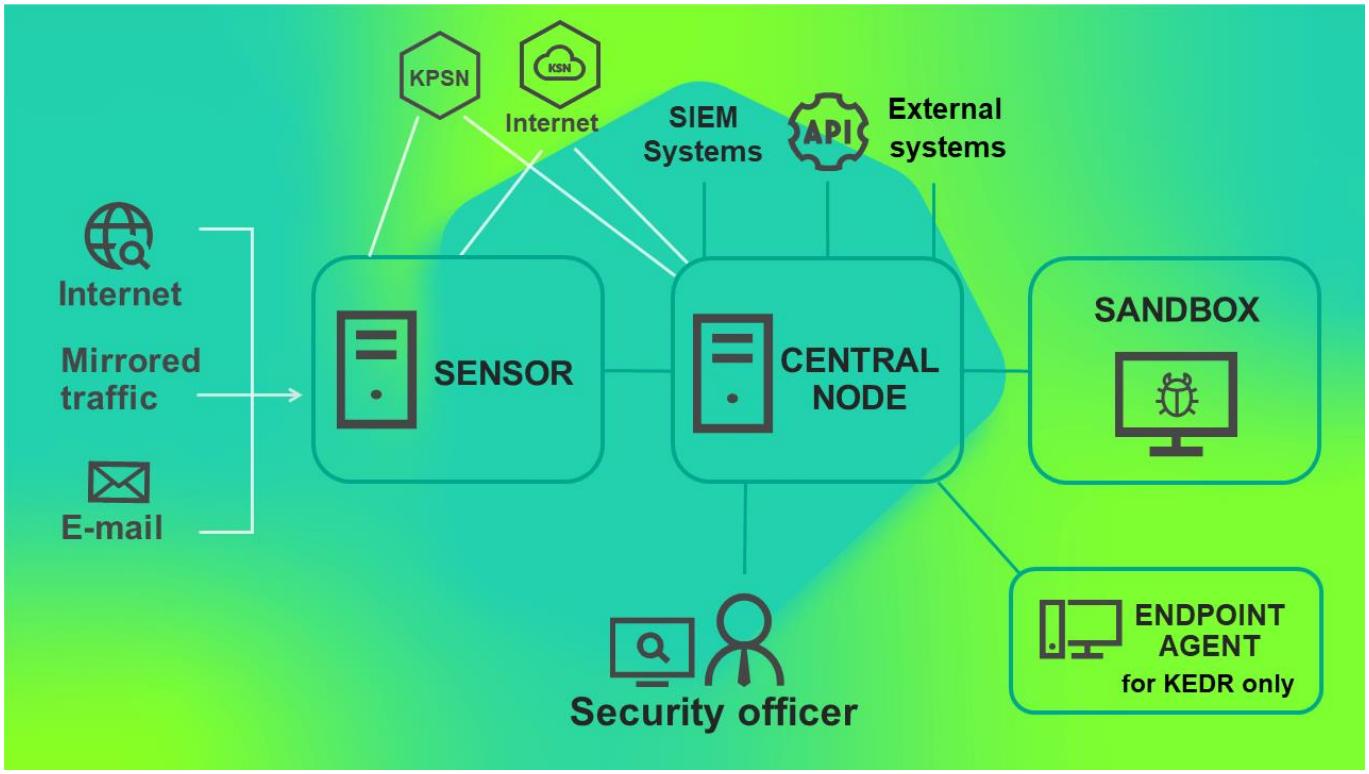


Схема развертывания на четыре и более сервера

При использовании функциональности KATA и KEDR вы можете установить компонент Endpoint Agent на компьютерах локальной сети организации. При использовании функциональности KATA компонент Endpoint Agent не устанавливается.

При большом объеме трафика вы можете установить несколько компонентов Sensor или несколько компонентов Sandbox на разных серверах. Эта схема рекомендуется для развертывания в крупных организациях.

Вы также можете использовать один компонент Sandbox для подключения к нескольким компонентам Central Node.

Схема работы приложения при развертывании на четыре и более сервера представлена на рисунке ниже.

Схема развертывания функциональности KEDR с компонентом Sandbox

При такой схеме развертывания вам требуется установить компонент Central Node отдельно от компонента Sensor (см. раздел "Установка и первоначальная настройка приложения" на стр. 110).

Схема работы приложения при развертывании функциональности KEDR с компонентом Sandbox представлена на рисунке ниже.

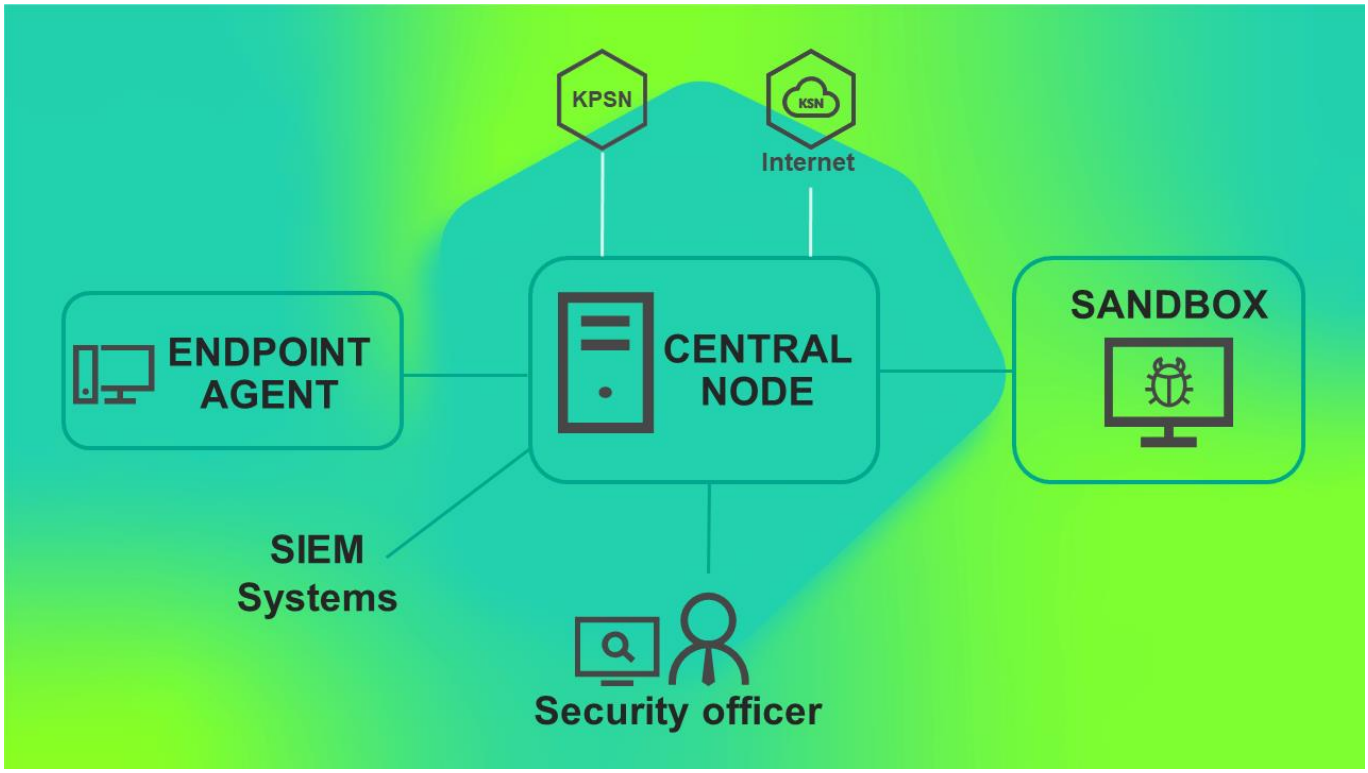
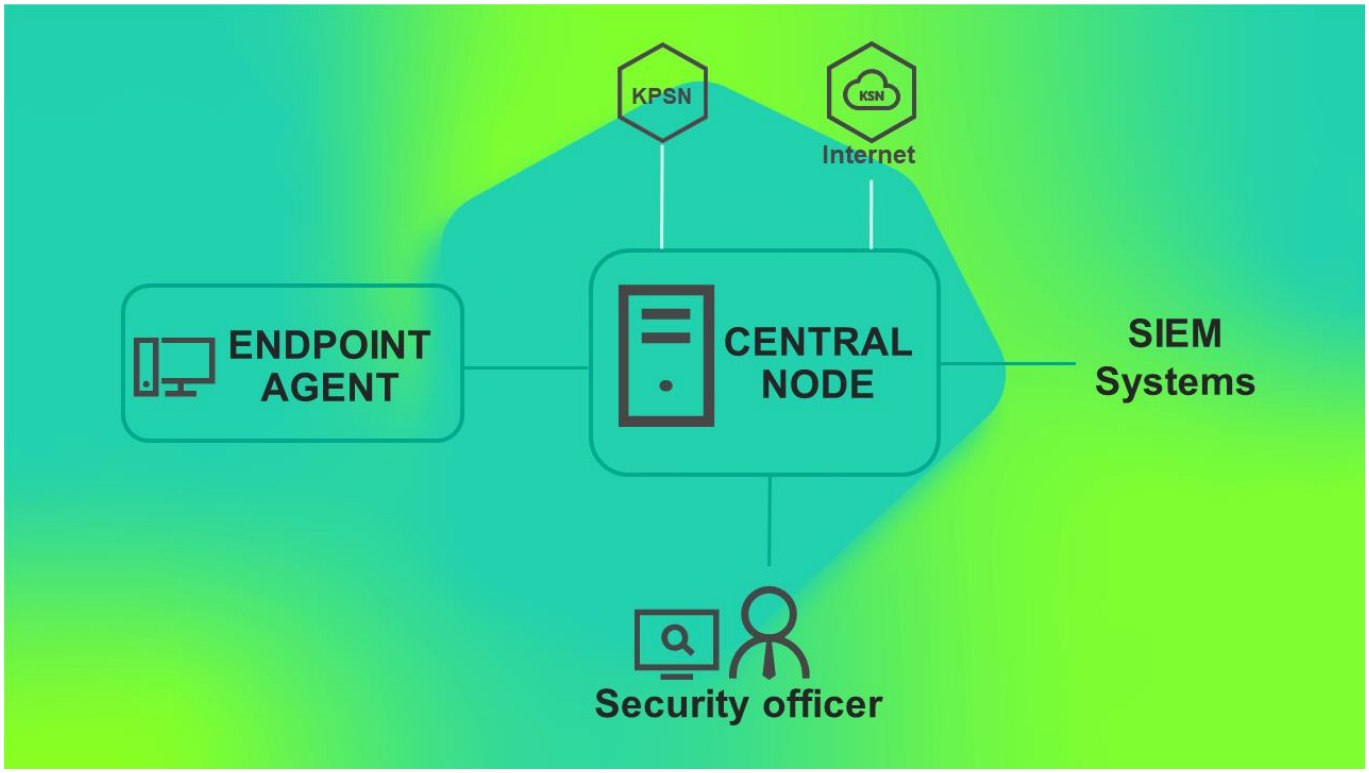


Схема развертывания функциональности KEDR без компонента Sandbox

Вы можете не устанавливать компонент Sandbox и использовать компонент Central Node только для управления компонентом Endpoint Agent и анализа данных.

При такой схеме развертывания вам требуется установить компонент Central Node отдельно от компонента Sensor (см. раздел "Установка и первоначальная настройка приложения" на стр. 110).

Схема работы приложения при развертывании функциональности KEDR без компонента Sandbox представлена на рис. ниже.



Калькулятор масштабирования

После того, как вы выбрали схему развертывания (см. раздел "Типовые схемы развертывания и установки компонентов приложения" на стр. 88), наиболее подходящую для вашей IT-инфраструктуры, вам требуется рассчитать аппаратные требования к серверам для установки компонентов приложения.

В этом разделе

Расчеты для компонента Sensor 95
Расчеты для компонента Central Node 97
Расчеты для компонента Sandbox 103
Расчеты для компонента Central Node, развернутого на платформе виртуализации KVM 106
Оптимизация настроек сетевых интерфейсов для компонента Sensor 108

Расчеты для компонента Sensor

Эти расчеты применимы также при развертывании приложения на виртуальной платформе.

При расчете аппаратных требований к компоненту Sensor требуется учитывать, что максимальный объем обрабатываемого трафика составляет 10 Гбит/с. Для обработки трафика максимального объема можно использовать как один компонент Sensor, установленный на отдельном сервере, так и несколько компонентов Sensor, установленных на отдельных серверах, которые подключены к одному компоненту Central Node. Суммарный объем передаваемого трафика от всех компонентов Sensor, подключенных к одному компоненту Central Node, не должен превышать 10 Гбит/с.

При наличии в сети более одного сегмента с пропускной способностью 10 Гбит/с и при необходимости обрабатывать трафик в этих сегментах, вам необходимо использовать режим распределенного решения (см. раздел "Распределенное решение и мультитенантность" на стр. 75).

Вы можете использовать сервер с компонентом Sensor в качестве прокси-сервера при обмене данными между компонентами Endpoint Agent и компонентом Central Node, чтобы упростить настройку сетевых правил. Например, если компоненты Endpoint Agent находятся в отдельном сегменте сети, то будет достаточно настроить соединение между серверами с компонентами Central Node и Sensor.

При настройке перенаправления трафика с компонентов Endpoint Agent на компонент Central Node учитывайте следующие ограничения:

- Максимальное количество компьютеров с компонентом Endpoint Agent, подключенных к одному компоненту Central Node, составляет 15 000 шт.
- Максимально допустимые потери пакетов, пересылаемых между серверами с компонентами Sensor и Central Node, составляют 10% при задержке отправки пакетов до 100 мс.

Аппаратные требования к серверу с компонентом Sensor зависят от объема обрабатываемого трафика. Требуемая пропускная способность канала связи между серверами с компонентами Central Node и Sensor определяется по следующей формуле:

```
10% от трафика на SPAN-порте при обычной нагрузке или 20% от трафика на SPAN-
порте при пиковой нагрузке + почтовый трафик + трафик по протоколу ICAP +
требования к каналу связи между компонентами Central Node и Endpoint Agent
```

Аппаратные требования к компоненту Sensor в зависимости от обрабатываемого трафика

Компонент Sensor может быть интегрирован с IT-инфраструктурой организации следующими способами:

- получение зеркалированного трафика от сетевых устройств со SPAN-портов (см. раздел "Настройка получения зеркалированного трафика со SPAN-портов" на стр. 263);
- подключение к почтовому серверу по протоколу POP3 (см. раздел "Настройка интеграции с почтовым сервером по протоколу POP3" на стр. 275);
- подключение к почтовому серверу по протоколу SMTP (см. раздел "Настройка интеграции с почтовым сервером по протоколу SMTP" на стр. 265);
- получение трафика от прокси-сервера по протоколу ICAP (см. раздел "Включение и отключение интеграции с прокси-сервером по протоколу ICAP" на стр. 267).

Аппаратные требования к компоненту Sensor приведены в таблице ниже. Расчеты приведены для случая, когда компонент Sensor не обрабатывает сообщения электронной почты и трафик по протоколу ICAP. Если компонент Sensor осуществляет перенаправление трафика компонентов Endpoint Agent, следует также учитывать требования к каналам связи.

Таблица 17. Аппаратные требования к компоненту Sensor в зависимости от объема обрабатываемого трафика со SPAN-портов

Количество компонентов Endpoint Agent	Объем обрабатываемого трафика (Мбит/с)	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер
10000	100	16	4
15000	500	24	8
15000	1000	32	12
15000	2000	64	20
15000	4000	92	32
15000	7000	128	52
15000	10000	160	72

Центральный процессор должен поддерживать набор инструкций BMI2.

Аппаратные требования к компоненту Sensor, интегрированному с почтовым сервером, приведены в таблице ниже. Расчеты приведены для случая, когда компонент Sensor не обрабатывает зеркалированный трафик и трафик по протоколу ICAP.

Таблица 18. Аппаратные требования к компоненту Sensor, интегрированному с почтовым сервером

Количество сообщений электронной почты в секунду	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер
1–4	16	4
5–20	16	8

Если один компонент Sensor обрабатывает трафик по нескольким протоколам, то для расчета конфигурации сервера необходимо учитывать, что при настроенной интеграции с почтовым сервером (на стр. 265) или почтовым сенсором (на стр. 300) необходимо выключить обработку трафика по протоколу SMTP (на стр. 263).

Требования к дисковому пространству на сервере с компонентом Sensor

Рекомендуется использовать дисковый массив RAID 1. Общий объем дискового пространства должен составлять не менее 500 ГБ.

Расчеты для компонента Central Node

При развертывании приложения на виртуальной платформе требуется на 10 процентов больше ресурсов процессора, чем в случае развертывания приложения на физическом сервере. В параметрах виртуального диска должен быть выбран тип диска Thick Provision.

Аппаратные требования к серверу с компонентами Central Node и Sensor

Аппаратные требования к серверу, на котором установлены компоненты Central Node и Sensor, зависят от следующих условий:

- объем обрабатываемого трафика;

  Объем обрабатываемого расшифрованного трафика для расчета нагрузки на сервер определяется по следующей формуле:

  ```
  <объем расшифрованного трафика, передаваемого приложением ArtX TLSProxy 1.9.1> = 5 * <объем незашифрованного трафика>
  ```

  Объем обрабатываемого на ICAP-сервере трафика для расчета нагрузки на сервер определяется по следующей формуле:

  ```
  <объем трафика, обрабатываемого на ICAP-сервере> = 5 * <объем трафика, который не обрабатывается на ICAP-сервере>
  ```

- количество обрабатываемых сообщений электронной почты в секунду;
- количество хостов с компонентом Endpoint Agent.

  Компонент Endpoint Agent может быть установлен на рабочую станцию, терминальный сервер, файловый сервер или в сетевое хранилище (NAS).

  Совместимость версий приложений, которыми представлен компонент Endpoint Agent, с версиями Kaspersky Anti Targeted Attack Platform см. в следующих разделах справки: Kaspersky Endpoint Agent для Windows (см. раздел "Совместимость версий Kaspersky Endpoint Agent для Windows с версиями Kaspersky Anti Targeted Attack Platform" на стр. 28), Kaspersky Endpoint Security для Windows (см. раздел "Совместимость версий Kaspersky Endpoint Security для Windows с версиями Kaspersky Anti Targeted Attack Platform" на стр. 33), Kaspersky Endpoint Security для Linux (см. раздел "Совместимость версий Kaspersky Endpoint Security для Linux с версиями Kaspersky Anti Targeted Attack Platform" на стр. 34), Kaspersky Endpoint Security для Mac (см. раздел "Совместимость Kaspersky Endpoint Security для Mac с версиями Kaspersky Anti Targeted Attack Platform" на стр. 35).

  Приложение Kaspersky Endpoint Agent для Windows также может быть установлено на сервер SCADA.

  Эффективное количество хостов с компонентом Endpoint Agent для расчета нагрузки на сервер определяется по следующей формуле:

  ```
  K = A+3*B+20*C
  ```

  где

  - "K" – эффективное количество хостов с компонентом Endpoint Agent.
  - "A" – количество рабочих станций и пользователей терминальных серверов под управлением операционной системы Windows с установленным компонентом Endpoint Agent.
  - "B" – количество рабочих станций и пользователей терминальных серверов под управлением операционной системы Linux или macOS с установленным компонентом Endpoint Agent.

- "C" – количество серверов с ролями файловый сервер, сетевое хранилище, SCADA сервер с установленным компонентом Endpoint Agent.

При объеме обрабатываемого трафика более 1 Гбит/с необходимо устанавливать компоненты Central Node и Sensor на отдельных серверах.

Аппаратные требования к серверу с компонентом Central Node в зависимости от используемой функциональности представлены в таблицах ниже.

Для работы Kaspersky Anti Targeted Attack Platform на базе операционной системы Astra Linux вам необходимо настроить приложение (см. раздел "Настройка Kaspersky Anti Targeted Attack Platform на базе операционной системы Astra Linux" на стр. 144).

Таблица 19. Аппаратные требования к серверу с компонентом Central Node при использовании функциональности KEDR

Максимальное количество хостов с компонентом Endpoint Agent	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер с частотой 3 ГГц	Первая дисковая подсистема				Вторая дисковая подсистема			
			ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)	Объем дискового массива RAID 1 или RAID 10 (ТБ)	Количество дисков в массиве RAID 1 или RAID 10	ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)	Объем дискового массива RAID 10 (ТБ)	Количество дисков в массиве RAID 10
1000	64	8	100	1000	1	4	300	200	Не более 6 дисков по 2,4 ТБ	4
3000	80	12	100	1000	1	4	700	500		6
5000	96	16	100	1000	1	4	1000	600		6
10 000	144	24	100	1000	1	4	2000	800		10
15 000	192	32	100	1000	1	4	2000	800		12

Таблица 20. Аппаратные требования к серверу с компонентом Central Node при использовании функциональности KATA и KEDR

Максимальное количество хостов с компонентом Endpoint Agent	Максимальное количество сообщений электронной почты в секунду	Максимальный объем трафика со SPAN-портов на сервере с компонентом Central Node	Максимальный объем трафика со SPAN-портов на серверах с компонентом Sensor (Мбит/с)	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер с частотой 3 ГГц	Первая дисковая подсистема				Вторая дисковая подсистема			
						ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)	Объем дискового массива RAID 1 или RAID 10 (ТБ)	Количество дисков в массиве RAID 1 или RAID 10	ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)	Объем дискового массива RAID 10 (ТБ)	Количество дисков в массиве RAID 10
1000	1	200	Не обрабатывается	96	16	100	1000	1,9	4	300	300	Не более 6 дисков по 2,4 ТБ	4
2000	2	500	Не обрабатывается	128	24	100	1000	2	4	500	500		4

Максимальное количество хостов с компонентом Endpoint Agent	Максимальное количество сообщений электронной почты в секунду	Максимальный объем трафика со SPAN-портов на сервере с компонентом Central Node	Максимальный объем трафика со SPAN-портов на серверах с компонентом Sensor (Мбит/с)	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер с частотой 3 ГГц	Первая дисковая подсистема				Вторая дисковая подсистема			
						ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)	Объем дискового массива RAID 1 или RAID 10 (ТБ)	Количество дисков в массиве RAID 1 или RAID 10	ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)	Объем дискового массива RAID 10 (ТБ)	Количество дисков в массиве RAID 10
5000	1	1000	Не обрабатывается	160	36	100	1000	2	4	1000	600		4
10 000	2	1000	Не обрабатывается	224	48	100	1000	2	4	2000	800		12
5000	5	Не обрабатывается	2000	144	32	100	1000	1,9	4	1000	600		6
10 000	20	Не обрабатывается	4000	224	56	100	1000	1,9	4	2000	800		12
15 000	20	Не обрабатывается	4000	256	64	100	1000	1,9	4	2000	800		12
15 000	20	Не обрабатывается	7000	320	104	100	1000	1,9	4	2000	800		12
15 000	20	Не обрабатывается	10 000	320	144	100	1000	1,9	4	2000	800		12

Таблица 21.
Аппаратные требования к серверу с компонентом Central Node при использовании функциональности KATA

Максимальное количество сообщений электронной почты в секунду	Максимальный объем трафика со SPAN-портов на сервере с компонентом Central Node	Максимальный объем трафика со SPAN-портов на серверах с компонентом Sensor (Мбит/с)	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер с частотой 3 ГГц	Первая дисковая подсистема			
					ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)	Объем дискового массива RAID 1 или RAID 10 (ТБ)	Количество дисков в массиве RAID 1 или RAID 10
2	500	Не обрабатывается	64	20	100	1000	2	4
2	1000	Не обрабатывается	80	28	100	1000	2	4
5	Не обрабатывается	2000	64	20	100	1000	2	4
20	Не обрабатывается	4000	80	40	100	1000	2	4
20	Не обрабатывается	7000	128	72	100	1000	2	4
20	Не обрабатывается	10000	128	112	100	1000	2	4

Kaspersky Anti Targeted Attack Platform не поддерживает работу с программным RAID-массивом.

Центральный процессор должен поддерживать набор инструкций BMI2.

Примеры расчета требуемой конфигурации серверов с компонентами Kaspersky Anti Targeted Attack Platform

Если вы хотите:

- обрабатывать трафик с сетевого устройства с пропускной способностью до 4 Гбит/с;
- обрабатывать 20 сообщений электронной почты в секунду;
- использовать 15 000 хостов с Kaspersky Endpoint Agent для Windows или Kaspersky Endpoint Security для Windows или 5000 хостов с Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac,

то вам требуется два сервера со следующими аппаратными характеристиками:

- сервер с компонентом Central Node: не менее 256 ГБ оперативной памяти и 64 логических ядер процессора;
- сервер с компонентом Sensor: не менее 92 ГБ оперативной памяти и 32 логических ядер процессора.

Требования к дисковому пространству на сервере с компонентом Central Node

На сервере с компонентом Central Node должно быть не менее 2000 ГБ свободного пространства на первой дисковой подсистеме и не менее 2400 ГБ на второй дисковой подсистеме. Объем требуемого пространства на второй дисковой подсистеме зависит от желаемой политики хранения данных и может быть вычислен по следующей формуле:

```
150 ГБ + <количество хостов с Kaspersky Endpoint Agent или Kaspersky Endpoint
Security для Windows>/15000 * (400 ГБ + 240 ГБ * <срок, за который требуется
хранить данные, в днях>)/0.65, но не более 12 ТБ.
```

Эта формула может быть использована для примерной оценки требуемого дискового пространства. Реальный объем хранимых данных зависит от профиля трафика организации и может отличаться от полученного результата вычислений.

Если вы настроили интеграцию для проверки объектов внешней системы с помощью REST API (см. раздел "API для проверки объектов внешних систем" на стр. 619), вам необходимо увеличить аппаратные характеристики сервера с компонентом Central Node. Дополнительные аппаратные требования приведены в таблице ниже.

Таблица 22. Дополнительные аппаратные требования к серверу с компонентом Central Node при наличии интегрированных внешних систем

Максимальное количество обрабатываемых объектов в секунду	Количество дополнительных логических ядер	Количество дополнительных серверов с компонентом Sandbox
8	2	1
16	4	2
24	7	3

Если вы настроили интеграцию для отправки событий во внешнюю систему с помощью REST API (см. раздел "API для получения внешними системами информации о событиях приложения" на стр. 633), вам необходимо увеличить аппаратные характеристики сервера с компонентом Central Node на 1 логическое ядро и 6 ГБ оперативной памяти.

Если вы установили компонент Central Node и Sensor не в виде кластера, вам необходимо рассчитать объем на диске для параметров База событий, ГБ и Хранилище, ГБ по следующей формуле:

```
A = F - R, ГБ.
```

где

- A – объем, используемый для базы событий и Хранилища.
- F – объем жесткого диска, на котором установлен компонент Central Node.
- R – зарезервированное количество свободного пространства (ГБ), соответствующее количеству подключенных хостов с компонентом Endpoint Agent, приведенное в таблице ниже.

Если количество подключенных к компоненту Central Node хостов находится в диапазоне между значениями, используйте в расчетах большее число.

Таблица 23. Зарезервированное количество свободного пространства в зависимости от количества хостов с компонентом Endpoint Agent

Количество хостов с компонентом Endpoint Agent	Рекомендуемое количество свободного пространства (ГБ)
1000	1000
3000	1200
5000	1400
10 000	1900
15 000	2400

Требования к серверу PCN в режиме распределенного решения

Если вы используете режим распределенного решения, при расчете аппаратных требований необходимо учитывать, что аппаратные требования к серверу PCN на 10% выше для минимального объема оперативной памяти и для минимального количества логических ядер, чем к серверу с компонентом Central Node. Аппаратные требования к серверу с компонентом Central Node указаны в таблицах *Аппаратные требования к серверу с компонентом Central Node при использовании функциональности KEDR*,

Аппаратные требования к серверу с компонентом Central Node при использовании функциональности KATA+KEDR, Аппаратные требования к серверу с компонентом Central Node при использовании функциональности KATA (см. выше).

Вы можете подключить к одному серверу PCN до 30 серверов SCN.

Требования к каналам связи

Необходимо обеспечить пропускную способность канала связи между сервером с компонентом Central Node и каждым сегментом сети в зависимости от количества хостов с компонентом Endpoint Agent в сегменте. Пропускная способность в зависимости от количества хостов с компонентом Endpoint Agent приведена в таблице ниже.

Таблица 24. Пропускная способность канала связи в зависимости от количества хостов с компонентом Endpoint Agent

Максимальное количество хостов с компонентом Endpoint Agent	Требуемая пропускная способность канала связи, зарезервированная для компонентов Endpoint Agent (Мбит/с)
10	1
50	2
100	3
1000	20
10 000	200

Минимальные требования к каналу связи между серверами PCN и SCN в режиме распределенного решения приведены в таблице ниже.

Таблица 25. Минимальные требования к каналу связи между серверами PCN и SCN

Максимальное количество хостов с компонентом Endpoint Agent	Максимальное количество сообщений электронной почты в секунду	Максимальный объем трафика со SPAN-портов (Мбит/с)	Требуемая пропускная способность канала связи (Мбит/с)
5000	5	2000	20
10 000	20	4000	30

Аппаратные требования к серверам кластера Central Node

Кластер должен включать минимум 4 сервера: 2 сервера хранения и 2 обрабатывающих сервера. При подключении до 15 000 хостов с компонентом Endpoint Agent, вам нужно минимум 2 сервера хранения и 2 обрабатывающих сервера. При подключении от 15 000 до 30 000 хостов с компонентом Endpoint Agent вам требуется не менее 2 серверов хранения и 3 обрабатывающих серверов.

Каждый сервер кластера должен иметь два сетевых адаптера для настройки кластерной и внешней подсети. Кластерная подсеть должна функционировать со скоростью 10 Гбит/с.

Для кластерной подсети также должны выполняться следующие требования:

- В кластерную подсеть должны входить только серверы кластера и сетевые коммутаторы.
- Серверы кластера должны находиться в одном L1- или L2-сегменте. Для этого вы можете подключить все серверы кластера к одному коммутатору или использовать программное туннелирование. Например, L2TPv3 или Overlay Transport Virtualization (OTV).

- Значение сетевой задержки ("network latency") должно удовлетворять требованию "single digit latency", то есть в миллисекундах значение должно быть менее 10.

Аппаратные требования к серверам кластера при использовании функциональности KEDR приведены в таблице ниже.

Таблица 26. Аппаратные требования к обрабатывающим серверам при использовании функциональности KEDR

Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Тип массива RAID	Количество дисков в массиве RAID	Объем одного жесткого диска (ГБ)
256	48	RAID 1	2	1200

Таблица 27. Аппаратные требования к серверам хранения при использовании функциональности KEDR

Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Первая дисковая подсистема			Вторая дисковая подсистема	
		Тип массива RAID	Количество дисков в массиве RAID	Объем одного жесткого диска (ГБ)	Количество дисков	Объем одного жесткого диска (ГБ)
128	16	RAID 1	2	1200	Не менее 6	Не менее 1200

Рекомендуется использовать для двух дисковых подсистем диски одинакового объема. Для второй дисковой подсистемы используются диски, не объединенные в RAID-массив.

Требования к скорости дисковых подсистем аналогичны требованиям, указанным в таблице *Аппаратные требования к серверу с компонентом Central Node при использовании функциональности KEDR* (см. выше).

Расчеты для компонента Sandbox

Аппаратные требования к серверу с компонентом Sandbox зависят от типа и объема обрабатываемого трафика и от допустимого времени проверки объекта.

По умолчанию допустимое время проверки объекта составляет 1 час. Для уменьшения этого времени требуется более мощный сервер или большее количество серверов с компонентом Sandbox.

Рекомендуется рассчитывать конфигурацию компонента Sandbox следующим образом:

1. Установите компоненты Central Node и Sensor на одном сервере и компонент Sandbox на другом сервере для пилотирования приложения.

   Для получения достаточных статистических данных необходимо, чтобы приложение обрабатывало трафик организации в течение недели.

2. Запустите скрипт для записи данных, выполнив команды:

```
sudo kata-run.sh kata-collect --output-dir path-to-folder
--output-dir <путь к директории>
```

Когда скрипт завершит работу, в указанную директорию будет помещен архив *collect.tar.gz*.

3. Передайте этот архив для анализа сотрудникам "Лаборатории Касперского".

При одновременном запуске нескольких виртуальных машин скорость обработки объектов из очереди увеличивается.

Работа компонента Sandbox не поддерживается на процессорах AMD.

Аппаратные требования к серверу с компонентом Sandbox

Расчет количества серверов с компонентом Sandbox при использовании преднастроенных образов операционных систем приведен в таблице ниже.

Таблица 28. Аппаратные требования к компоненту Sandbox при использовании преднастроенных образов операционных систем

Максимальное количество сообщений электронной почты в секунду	Максимальный объем трафика со SPAN-портов (Мбит/с)	Максимальное количество компьютеров с компонентом Endpoint Agent	Количество физических серверов с компонентом Sandbox	
			При использовании всех образов	При использовании только двух образов с ОС Linux
1	200	1000	1	1
2	500	3000	1	1
1	1000	5000	1	1
5	2000	5000	1	1
20	4000	10000	2	1
20	7000	15000	4	2
20	10000	15000	5	2

Если вы хотите установить компонент Sandbox на виртуальный сервер, для получения аналогичной физическому серверу производительности вам понадобится в 3–4 раза больше серверов.

При использовании пользовательских образов для серверов с компонентом Sandbox могут потребоваться дополнительные мощности. Расчет количества физических серверов с компонентом Sandbox, необходимых при использовании пользовательских образов операционных систем, выполняется по следующей формуле:

```
<количество файлов, которое будет поступать на обработку согласно
пользовательским правилам Sandbox, в час> * <количество пользовательских
образов операционных систем> / 1000
```

Расчет количества виртуальных серверов с компонентом Sandbox, необходимых при использовании пользовательских образов операционных систем, выполняется по следующей формуле:

```
<количество файлов, которое будет поступать на обработку согласно
пользовательским правилам Sandbox, в час> * <количество пользовательских
образов операционных систем> / 280
```

Оценка количества серверов Sandbox приведена для серверов следующей конфигурации:

- При установке компонента Sandbox на физический сервер:

- 2 процессора Intel® Xeon® 8 Core™ (HT) с частотой 2,6 ГГц или выше.
- 80 ГБ оперативной памяти.
- 2 HDD объемом 300 ГБ каждый, объединенные в массив RAID1.

- При установке компонента Sandbox на виртуальную машину VMware ESXi:
  - Процессор Intel Xeon 15 Core (HT) с частотой 2,1 ГГц или выше;
  - 32 ГБ оперативной памяти;
  - HDD объемом 300 ГБ.

    На виртуальной машине:

    1. Разрешена вложенная виртуализация.
    2. Установлены параметры High Latency Sensitivity.
    3. Зарезервирована вся оперативная память.
    4. Зарезервирована вся частота процессора.

При настройке виртуальной машины вам требуется задать описанную выше конфигурацию. Допускается изменение только частоты процессора: вы можете задать частоту 2.2 ГГц и выше. Если при настройке виртуальной машины вы зададите конфигурацию, отличную от описанной, корректная установка и работа компонента Sandbox не гарантируется.

При установке компонента Sandbox на виртуальную машину VMware ESXi нужно установить ограничение для количества одновременно запускаемых виртуальных машин (см. раздел "Установка максимального количества одновременно запускаемых виртуальных машин" на стр. 239) – 12.

Расчеты для компонента Central Node, развернутого на платформе виртуализации KVM

Для развертывания компонента Central Node в виртуальной инфраструктуре должен быть установлен гипервизор KVM на базе операционной системы Debian GNU/Linux 12 и с использованием эмулятора QEMU version 8.0.2.

При развертывании компонента Central Node в виртуальной инфраструктуре учитывайте следующие ограничения:

- Возможна установка приложения с установочными файлами операционной системы Ubuntu.
- Возможна установка только неотказоустойчивой версии приложения.
- Возможно использование только компонента Sensor, развернутого на одном сервере с компонентом Central Node.
- Возможно подключение только компонента Sandbox, развернутого вне платформы виртуализации KVM на физическом сервере или на другой поддерживаемой платформе виртуализации.
- Для каждого компонента Central Node, развернутого в виртуальной инфраструктуре, необходимо использовать отдельный сетевой интерфейс для получения зеркалированного SPAN-трафика.

- Невозможно использование API для получения внешними системами информации об обнаружениях приложения и API для получения внешними системами информации о событиях приложения.
- Не гарантируется поддержка KVM-виртуализаций, используемых в облачных решениях.

Аппаратные требования к серверу с компонентом Central Node в зависимости от используемой функциональности представлены в таблицах ниже.

Таблица 29. Аппаратные требования к серверу с компонентом Central Node при использовании функциональности KEDR

Максимальное количество хостов с компонентом Endpoint Agent	Максимальное количество сообщений электронной почты в минуту	Максимальный объем трафика со SPAN-портов на сервере с компонентом Central Node (Мбит/с)	Минимальное количество логических ядер с частотой 3 ГГц	Минимальный объем оперативной памяти (ГБ)
50	0	0	4	20
100	0	0	4	20
150	0	0	4	20
250	0	0	6	22
500	0	0	6	24
750	0	0	6	26

Таблица 30. Аппаратные требования к серверу с компонентом Central Node при использовании функциональности KATA+KEDR

Максимальное количество хостов с компонентом Endpoint Agent	Максимальное количество сообщений электронной почты в минуту	Максимальный объем трафика со SPAN-портов на сервере с компонентом Central Node (Мбит/с)	Минимальное количество логических ядер с частотой 3 ГГц	Минимальный объем оперативной памяти (ГБ)
100	1	20	6	26
250	5	50	6	28
500	30	100	10	31
750	30	100	12	31

kaspersky

Оптимизация настроек сетевых интерфейсов для компонента Sensor

Следуйте инструкции, если в процессе работы приложения наблюдаются потери сетевых пакетов или проблемы с производительностью при обработке сетевого трафика.

► *Чтобы уменьшить потери сетевых пакетов и неполного извлечения файлов из трафика:*

1. Укажите максимальное количество RSS-очередей:
   - Если скорость передачи данных в вашей сети составляет менее 1 Гбит/с, установите значение 1.
   - Если скорость передачи данных в вашей сети составляет более 1 Гбит/с, установите значение 16.

   Если ваша сетевой интерфейс не позволяет установить значение 16 для параметра максимальное количество RSS-очередей, установите максимально возможное значение параметра.

2. Настройте симметричное RSS-хеширование для сетевого интерфейса. Подробнее о настройке RSS-хеширования см. в документации производителя сетевой карты.
3. Создайте файл interrupts.sh со следующим содержимым:

```
#!/usr/bin/env bash

set -e

dev=$1
min_cpu=$2
max_cpu=$3
step=$4

irs=($(cat /proc/interrupts | grep "$dev" | awk '{split($1,a,":");
print a[1]}'))

cpu=$min_cpu
for ir in ${irs[@]}; do
        echo $cpu > /proc/irq/$ir/smp_affinity_list
        cpu=$(((cpu + step) % max_cpu))
        cat "/proc/irq/$ir/smp_affinity_list"
done
```

4. Выполните команду:

   `sudo bash interrupts.sh <dev> <min_cpu> <max_cpu> <step>`, где
   - `<dev>` – сетевой интерфейс, прерывания которого нужно распределить по ядрам.
   - `<min_cpu>` – ядро, с которого нужно начать распределять прерывания от сетевой карты;
   - `<max_cpu>` – ядро, на котором нужно закончить распределять прерывания от сетевой карты;
   - `<step>` – шаг , с которым будет назначаться ядро для прерывания.

Пример:

```
sudo bash interrupts.sh ens192 2 11 1
```

5. Если вы используете сетевые карты семейства NVIDIA Mellanox (mlx4), настройте количество RSS-очередей и RSS-хеширование, выполнив команды:

```
ethtool -L $dev rx 16
ethtool -X $dev equal 16
ethtool -X $dev hfunc xor
```

6. Если вы используете сетевые карты семейства Intel (i40e), настройте количество RSS-очередей и RSS-хеширование, выполнив команды:

```
rmmod i40e && modprobe i40e
ifconfig $dev down
ethtool -L $dev combined 16
ethtool -K $dev rxhash on
ethtool -K $dev ntuple on
ifconfig $dev up
ethtool -X $dev hkey
6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A
:6D:5A:6D:5A:6D:
5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A:6D:5A
equal 16
ethtool -A $dev rx off
ethtool -C $dev adaptive-rx off adaptive-tx off rx-usecs 125
ethtool -G $dev rx 1024
ethtool -N $dev rx-flow-hash tcp4 sdfn
ethtool -N $dev rx-flow-hash tcp6 sdfn
ethtool -N $dev rx-flow-hash udp4 sdfn
ethtool -N $dev rx-flow-hash udp6 sdfn
```

Сетевые интерфейсы будут настроены.

После перезагрузки приложения вам необходимо заново настроить сетевые интерфейсы следуя инструкции.

kaspersky

Установка и первоначальная настройка приложения

В этом разделе содержатся инструкции по установке и первоначальной настройке Kaspersky Anti Targeted Attack Platform.

В этом разделе

Подготовка к установке компонентов приложения 110

Порядок установки и настройки компонентов приложения 116

Установка компонента Sandbox 119

Развертывание компонентов Central Node и Sensor в виде кластера 124

Установка компонентов Central Node и Sensor на сервере 136

Установка компонента Sensor на отдельном сервере 142

Настройка Kaspersky Anti Targeted Attack Platform на базе операционной системы Astra Linux 144

Установка пакета обновления приложения до версии 6.0.2 146

Подключение и настройка внешнего хранилища для компонента Sensor 147

Подготовка к установке компонентов приложения

В этом разделе представлена информация о том, как подготовить IT-инфраструктуру вашей организации к установке компонентов Kaspersky Anti Targeted Attack Platform.

В этом разделе

Подготовка IT-инфраструктуры к установке компонентов приложения 111

Подготовка IT-инфраструктуры к интеграции с почтовым сервером для приема сообщений по протоколу POP3 113

Подготовка IT-инфраструктуры к интеграции с почтовым сервером для отправки сообщений по протоколу SMTP 113

Подготовка виртуальной машины к установке компонента Sandbox 114

Подготовка IT-инфраструктуры к установке компонентов приложения

► *Перед установкой приложения подготовьте IT-инфраструктуру вашей организации к установке компонентов Kaspersky Anti Targeted Attack Platform:*

1. Убедитесь, что серверы, а также компьютер, предназначенный для работы с веб-интерфейсом приложения, и компьютеры, на которых устанавливается компонент Endpoint Agent, удовлетворяют аппаратным и программным требованиям (см. раздел "Аппаратные и программные требования" на стр. 27).
2. Произведите следующую предварительную подготовку IT-инфраструктуры организации к установке компонента Sandbox:
   a. Для обоих сетевых интерфейсов запретите доступ сервера с компонентом Sandbox в локальную сеть организации для обеспечения безопасности сети от анализируемых объектов.
   b. Для первого сетевого интерфейса разрешите доступ сервера с компонентом Sandbox в интернет для анализа поведения объектов.
   c. Для второго сетевого интерфейса разрешите входящее соединение сервера с компонентом Sandbox на следующие порты:
      - TCP 22 для подключения к серверу по протоколу SSH.
      - TCP 443 для получения объектов на проверку от компонента Central Node.
      - TCP 8443 для использования веб-интерфейса приложения.
   d. Для второго сетевого интерфейса разрешите исходящее соединение сервера с компонентом Sandbox на следующие порты:
      - TCP 80, 443 для связи с серверами обновлений "Лаборатории Касперского".
3. Произведите следующую предварительную подготовку IT-инфраструктуры организации к установке компонента Central Node:
   a. Разрешите входящие соединения к серверу с компонентом Central Node на следующие порты:
      - TCP 22 для подключения к серверу по SSH.
      - TCP 443 для получения данных от компьютеров с компонентом Endpoint Agent.
      - TCP 8443 для просмотра результатов проверки в веб-интерфейсе приложения.
      - UDP 53 для связи с сервером с компонентом Sensor.
      - TCP 9081 для получения данных от компонентов Sensor, установленных на отдельных серверах.
   b. Разрешите исходящее соединение сервера с компонентом Central Node на следующие порты:
      - TCP 80, 443 и 1443 для связи с серверами службы KSN и серверами обновлений "Лаборатории Касперского".
      - TCP 443 для передачи объектов на проверку компоненту Sandbox.
      - TCP 601 для отправки сообщений в SIEM-систему.
      - UDP 53 для связи с сервером с компонентом Sensor.
4. Произведите следующую предварительную подготовку IT-инфраструктуры организации к установке компонента Sensor:

a. Для сетевого интерфейса, используемого для интеграции с прокси-сервером и почтовым сервером, разрешите входящее соединение сервера с компонентом Sensor на следующие порты:
   - TCP 22 для подключения к серверу по SSH.
   - TCP 1344 для получения трафика от прокси-сервера.
   - TCP 25 для получения SMTP-трафика от почтового сервера.
   - TCP 443 при перенаправлении трафика от компьютеров с компонентом Endpoint Agent на сервер с компонентом Central Node.
   - UDP 53 для связи с сервером с компонентом Central Node.

b. Разрешите исходящее соединение сервера с компонентом Sensor на следующие порты:
   - TCP 80 и 443 для связи с серверами службы KSN и серверами обновлений "Лаборатории Касперского".
   - TCP 995 (или TCP 110 для незащищенных соединений) для интеграции с почтовым сервером.
   - TCP 9081 для перенаправления трафика на сервер с компонентом Central Node.
   - UDP 53 для связи с сервером с компонентом Central Node.

   При установке дополнительного сетевого интерфейса, принимающего только зеркалированный трафик, в виртуальной среде VMware ESXi используйте сетевой адаптер E1000 или отключите опцию LRO (large receive offload) на сетевом адаптере VMXNET3.

5. Разрешите на сетевом оборудовании шифрованный канал связи между серверами с компонентами Central Node и Sensor.

   Соединение между серверами с компонентами Central Node и Sensor происходит внутри шифрованного канала связи на базе IPSec с использованием протоколов ESP, AH, IKEv1 и IKEv2.

6. Если вы используете режим распределенного решения и мультитенантности, произведите следующую предварительную подготовку IT-инфраструктуры организации к установке компонентов Central Node:

   a. Разрешите входящее соединение сервера с ролью PCN на порты 8443.

   b. Разрешите на сетевом оборудовании установку шифрованного канала связи между серверами PCN и SCN.

      Соединение между серверами с ролью PCN и SCN происходит внутри шифрованного канала связи на базе IPSec с использованием протокола ESP.

При необходимости вы можете назначить другие порты для работы компонентов приложения в меню администратора сервера с компонентом Central Node. При изменении портов в меню администратора вам нужно разрешить соединения на эти порты внутри IT-инфраструктуры вашей организации.

Подготовка IT-инфраструктуры к интеграции с почтовым сервером для приема сообщений по протоколу POP3

Если в качестве почтового сервера вы используете почтовый сервер Microsoft Exchange и отправитель настроил запрос уведомления о прочтении сообщения электронной почты, то необходимо отключить отправку уведомлений о прочтении. В противном случае уведомления о прочтении будут отправляться с того адреса электронной почты, который вы настроили в качестве адреса электронной почты для приема сообщений Kaspersky Anti Targeted Attack Platform. Также необходимо отключить автоматическую обработку приглашений на встречи для предотвращения заполнения почтового ящика для приема сообщений Kaspersky Anti Targeted Attack Platform.

► *Чтобы отключить отправку уведомлений о прочтении с адреса электронной почты для приема сообщений Kaspersky Anti Targeted Attack Platform:*

1. На сервере Microsoft Exchange проверьте, включена ли отправка уведомлений. Для этого выполните команду:

   ```
   Get-MailboxMessageConfiguration -Identity <адрес электронной почты для приема сообщений Kaspersky Anti Targeted Attack Platform> | fl
   ```

2. Если отправка уведомлений включена, выполните команду:

   ```
   Set-MailboxMessageConfiguration -Identity <адрес электронной почты для приема сообщений Kaspersky Anti Targeted Attack Platform> -ReadReceiptResponse NeverSend
   ```

Отправка уведомлений о прочтении с адреса электронной почты для приема сообщений Kaspersky Anti Targeted Attack Platform будет отключена.

► *Чтобы отключить автоматическую обработку приглашений на встречи:*

1. На сервере Microsoft Exchange проверьте, включена ли отправка уведомлений. Для этого выполните команду:

   ```
   Get-CalendarProcessing -Identity <адрес электронной почты для приема сообщений Kaspersky Anti Targeted Attack Platform> | fl
   ```

2. Если автоматическая обработка приглашений на встречи включена, выполните команду:

   ```
   Set-CalendarProcessing -Identity <адрес электронной почты для приема сообщений Kaspersky Anti Targeted Attack Platform> -AutomateProcessing:None
   ```

Автоматическая обработка приглашений на встречи будет отключена.

Подготовка IT-инфраструктуры к интеграции с почтовым сервером для отправки сообщений по протоколу SMTP

► *Чтобы подготовить IT-инфраструктуру вашей организации к интеграции Kaspersky Anti Targeted Attack Platform с почтовым сервером по протоколу SMTP:*

1. На внешнем почтовом сервере настройте правила пересылки копий тех сообщений, которые вы хотите отправлять на проверку Kaspersky Anti Targeted Attack Platform на адреса, указанные в Kaspersky Anti Targeted Attack Platform.

2. Укажите маршрут для пересылки сообщений электронной почты на сервер с компонентом Sensor.

   Рекомендуется указать статический маршрут – IP-адрес сервера с компонентом Sensor.

3. На сетевом экране вашей организации разрешите входящие соединения сервера с компонентом Sensor на порт 25 от почтовых серверов, пересылающих копии сообщений электронной почты.

Вы также можете увеличить безопасность интеграции Kaspersky Anti Targeted Attack Platform с почтовым сервером по протоколу SMTP.

► *Чтобы увеличить безопасность интеграции Kaspersky Anti Targeted Attack Platform с почтовым сервером по протоколу SMTP:*

1. Настройте аутентификацию сервера Kaspersky Anti Targeted Attack Platform на стороне почтовых серверов, передающих сообщения электронной почты для Kaspersky Anti Targeted Attack Platform.
2. Настройте обязательное шифрование трафика на почтовых серверах, передающих сообщения электронной почты для Kaspersky Anti Targeted Attack Platform.
3. Настройте аутентификацию почтовых серверов, передающих сообщения электронной почты для Kaspersky Anti Targeted Attack Platform, на стороне Kaspersky Anti Targeted Attack Platform.

Подготовка виртуальной машины к установке компонента Sandbox

► *Чтобы подготовить виртуальную машину к установке компонента Sandbox:*

1. Запустите гипервизор VMware ESXi.
2. Откройте консоль для управления виртуальными машинами.
3. В контекстном меню виртуальной машины, на которой вы хотите установить компонент Sandbox, выберите пункт **Edit Settings**.

   Откроется окно свойств виртуальной машины.

4. На закладке **Virtual Hardware** раскройте блок параметров **CPU** и установите флажок **Expose hardware-assisted virtualization to guest OS**.
5. На закладке **VM Options** в раскрывающемся списке **Latency Sensitivity** выберите **High**.
6. Нажмите на кнопку **OK**.

Виртуальная машина будет готова к установке компонента Sandbox.

Подготовка установочного образа диска с компонентами Central Node, Sensor и Sandbox

Перед установкой приложения вам необходимо подготовить установочный iso-образ диска с компонентами Central Node, Sensor и Sandbox на базе операционной системы Astra Linux.

Минимальные аппаратные требования к устройству, на котором будет происходить создание iso-образа:

- Процессор: 4 ядра, частота от 2500 МГц.
- Оперативная память: 8 ГБ.
- Объем свободного места на диске: 100 ГБ.

Требования к программному обеспечению:

- Операционная система на базе актуального ядра Linux.
- Docker версии 20 и выше.
- Наличие iso-образа операционной системы Astra Linux Special Edition версии 1.7.4. UU1.

Kaspersky Anti Targeted Attack Platform не поддерживает работу с другими версиями операционной системы Astra Linux.

► *Чтобы смонтировать iso-образ на базе операционной системы Astra Linux компонентов Central Node и Sensor или Sandbox:*

1. Загрузите из комплекта поставки дистрибутив компонентов Central Node и Sensor kata-cn-distribution-6.0.0-200-x86_64_en-ru.tar.gz, дистрибутив компонента Sandbox kata-sb-distribution-6.0.0-30-x86_64_en-ru.tar.gz и файл iso-builder-6.0.0-200-x86_64_en-ru.tar.
2. Создайте файл iso_builder.sh со следующим содержимым.

```
# $1 - absolute source_iso_host_path
# $2 - absolute distribution_host_path
# $3 - absolute iso_builder_image_host_path
# $4 - absolute build_host_path
# $5 - absolute target_iso_name
docker load -i $3
docker run -v $1:$1 -v $2:$2 -v $4:/build
kaspersky/kata/deployment/iso_builder:6.0 --source-iso-uri file://$1
--kata-distribution-uri file://$2 --target-iso-name $5
```

3. Выполните команду `mkdir /var/kata_builder`.
4. Поместите в созданный каталог kata_builder файлы, указанные в шаге 1. Убедитесь, что iso-образ Astra Linux Special Edition версии 1.7.4. UU1 имеет имя installation-1.7.4.11-23.06.23_17.13.iso. Если имя iso-образа отличается, вам необходимо его переименовать.
5. Выполните команду:
   - Если вы подготавливаете образ диска с компонентами Central Node и Sensor:

     ```
     sudo./iso_builder.sh /var/kata_builder/installation-1.7.4.11-
     23.06.23_17.13.iso /var/kata_builder/kata-cn-distribution-6.0.0-200-
     x86_64_en-ru.tar.gz /var/kata_builder/iso-builder-6.0.0-200-
     x86_64_en-ru.tar /var/kata_builder buildCNSensorAstra.iso
     ```

   - Если вы подготавливаете образ диска с компонентом Sandbox: `sudo ./iso_builder.sh /var/kata_builder/installation-1.7.4.11-23.06.23_17.13.iso /var/kata_builder/kata-sb-distribution-6.0.0-30-x86_64_en-ru.tar.gz /var/kata_builder/iso-builder-6.0.0-200-x86_64_en-ru.tar /var/kata_builder buildSandboxAstra.iso`

После выполнения команд установочный образ диска с компонентами Central Node и Sensor с именем buildCNSensorAstra.iso и buildSandboxAstra.iso будут размещены по пути /var/kata_builder.

Если вы используете другие директории для хранения файлов, вы можете выполнить команду: `sudo ./iso_builder.sh <source_iso_host_path> <distribution_host_path> <iso_builder_image_host_path> <build_host_path> <target_iso_name>`, где:

- source_iso_host_path – путь к дистрибутиву Astra Linux Special Edition 1.7.4. UU1.
- distribution_host_path – путь к дистрибутиву kata-cn-distribution-6.0.0-200-x86_64_en-ru.tar.gz или kata-sb-distribution-6.0.0-30-x86_64_en-ru.tar.gz.
- iso_builder_image_host_path – путь к файлу iso-builder-6.0.0-200-x86_64_en-ru.tar.
- build_host_path – путь, где будет размещен смонтированный iso-образ без указания присваиваемого имени iso-образа.
- target_iso_name – присваиваемое имя iso-образу.

Порядок установки и настройки компонентов приложения

Установка и настройка приложения состоит из следующих этапов:

a. **Установка образа диска с компонентом Sandbox (см. раздел "Установка компонента Sandbox" на стр. 119)**

b. **Настройка компонента Sandbox через веб-интерфейс Sandbox (см. раздел "Работа с компонентом Sandbox через веб-интерфейс" на стр. 213)**

c. **Установка образов дисков операционных систем Microsoft Windows и приложений для работы компонента Sandbox (см. раздел "Установка и настройка образов операционных систем и приложений для работы компонента Sandbox" на стр. 221)**

d. **Установка компонентов Central Node и Sensor**

   Вы можете установить компоненты Central Node и Sensor в одной из следующих конфигураций:

   - Кластер (см. раздел "Развертывание компонентов Central Node и Sensor в виде кластера" на стр. 124).
   - Сервер (см. раздел "Установка компонентов Central Node и Sensor на сервере" на стр. 136).

   При наличии нескольких компонентов Central Node вы можете использовать приложение в режиме распределенного решения (см. раздел "Распределенное решение и мультитенантность" на стр. 75).

e. **Установка компонента Sensor (см. раздел "Установка компонента Sensor на отдельном сервере" на стр. 142)**

   При наличии нескольких компонентов Sensor вы можете установить и настроить компонент Sensor на необходимом количестве серверов.

f. **Настройка компонентов Central Node (см. раздел "Управление серверами Central Node, PCN или SCN с помощью веб-интерфейса приложения" на стр. 253) и Sensor (см. раздел "Управление компонентом Sensor" на стр. 260)**

g. **Установка компонента Endpoint Agent на компьютеры, входящие в IT-инфраструктуру организации**

   В качестве компонента Endpoint Agent вы можете использовать следующие приложения: Kaspersky Endpoint Agent для Windows, Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux, Kaspersky Endpoint Security для Mac.

Совместимость версий приложений, которыми представлен компонент Endpoint Agent, с версиями Kaspersky Anti Targeted Attack Platform см. в следующих разделах справки: Kaspersky Endpoint Agent для Windows (см. раздел "Совместимость версий Kaspersky Endpoint Agent для Windows с версиями Kaspersky Anti Targeted Attack Platform" на стр. 28), Kaspersky Endpoint Security для Windows (см. раздел "Совместимость версий Kaspersky Endpoint Security для Windows с версиями Kaspersky Anti Targeted Attack Platform" на стр. 33), Kaspersky Endpoint Security для Linux (см. раздел "Совместимость версий Kaspersky Endpoint Security для Linux с версиями Kaspersky Anti Targeted Attack Platform" на стр. 34), Kaspersky Endpoint Security для Mac (см. раздел "Совместимость Kaspersky Endpoint Security для Mac с версиями Kaspersky Anti Targeted Attack Platform" на стр. 35).

Приложение Kaspersky Endpoint Agent может использоваться в следующих конфигурациях:

- Без интеграции с приложением EPP.

  В этом случае вам требуется установить только приложение Kaspersky Endpoint Agent для Windows.

- В интеграции с приложением EPP.

  В этом случае Kaspersky Endpoint Agent также передает на сервер Central Node данные об угрозах, обнаруженных приложением EPP, и о результатах обработки угроз этой приложением.

Kaspersky Endpoint Agent для Windows может интегрироваться со следующими приложениями EPP (см. раздел «Совместимость версий Kaspersky Endpoint Agent для Windows с приложениями EPP» на стр. 30):

- Kaspersky Endpoint Security для Windows.

  Интеграция Kaspersky Endpoint Agent для Windows с Kaspersky Endpoint Security для Windows

Для интеграции приложений вам требуется установить Kaspersky Endpoint Agent в составе Kaspersky Endpoint Security. Возможность настроить интеграцию для отдельно установленных приложений не предусмотрена.

► *Чтобы установить Kaspersky Endpoint Agent в составе Kaspersky Endpoint Security:*

1. Запустите установку приложения Kaspersky Endpoint Security, в комплект поставки которой входит Kaspersky Endpoint Agent.

   Подробнее об установке Kaspersky Endpoint Security см. в *справке Kaspersky Endpoint Security для Windows*.

2. При установке выберите компонент Endpoint Agent.

После установки приложения с компонентом Endpoint Agent в список установленных приложений будут добавлены Kaspersky Endpoint Security и Kaspersky Endpoint Agent.

При необходимости вы можете обновить приложение Kaspersky Endpoint Agent, уже установленное в составе Kaspersky Endpoint Security. Интеграция между совместимыми версиями приложений сохранится как при обновлении приложения Kaspersky Endpoint Agent, так и при обновлении приложения Kaspersky Endpoint Security. Обновление с предыдущей версии Kaspersky Endpoint Agent доступно для Kaspersky Endpoint Agent версии 3.7 и выше.

- Kaspersky Security для Windows Server.

  Интеграция Kaspersky Endpoint Agent для Windows с Kaspersky Security для Windows Server

Для интеграции приложений вам требуется установить Kaspersky Endpoint Agent в составе Kaspersky Security для Windows Server. Возможность настроить интеграцию для отдельно установленных приложений не предусмотрена.

► *Чтобы установить Kaspersky Endpoint Agent в составе Kaspersky Security для Windows Server:*

1. Запустите установку приложения Kaspersky Security для Windows Server, в комплект поставки которого входит Kaspersky Endpoint Agent.

   Подробнее об установке Kaspersky Security для Windows Server см. в *справке Kaspersky Security для Windows Server* https://support.kaspersky.com/KSWS/11.0.1/ru-RU/147631.htm.

2. При установке выберите компонент Kaspersky Endpoint Agent.

После установки приложения с компонентом Kaspersky Endpoint Agent в список установленных приложений будут добавлены Kaspersky Security для Windows Server и Kaspersky Endpoint Agent.

При необходимости вы можете обновить приложение Kaspersky Endpoint Agent, уже установленное в составе Kaspersky Security для Windows Server. Интеграция между совместимыми версиями приложений сохранится как при обновлении приложения Kaspersky Endpoint Agent, так и при обновлении приложения Kaspersky Security для Windows Server.

- Kaspersky Security для виртуальных сред Легкий агент для Windows.

  Интеграция Kaspersky Endpoint Agent для Windows с Kaspersky Security для виртуальных сред Легкий агент

Kaspersky Endpoint Agent и Kaspersky Security для виртуальных сред Легкий агент устанавливаются отдельно. Установка Kaspersky Endpoint Agent в составе Kaspersky Security для виртуальных сред Легкий агент не предусмотрена.

► *Чтобы включить интеграцию Kaspersky Endpoint Agent в составе Kaspersky Security для виртуальных сред Легкий агент:*

1. Установите приложение Kaspersky Security для виртуальных сред Легкий агент, если оно не было установлено ранее.
2. Включите интеграцию Легкого агента с Kaspersky Endpoint Agent.

Вы можете включить интеграцию с Kaspersky Endpoint Agent во время установки или обновления Легкого агента. Вы также можете включить интеграцию с Kaspersky Endpoint Agent с помощью процедуры изменения состава установленных компонентов Легкого агента.

3. На виртуальную машину с установленным Легким агентом установите приложение Kaspersky Endpoint Agent, если оно не было установлено ранее.

► *Чтобы включить интеграцию Kaspersky Endpoint Agent с Kaspersky Industrial CyberSecurity for Nodes:*

1. Установите приложение Kaspersky Industrial CyberSecurity for Nodes, если оно не было установлено ранее. Подробнее об установке см. в справке Kaspersky Industrial CyberSecurity for Nodes.
2. Установите на том же устройстве приложение Kaspersky Endpoint Agent, если оно не было установлено ранее. Приложения интегрируются автоматически.

Для интеграции с Kaspersky Industrial CyberSecurity for Nodes в Kaspersky Endpoint Agent должен быть установлен соответствующий лицензионный ключ.

Для получения детальной информации вы можете обратиться к вашему аккаунт-менеджеру.

Совместимость версий приложения Kaspersky Endpoint Agent для Windows с приложениями EPP см. в разделе Совместимость версий Kaspersky Endpoint Agent для Windows с приложениями EPP (на стр. 30).

Подробнее об установке Kaspersky Endpoint Security см. в справке соответствующего приложения:

- Установка Kaspersky Endpoint Security для Windows
- Установка Kaspersky Endpoint Security для Linux
- Установка Kaspersky Endpoint Security для Mac

Если на хостах установлены более ранние версии приложений, вы можете обновить их.

Установка компонента Sandbox

Этот раздел представляет собой пошаговую инструкцию по установке компонента Sandbox.

► *Чтобы приступить к установке компонента Sandbox, выполните следующие действия:*

1. Запустите образ диска с компонентом Sandbox.

   Запустится мастер установки.
2. Нажмите на кнопку **Ok**.

В этом разделе

Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности 120

Шаг 2. Выбор диска для установки компонента Sandbox 121

Шаг 3. Назначение имени хоста 121

Шаг 4. Выбор управляющего сетевого интерфейса в списке 121

Шаг 5. Назначение адреса и маски сети управляющего интерфейса 122

Шаг 6. Добавление адресов DNS-серверов 122

Шаг 7. Настройка статического сетевого маршрута 122

Шаг 8. Настройка минимальной длины пароля администратора Sandbox 123

Шаг 9. Создание учетной записи администратора Sandbox 123

Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности

Для продолжения установки вам нужно ознакомиться с Лицензионным соглашением и принять его условия. Если условия Лицензионного соглашения не приняты, установка не выполняется.

Также вам нужно ознакомиться с Политикой конфиденциальности и принять ее условия. Если Политика конфиденциальности не принята, установка не выполняется.

► *Чтобы принять условия Лицензионного соглашения и Политики конфиденциальности при установке компонента Sandbox на базе операционной системы CentOS:*

1. Выберите язык для просмотра Лицензионного соглашения и Политики конфиденциальности в списке.

   Например, если вы хотите просмотреть Лицензионное соглашение и Политику конфиденциальности на английском языке, выберите **English** и нажмите на клавишу **ENTER**.

   Откроется окно с текстом Лицензионного соглашения.
2. Ознакомьтесь с Лицензионным соглашением.
3. Если вы принимаете условия Лицензионного соглашения, нажмите на кнопку **I accept**.

   Откроется окно с текстом Политики конфиденциальности.
4. Ознакомьтесь с Политикой конфиденциальности.
5. Если вы принимаете условия Политики конфиденциальности, нажмите на кнопку **I accept**.

Мастер установки перейдет к следующему шагу.

► *Чтобы принять условия Лицензионного соглашения и Политики конфиденциальности при установке компонента Sandbox на базе операционной системы Astra Linux:*

1. Выберите язык для просмотра Лицензионного соглашения и Политики конфиденциальности в списке, нажав на клавишу **F1**.

   Например, если вы хотите просмотреть Лицензионное соглашение и Политику конфиденциальности на английском языке, выберите **English** и нажмите на клавишу **ENTER**.

   Откроется окно с текстом Лицензионного соглашения на использование операционных систем Astra Linux.
2. Ознакомьтесь с Лицензионным соглашением на использование операционных систем Astra Linux.
3. Если вы принимаете условия Лицензионного соглашения на использование операционных систем Astra Linux, нажмите на кнопку **Yes**.

   Откроется окно с текстом Лицензионного соглашения АО "Лаборатория Касперского".
4. Ознакомьтесь с Лицензионным соглашением АО "Лаборатория Касперского".
5. Если вы принимаете условия Лицензионного соглашения, нажмите на кнопку **Yes**.

   Откроется окно с текстом Политики конфиденциальности.
6. Ознакомьтесь с Политикой конфиденциальности.
7. Если вы принимаете условия Политики конфиденциальности, нажмите на кнопку **Yes**.

Мастер установки перейдет к следующему шагу.

Шаг 2. Выбор диска для установки компонента Sandbox

Выберите физический диск для установки компонента Sandbox.

► *Чтобы выбрать диск для установки компонента Sandbox:*

1. В окне **Select device** в списке дисков выберите диск для установки компонента Sandbox и нажмите на клавишу **ENTER**.

   Если диск не пустой, отобразится окно подтверждения форматирования этого диска и установки приложения на него.

2. Нажмите на кнопку **Install**.

   Архив с установочными файлами распакуется на диск. Сервер перезагрузится.

Мастер установки перейдет к следующему шагу.

Шаг 3. Назначение имени хоста

Назначьте имя хоста сервера для использования DNS-серверами.

► *Чтобы назначить имя хоста сервера:*

1. В поле **Hostname** введите полное доменное имя сервера.

   Указывайте имя сервера в формате FQDN (например, host.domain.com или host.domain.subdomain.com).

2. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 4. Выбор управляющего сетевого интерфейса в списке

Для работы компонента Sandbox необходимо подключить минимум две сетевые карты и настроить следующие сетевые интерфейсы:

- Управляющий сетевой интерфейс. Этот интерфейс предназначен для доступа к серверу с компонентом Sandbox по протоколу SSH, а также через этот интерфейс сервер с компонентом Sandbox будет принимать объекты с сервера с компонентом Central Node.
- Сетевой интерфейс для доступа обрабатываемых объектов в интернет. Через этот интерфейс объекты, которые обрабатывает компонент Sandbox, смогут предпринимать попытки действий в интернете, а компонент Sandbox сможет анализировать их поведение. Если вы запретите доступ в интернет, компонент Sandbox не сможет анализировать поведение объектов в интернете, и будет анализировать поведение объектов без доступа в интернет.

  Сетевой интерфейс для доступа обрабатываемых объектов в интернет должен быть изолирован от локальной сети вашей организации.

Выберите сетевой интерфейс, который вы хотите использовать в качестве управляющего.

► *Чтобы выбрать управляющий сетевой интерфейс:*

1. В списке сетевых интерфейсов выберите сетевой интерфейс, который вы хотите использовать в качестве управляющего.
2. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 5. Назначение адреса и маски сети управляющего интерфейса

► *Чтобы назначить IP-адрес и маску сети управляющего сетевого интерфейса:*

1. В поле **Address** введите IP-адрес, который вы хотите назначить этому сетевому интерфейсу.
2. В поле **Netmask** введите маску сети, в которой вы хотите использовать этот сетевой интерфейс.
3. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 6. Добавление адресов DNS-серверов

► *Чтобы добавить адреса DNS-серверов:*

1. В окне **DNS servers** выберите **New** и нажмите на клавишу **ENTER**.

   Откроется окно ввода адреса DNS-сервера.
2. В поле **DNS server** введите IP-адрес основного DNS-сервера в формате IPv4.
3. Нажмите на кнопку **Ok**.

   Окно ввода адреса DNS-сервера закроется.
4. Если вы хотите добавить IP-адрес дополнительного DNS-сервера, повторите действия в окне **DNS servers**.
5. Когда вы добавите все DNS-серверы, в окне **DNS servers** выберите **Continue** и нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 7. Настройка статического сетевого маршрута

► *Чтобы настроить статический сетевой маршрут:*

1. В окне **IPv4 Routes** выберите **New** и нажмите на клавишу **ENTER**.

   Откроется окно **IPv4 Static Route**.
2. В поле **Address/Mask** введите IP-адрес и маску подсети, для которой вы хотите настроить сетевой маршрут.
3. Если вы хотите использовать сетевой маршрут по умолчанию, введите 0.0.0.0/0.
4. В поле **Gateway** введите IP-адрес шлюза.

5. Нажмите на кнопку **Ok**.
6. Если вы хотите добавить другие сетевые маршруты, повторите действия в окне **IPv4 Static Route**.
7. Когда вы закончите добавлять сетевые маршруты, нажмите на кнопку **Continue**.

Мастер установки перейдет к следующему шагу.

Шаг 8. Настройка минимальной длины пароля администратора Sandbox

► *Чтобы задать минимальную длину пароля администратора компонента Sandbox:*

1. В поле **Minimal length** введите количество символов. Рекомендуется использовать пароли длиной 12 и более символов.
2. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 9. Создание учетной записи администратора Sandbox

Создайте учетную запись администратора для работы в веб-интерфейсе Sandbox, в меню администратора и в консоли управления сервером с компонентом Sandbox.

► *Чтобы создать учетную запись администратора Sandbox:*

1. В поле **Username** введите имя учетной записи администратора. По умолчанию используется учетная запись admin.
2. В поле **Password** введите пароль учетной записи администратора.

   Пароль должен удовлетворять следующим требованиям:

   - должен содержать минимум 8 символов;
   - должен содержать символы минимум трех типов:
     - символ верхнего регистра (A-Z);
     - символ нижнего регистра (a-z);
     - цифру;
     - специальный символ;
   - не должен совпадать с именем пользователя.
3. В поле **Confirm password** введите пароль повторно.
4. Нажмите на кнопку **Ok**.

   Откроется окно с IP-адресом сервера Sandbox. По этому адресу вы можете открыть веб-интерфейс Sandbox в браузере. Для входа используйте созданную учетную запись администратора Sandbox.

   Сервер Sandbox перезагрузится.

Перейдите к настройке компонента Sandbox через веб-интерфейс (см. раздел "Работа с компонентом Sandbox через веб-интерфейс" на стр. 213).

Развертывание компонентов Central Node и Sensor в виде кластера

Развертывание компонентов Central Node и Sensor в виде кластера включает следующие этапы:

a. **Развертывание первого сервера хранения (см. раздел "Развертывание сервера хранения данных" на стр. 124)**

   Первым требуется развернуть сервер хранения. После того, как он будет развернут, вы можете добавить в кластер дополнительные серверы хранения и обрабатывающие серверы.

   > Кластер должен включать минимум 4 сервера: 2 сервера хранения и 2 обрабатывающих сервера. Чтобы определить подходящее для вашей организации количество серверов, вы можете воспользоваться Руководством по масштабированию (см. раздел "Расчеты для компонента Central Node" на стр. 97).

b. **Развертывание обрабатывающих серверов (см. раздел "Развертывание обрабатывающего сервера" на стр. 131) и дополнительных серверов хранения (см. раздел "Развертывание сервера хранения данных" на стр. 124)**

   Вы можете разворачивать серверы в произвольном порядке.

c. **Настройка параметров масштабирования приложения**

   На завершающем этапе развертывания кластера вам нужно настроить параметры масштабирования приложения: указать планируемый объем SPAN-трафика, почтового трафика, количество хостов с компонентом Endpoint Agent, а также размер Хранилища и базы событий.

> Компонент Central Node всегда устанавливается вместе с компонентом Sensor. Если вам требуется использовать компонент Central Node отдельно, при развертывании обрабатывающего сервера откажитесь от получения зеркалированного трафика со SPAN-портов на шаге 11 (см. раздел "Шаг 11. Настройка получения зеркалированного трафика со SPAN-портов" на стр. 135).

В этом разделе

Развертывание сервера хранения данных 124

Развертывание обрабатывающего сервера 131

Развертывание сервера хранения данных

Для развертывания сервера хранения данных вам нужно запустить образ диска с компонентами Central Node и Sensor.

Если при выполнении шагов мастера установки возникла ошибка, обратитесь в Службу технической поддержки (см. раздел "Обращение в Службу технической поддержки" на стр. 670).

Шаг 1. Выбор роли сервера

► *Чтобы выбрать роль сервера:*

1. Выберите один из следующих вариантов:
   - **storage**.

     Эта роль предполагает установку сервера хранения для развертывания компонента Central Node в виде кластера.
   - **processing**.

     Эта роль предполагает установку обрабатывающего сервера для развертывания компонента Central Node в виде кластера.

     Роль включает также установку и настройку компонента Sensor.
   - **single**.

     Эта роль предполагает установку компонентов Central Node и Sensor на одном сервере.
   - **sensor**.

     Эта роль предполагает установку компонента Sensor на отдельном сервере.
2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 2. Выбор режима развертывания

► *Чтобы выбрать режим развертывания:*

1. Выберите один из следующих вариантов:
   - **First node installation**.

     Это значение нужно выбрать при развертывании первого сервера кластера.
   - **Add extra node to the cluster**.

     Это значение нужно выбрать при развертывании сервера, который будет добавлен в существующий кластер.
2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 3. Выбор диска для установки компонента

► *Чтобы выбрать диск для установки компонента:*

1. Выберите один из предложенных дисков для установки компонента и нажмите на клавишу **Enter**.

   Отобразится окно подтверждения.

2. Выберите **Yes** и нажмите на клавишу **Enter.**

Мастер установки перейдет к следующему шагу.

Шаг 4. Просмотр Лицензионного соглашения и Политики конфиденциальности

Для продолжения установки вам нужно ознакомиться с Лицензионным соглашением и Политикой конфиденциальности и принять их условия. Если условия Лицензионного соглашения и Политики конфиденциальности не приняты, установка не выполняется.

► *Чтобы принять условия Лицензионного соглашения и Политики конфиденциальности при установке компонентов на базе операционной системы Astra Linux:*

1. Выберите язык для просмотра Лицензионного соглашения и Политики конфиденциальности в списке, нажав на клавишу **F1**.

   Например, если вы хотите просмотреть Лицензионное соглашение и Политику конфиденциальности на английском языке, выберите **English** и нажмите на клавишу **ENTER**.

   Откроется окно с текстом Лицензионного соглашения на использование операционных систем Astra Linux.

2. Ознакомьтесь с Лицензионным соглашением на использование операционных систем Astra Linux.
3. Если вы принимаете условия Лицензионного соглашения на использование операционных систем Astra Linux, нажмите на кнопку **Yes**.

   Откроется окно с текстом Лицензионного соглашения АО "Лаборатория Касперского".

4. Ознакомьтесь с Лицензионным соглашением АО "Лаборатория Касперского".
5. Если вы принимаете условия Лицензионного соглашения, нажмите на кнопку **Yes**.

   Откроется окно с текстом Политики конфиденциальности.

6. Ознакомьтесь с Политикой конфиденциальности.
7. Если вы принимаете условия Политики конфиденциальности, нажмите на кнопку **Yes**.

Мастер установки перейдет к следующему шагу.

Шаг 5. Выбор маски сети для адресации серверов кластера

Рекомендуется использовать значения по умолчанию.
Маска сети не должна совпадать с используемыми в инфраструктуре организации масками сети.

► *Чтобы указать маску сети для адресации серверов кластера:*

- Если вы хотите использовать предустановленное значение для маски сети, нажмите на клавишу **Enter**.

  Значение по умолчанию: 198.18.0.0/16.

- Если вы хотите указать другую маску сети, введите значение и нажмите на клавишу **Enter**.

  Маска должна соответствовать шаблону x.x.0.0/16.

Мастер установки перейдет к следующему шагу.

Шаг 6. Выбор маски сети для адресации компонентов приложения

На этом шаге вам нужно указать маску сети для адресации основных компонентов приложения, которые будут функционировать на серверах с компонентом Central Node.

Сеть для адресации компонентов приложения не должна пересекаться с сетью для адресации серверов кластера.

► *Чтобы указать маску сети для адресации основных компонентов приложения:*

- Если вы хотите использовать предустановленное значение для маски сети, нажмите на клавишу **Enter**.

  Значение по умолчанию: 198.19.0.0/16.

- Если вы хотите указать другую маску сети, введите значение и нажмите на клавишу **Enter**.

  Маска должна соответствовать шаблону x.x.0.0/16.

Мастер установки перейдет к следующему шагу.

Шаг 7. Выбор кластерного сетевого интерфейса

Кластерный сетевой интерфейс используется для взаимодействия между серверами кластера.

► *Чтобы выбрать кластерный сетевой интерфейс:*

1. Выберите строку с сетевым интерфейсом, который используется для внутренней сети.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 8. Выбор внешнего сетевого интерфейса

Внешний сетевой интерфейс используется для доступа к серверу по протоколу SSH, работы в веб-интерфейсе Kaspersky Anti Targeted Attack Platform и других внешних подключений.

► *Чтобы выбрать внешний сетевой интерфейс:*

1. Выберите строку с сетевым интерфейсом, который используется для внешней сети.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 9. Выбор способа получения IP-адресов для сетевых интерфейсов

► *Чтобы выбрать способ получения IP-адреса для сетевых интерфейсов:*

1. Выберите строку **Configuration type:** и нажмите на клавишу **Enter**.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. В открывшемся окне выберите один из следующих вариантов:
   - **dhcp**.
   - **static**.
3. Если вы выбрали **static**, выполните следующие действия:
   a. Выберите строку с параметром и нажмите на клавишу **Enter**.
   b. В открывшемся окне введите требуемые данные и дважды нажмите на клавишу **Enter**.

   Вам нужно указать значение для каждого параметра.

4. Выберите строку **Save**.
5. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 10. Создание учетной записи администратора и аутентификация сервера в кластере

На этом шаге вам нужно выполнить одно из следующих действий:

- Создать учетную запись администратора (см. раздел "Создание учетной записи администратора" на стр. 129), если вы разворачиваете первый сервер кластера.
- Аутентифицировать сервер в кластере (см. раздел "Аутентификация сервера в кластере" на стр. 129), если вы разворачиваете дополнительные серверы хранения.

Создание учетной записи администратора

Создание учетной записи администратора требуется только при развертывании первого сервера кластера. Если вы разворачиваете дополнительный сервер хранения, вместо окна для создания учетной записи администратора приложение предлагает аутентифицировать сервер в кластере (см. раздел "Аутентификация сервера в кластере" на стр. 129).

При развертывании первого сервера кластера вам нужно создать учетную запись администратора. Эта учетная запись используется для работы в веб-интерфейсе для управления масштабированием (см. раздел "Начало работы в веб-интерфейсе для управления масштабированием" на стр. 187), меню администратора приложения и для работы с приложением в режиме Technical Support Mode.

По умолчанию в качестве имени пользователя для учетной записи администратора используется *admin*. Вам требуется задать пароль для этой учетной записи.

► *Чтобы задать пароль для учетной записи администратора:*

1. В поле **password** введите пароль учетной записи администратора.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. В поле **confirm** введите пароль повторно.
3. Выберите кнопку **Ok** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Аутентификация сервера в кластере

Аутентификация сервера в кластере требуется только при развертывании дополнительных серверов хранения. Если вы разворачиваете первый сервер кластера, вместо аутентификации сервера приложение предлагает создать учетную запись администратора (см. раздел "Шаг 10. Создание учетной записи администратора и аутентификация сервера в кластере" на стр. 128).

Для аутентификации сервера в кластере вам нужно ввести пароль для учетной записи admin (см. раздел "Шаг 10. Создание учетной записи администратора и аутентификация сервера в кластере" на стр. 128), заданный при развертывании первого сервера кластера.

► *Чтобы аутентифицировать сервер в кластере:*

1. В поле **password** введите пароль учетной записи администратора.
2. Выберите кнопку **Ok** и нажмите на клавишу **Enter**.

   Для выбора кнопки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown.

Сервер кластера будет аутентифицирован. Мастер установки перейдет к следующему шагу.

Шаг 11. Добавление адресов DNS-серверов

Настройте параметры DNS для работы серверов с компонентами приложения.

► *Чтобы добавить адреса DNS-серверов:*

1. Введите IP-адрес основного DNS-сервера в формате IPv4.

   Вам требуется ввести хотя бы один адрес DNS-сервера.

2. Если вы хотите добавить IP-адрес дополнительного DNS-сервера, нажмите на клавишу **Enter** и введите адрес сервера.
3. Когда вы добавите все DNS-серверы, дважды нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 12. Выбор дисков для Ceph-хранилища

Выберите диски для Ceph-хранилища. Количество дисков определяется в соответствии с руководством по масштабированию.

► *Чтобы выбрать диски для Ceph-хранилища:*

1. Выберите строку с требуемым диском.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. Нажмите на клавишу **Enter**.
3. Повторите шаги 1–2 для выбора следующих дисков.

Настройка займет какое-то время. После этого установка завершится. Вы можете перейти к настройке конфигурации серверов кластера в веб-интерфейсе для управления масштабированием (см. раздел "Начало работы в веб-интерфейсе для управления масштабированием" на стр. 187).

kaspersky

Развертывание обрабатывающего сервера

Для развертывания обрабатывающего сервера вам нужно запустить образ диска с компонентами Central Node и Sensor.

Если при выполнении шагов мастера установки возникла ошибка, обратитесь в Службу технической поддержки (см. раздел "Обращение в Службу технической поддержки" на стр. 670).

В этом разделе

Шаг 1. Выбор роли сервера 131
Шаг 2. Выбор режима развертывания 132
Шаг 3. Выбор диска для установки компонента 132
Шаг 4. Просмотр Лицензионного соглашения и Политики конфиденциальности 132
Шаг 5. Выбор маски сети для адресации серверов кластера 133
Шаг 6. Выбор маски сети для адресации компонентов приложения 133
Шаг 7. Выбор кластерного сетевого интерфейса 134
Шаг 8. Выбор внешнего сетевого интерфейса 134
Шаг 9. Выбор способа получения IP-адресов для сетевых интерфейсов 134
Шаг 10. Аутентификация сервера в кластере 135
Шаг 11. Настройка получения зеркалированного трафика со SPAN-портов 135
Шаг 12. Добавление адресов DNS-серверов 135

Шаг 1. Выбор роли сервера

► *Чтобы выбрать роль сервера:*

1. Выберите один из следующих вариантов:
   - **storage**.

     Эта роль предполагает установку сервера хранения для развертывания компонента Central Node в виде кластера.
   - **processing**.

     Эта роль предполагает установку обрабатывающего сервера для развертывания компонента Central Node в виде кластера.

     Роль включает также установку и настройку компонента Sensor.

- **single**.

  Эта роль предполагает установку компонентов Central Node и Sensor на одном сервере.

- **sensor**.

  Эта роль предполагает установку компонента Sensor на отдельном сервере.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 2. Выбор режима развертывания

► *Чтобы выбрать режим развертывания:*

1. Выберите один из следующих вариантов:
   - **First node installation**.

     Это значение нужно выбрать при развертывании первого сервера кластера.

   - **Add extra node to the cluster**.

     Это значение нужно выбрать при развертывании сервера, который будет добавлен в существующий кластер.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 3. Выбор диска для установки компонента

► *Чтобы выбрать диск для установки компонента:*

1. Выберите один из предложенных дисков для установки компонента и нажмите на клавишу **Enter**.

   Отобразится окно подтверждения.

2. Выберите **Yes** и нажмите на клавишу **Enter.**

Мастер установки перейдет к следующему шагу.

Шаг 4. Просмотр Лицензионного соглашения и Политики конфиденциальности

Для продолжения установки вам нужно ознакомиться с Лицензионным соглашением и Политикой конфиденциальности и принять их условия. Если условия Лицензионного соглашения и Политики конфиденциальности не приняты, установка не выполняется.

► *Чтобы принять условия Лицензионного соглашения и Политики конфиденциальности при установке компонентов на базе операционной системы Astra Linux:*

1. Выберите язык для просмотра Лицензионного соглашения и Политики конфиденциальности в списке, нажав на клавишу **F1**.

   Например, если вы хотите просмотреть Лицензионное соглашение и Политику конфиденциальности на английском языке, выберите **English** и нажмите на клавишу **ENTER**.

Откроется окно с текстом Лицензионного соглашения на использование операционных систем Astra Linux.

2. Ознакомьтесь с Лицензионным соглашением на использование операционных систем Astra Linux.
3. Если вы принимаете условия Лицензионного соглашения на использование операционных систем Astra Linux, нажмите на кнопку **Yes**.

   Откроется окно с текстом Лицензионного соглашения АО "Лаборатория Касперского".
4. Ознакомьтесь с Лицензионным соглашением АО "Лаборатория Касперского".
5. Если вы принимаете условия Лицензионного соглашения, нажмите на кнопку **Yes**.

   Откроется окно с текстом Политики конфиденциальности.
6. Ознакомьтесь с Политикой конфиденциальности.
7. Если вы принимаете условия Политики конфиденциальности, нажмите на кнопку **Yes**.

Мастер установки перейдет к следующему шагу.

Шаг 5. Выбор маски сети для адресации серверов кластера

Рекомендуется использовать значения по умолчанию.
Маска сети не должна совпадать с используемыми в инфраструктуре организации масками сети.

► *Чтобы указать маску сети для адресации серверов кластера:*

- Если вы хотите использовать предустановленное значение для маски сети, нажмите на клавишу **Enter**.

  Значение по умолчанию: 198.18.0.0/16.
- Если вы хотите указать другую маску сети, введите значение и нажмите на клавишу **Enter**.

  Маска должна соответствовать шаблону x.x.0.0/16.

Мастер установки перейдет к следующему шагу.

Шаг 6. Выбор маски сети для адресации компонентов приложения

На этом шаге вам нужно указать маску сети для адресации основных компонентов приложения, которые будут функционировать на серверах с компонентом Central Node.

Сеть для адресации компонентов приложения не должна пересекаться с сетью для адресации серверов кластера.

► *Чтобы указать маску сети для адресации основных компонентов приложения:*

- Если вы хотите использовать предустановленное значение для маски сети, нажмите на клавишу **Enter**.

  Значение по умолчанию: 198.19.0.0/16.

- Если вы хотите указать другую маску сети, введите значение и нажмите на клавишу **Enter**.

  Маска должна соответствовать шаблону x.x.0.0/16.

Мастер установки перейдет к следующему шагу.

Шаг 7. Выбор кластерного сетевого интерфейса

Кластерный сетевой интерфейс используется для взаимодействия между серверами кластера.

► *Чтобы выбрать кластерный сетевой интерфейс:*

1. Выберите строку с сетевым интерфейсом, который используется для внутренней сети.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 8. Выбор внешнего сетевого интерфейса

Внешний сетевой интерфейс используется для доступа к серверу по протоколу SSH, работы в веб-интерфейсе Kaspersky Anti Targeted Attack Platform и других внешних подключений.

► *Чтобы выбрать внешний сетевой интерфейс:*

1. Выберите строку с сетевым интерфейсом, который используется для внешней сети.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 9. Выбор способа получения IP-адресов для сетевых интерфейсов

► *Чтобы выбрать способ получения IP-адреса для сетевых интерфейсов:*

1. Выберите строку **Configuration type:** и нажмите на клавишу **Enter**.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. В открывшемся окне выберите один из следующих вариантов:
   - **dhcp**.
   - **static**.
3. Если вы выбрали **static**, выполните следующие действия:
   a. Выберите строку с параметром и нажмите на клавишу **Enter**.
   b. В открывшемся окне введите требуемые данные и дважды нажмите на клавишу **Enter**.

Вам нужно указать значение для каждого параметра.

4. Выберите строку **Save**.
5. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 10. Аутентификация сервера в кластере

Для аутентификации сервера в кластере вам нужно ввести пароль для учетной записи admin (см. раздел "Шаг 10. Создание учетной записи администратора и аутентификация сервера в кластере" на стр. 128), заданный при развертывании первого сервера кластера.

► *Чтобы аутентифицировать сервер в кластере:*

1. В поле **password** введите пароль учетной записи администратора.
2. Выберите кнопку **Ok** и нажмите на клавишу **Enter**.

   Для выбора кнопки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown.

Сервер кластера будет аутентифицирован. Мастер установки перейдет к следующему шагу.

Шаг 11. Настройка получения зеркалированного трафика со SPAN-портов

► *Чтобы включить получение зеркалированного трафика со SPAN-портов:*

1. Введите **y**.
2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

► *Чтобы отказаться от получения зеркалированного трафика со SPAN-портов:*

1. Введите **n**.
2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 12. Добавление адресов DNS-серверов

Настройте параметры DNS для работы серверов с компонентами приложения.

► *Чтобы добавить адреса DNS-серверов:*

1. Введите IP-адрес основного DNS-сервера в формате IPv4.

   Вам требуется ввести хотя бы один адрес DNS-сервера.

2. Если вы хотите добавить IP-адрес дополнительного DNS-сервера, нажмите на клавишу **Enter** и введите адрес сервера.
3. Когда вы добавите все DNS-серверы, дважды нажмите на клавишу **Enter**.

Установка завершится. Вы можете перейти к настройке конфигурации серверов кластера в веб-интерфейсе для управления масштабированием (см. раздел "Начало работы в веб-интерфейсе для управления масштабированием" на стр. 187).

Установка компонентов Central Node и Sensor на сервере

Развертывание компонентов Central Node и Sensor на одном сервере включает следующие этапы:

a. **Установка компонентов Central Node и Sensor**

Для установки компонентов на физическом сервере вам нужно запустить образ диска с компонентами Central Node и Sensor.

Для установки компонентов на виртуальном сервере вам нужно подключить образ диска с компонентами Central Node и Sensor к выбранной виртуальной машине и запустить ее. Установка запускается сразу после включения виртуальной машины. Вы можете управлять процессом установки с помощью консоли виртуальной машины.

b. **Настройка параметров масштабирования приложения**

На завершающем этапе развертывания кластера вам нужно настроить параметры масштабирования приложения: указать планируемый объем SPAN-трафика, почтового трафика, количество хостов с компонентом Endpoint Agent, а также размер Хранилища и базы событий.

Компонент Central Node всегда устанавливается вместе с компонентом Sensor. Если вам требуется использовать компонент Central Node отдельно, откажитесь от получения зеркалированного трафика со SPAN-портов на шаге 10.
Если при выполнении шагов мастера установки возникла ошибка, обратитесь в Службу технической поддержки (см. раздел "Обращение в Службу технической поддержки" на стр. 670).

kaspersky

В этом разделе

Шаг 1. Выбор роли сервера 137
Шаг 2. Просмотр Лицензионного соглашения и Политики конфиденциальности 138
Шаг 3. Выбор диска для установки компонента 138
Шаг 4. Выделение диска для базы данных компонента Targeted Attack Analyzer 138
Шаг 5. Выбор маски сети для адресации серверов кластера 139
Шаг 6. Выбор внешнего сетевого интерфейса 139
Шаг 7. Выбор способа получения IP-адресов для сетевых интерфейсов 140
Шаг 8. Создание учетной записи администратора 140
Шаг 9. Добавление адресов DNS-серверов 140
Шаг 10. Настройка получения зеркалированного трафика со SPAN-портов 141
Шаг 11. Настройка синхронизации времени с NTP-сервером 141

Шаг 1. Выбор роли сервера

► *Чтобы выбрать роль сервера:*

1. Выберите один из следующих вариантов:
   - **storage**.

     Эта роль предполагает установку сервера хранения для развертывания компонента Central Node в виде кластера.
   - **processing**.

     Эта роль предполагает установку обрабатывающего сервера для развертывания компонента Central Node в виде кластера.

     Роль включает также установку и настройку компонента Sensor.
   - **single**.

     Эта роль предполагает установку компонентов Central Node и Sensor на одном сервере.
   - **sensor**.

     Эта роль предполагает установку компонента Sensor на отдельном сервере.
2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 2. Просмотр Лицензионного соглашения и Политики конфиденциальности

Для продолжения установки вам нужно ознакомиться с Лицензионным соглашением и Политикой конфиденциальности и принять их условия. Если условия Лицензионного соглашения и Политики конфиденциальности не приняты, установка не выполняется.

► *Чтобы принять условия Лицензионного соглашения и Политики конфиденциальности при установке компонентов на базе операционной системы Astra Linux:*

1. Выберите язык для просмотра Лицензионного соглашения и Политики конфиденциальности в списке, нажав на клавишу **F1**.

   Например, если вы хотите просмотреть Лицензионное соглашение и Политику конфиденциальности на английском языке, выберите **English** и нажмите на клавишу **ENTER**.

   Откроется окно с текстом Лицензионного соглашения на использование операционных систем Astra Linux.
2. Ознакомьтесь с Лицензионным соглашением на использование операционных систем Astra Linux.
3. Если вы принимаете условия Лицензионного соглашения на использование операционных систем Astra Linux, нажмите на кнопку **Yes**.

   Откроется окно с текстом Лицензионного соглашения АО "Лаборатория Касперского".
4. Ознакомьтесь с Лицензионным соглашением АО "Лаборатория Касперского".
5. Если вы принимаете условия Лицензионного соглашения, нажмите на кнопку **Yes**.

   Откроется окно с текстом Политики конфиденциальности.
6. Ознакомьтесь с Политикой конфиденциальности.
7. Если вы принимаете условия Политики конфиденциальности, нажмите на кнопку **Yes**.

Мастер установки перейдет к следующему шагу.

Шаг 3. Выбор диска для установки компонента

► *Чтобы выбрать диск для установки компонента:*

1. Выберите один из предложенных дисков для установки компонента и нажмите на клавишу **Enter**.

   Отобразится окно подтверждения..
2. Выберите **Yes** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 4. Выделение диска для базы данных компонента Targeted Attack Analyzer

Для оптимальной работы компонента Targeted Attack Analyzer рекомендуется выделить на сервере физический диск объемом не менее 1 ТБ для базы данных компонента.

На этом шаге вы можете выделить физический диск для базы данных компонента Targeted Attack Analyzer или отказаться от выделения физического диска.

► *Чтобы выделить диск для базы данных компонента Targeted Attack Analyzer:*

1. Выберите один из предложенных дисков для базы данных компонента Targeted Attack Analyzer.

   Если вам не требуется база данных компонента Targeted Attack Analyzer, выберите строку **Don't want TAA.**

   Отобразится окно подтверждения.

2. Выберите **Yes** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 5. Выбор маски сети для адресации серверов кластера

Рекомендуется использовать значения по умолчанию.
Маска сети не должна совпадать с используемыми в инфраструктуре организации масками сети.

► *Чтобы указать маску сети для адресации серверов кластера:*

- Если вы хотите использовать предустановленное значение для маски сети, нажмите на клавишу **Enter**.

  Значение по умолчанию: 198.18.0.0/16.

- Если вы хотите указать другую маску сети, введите значение и нажмите на клавишу **Enter**.

  Маска должна соответствовать шаблону x.x.0.0/16.

Мастер установки перейдет к следующему шагу.

Шаг 6. Выбор внешнего сетевого интерфейса

Внешний сетевой интерфейс используется для доступа к серверу по протоколу SSH, работы в веб-интерфейсе Kaspersky Anti Targeted Attack Platform и других внешних подключений.

► *Чтобы выбрать внешний сетевой интерфейс:*

1. Выберите строку с сетевым интерфейсом, который используется для внешней сети.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 7. Выбор способа получения IP-адресов для сетевых интерфейсов

► *Чтобы выбрать способ получения IP-адреса для сетевых интерфейсов:*

1. Выберите строку **Configuration type:** и нажмите на клавишу **Enter**.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. В открывшемся окне выберите один из следующих вариантов:
   - **dhcp**.
   - **static**.
3. Если вы выбрали **static**, выполните следующие действия:
   a. Выберите строку с параметром и нажмите на клавишу **Enter**.
   b. В открывшемся окне введите требуемые данные и дважды нажмите на клавишу **Enter**.

   Вам нужно указать значение для каждого параметра.

4. Выберите строку **Save**.
5. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 8. Создание учетной записи администратора

Учетная запись администратора используется для работы в веб-интерфейсе для управления масштабированием (см. раздел "Начало работы в веб-интерфейсе для управления масштабированием" на стр. 187), меню администратора приложения и для работы с приложением в режиме Technical Support Mode.

По умолчанию в качестве имени пользователя для учетной записи администратора используется *admin*. Вам требуется задать пароль для этой учетной записи.

► *Чтобы задать пароль для учетной записи администратора:*

1. В поле **password** введите пароль учетной записи администратора.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. В поле **confirm** введите пароль повторно.
3. Выберите кнопку **Ok** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 9. Добавление адресов DNS-серверов

Настройте параметры DNS для работы серверов с компонентами приложения.

► *Чтобы добавить адреса DNS-серверов:*

1. Введите IP-адрес основного DNS-сервера в формате IPv4.

   Вам требуется ввести хотя бы один адрес DNS-сервера.

2. Если вы хотите добавить IP-адрес дополнительного DNS-сервера, нажмите на клавишу **Enter** и введите адрес сервера.
3. Когда вы добавите все DNS-серверы, дважды нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 10. Настройка получения зеркалированного трафика со SPAN-портов

На этом шаге вы можете настроить получение зеркалированного трафика со SPAN-портов.

► *Чтобы включить получение зеркалированного трафика со SPAN-портов:*

1. Введите **y**.
2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

► *Чтобы отказаться от получения зеркалированного трафика со SPAN-портов:*

1. Введите **n**.
2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 11. Настройка синхронизации времени с NTP-сервером

Настройте синхронизацию времени сервера с NTP-сервером.

► *Чтобы настроить синхронизацию времени с NTP-сервером:*

1. Введите IP-адрес или имя NTP-сервера.
2. Если вы хотите добавить дополнительный NTP-сервер, нажмите на клавишу **Enter** и введите IP-адрес или имя NTP-сервера.
3. Когда вы добавите все NTP-серверы, дважды нажмите на клавишу **Enter**.

Настройка займет какое-то время. После этого установка завершится. Вы можете перейти к настройке конфигурации сервера в веб-интерфейсе для управления масштабированием (см. раздел "Начало работы в веб-интерфейсе для управления масштабированием" на стр. 187).

Установка компонента Sensor на отдельном сервере

Для установки компонента Sensor на физическом сервере вам нужно запустить образ диска с компонентами Central Node и Sensor.

Для установки компонента Sensor на виртуальном сервере вам нужно подключить образ диска с компонентами Central Node и Sensor к выбранной виртуальной машине и запустить ее. Установка запускается сразу после включения виртуальной машины. Вы можете управлять процессом установки с помощью консоли виртуальной машины.

В этом разделе

Шаг 1. Выбор роли сервера 142

Шаг 2. Просмотр Лицензионного соглашения и Политики конфиденциальности 143

Шаг 3. Выбор диска для установки компонента 143

Шаг 4. Выбор внешнего сетевого интерфейса 143

Шаг 5. Подключение к серверу с компонентом Central Node 144

Шаг 6. Создание учетной записи администратора 144

Шаг 1. Выбор роли сервера

► *Чтобы выбрать роль сервера:*

1. Выберите один из следующих вариантов:
   - **storage**.

     Эта роль предполагает установку сервера хранения для развертывания компонента Central Node в виде кластера.
   - **processing**.

     Эта роль предполагает установку обрабатывающего сервера для развертывания компонента Central Node в виде кластера.

     Роль включает также установку и настройку компонента Sensor.
   - **single**.

     Эта роль предполагает установку компонентов Central Node и Sensor на одном сервере.
   - **sensor**.

     Эта роль предполагает установку компонента Sensor на отдельном сервере.
2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 2. Просмотр Лицензионного соглашения и Политики конфиденциальности

Для продолжения установки вам нужно ознакомиться с Лицензионным соглашением и Политикой конфиденциальности и принять их условия. Если условия Лицензионного соглашения и Политики конфиденциальности не приняты, установка не выполняется.

► *Чтобы принять условия Лицензионного соглашения и Политики конфиденциальности при установке компонентов на базе операционной системы Astra Linux:*

1. Выберите язык для просмотра Лицензионного соглашения и Политики конфиденциальности в списке, нажав на клавишу **F1**.

   Например, если вы хотите просмотреть Лицензионное соглашение и Политику конфиденциальности на английском языке, выберите **English** и нажмите на клавишу **ENTER**.

   Откроется окно с текстом Лицензионного соглашения на использование операционных систем Astra Linux.
2. Ознакомьтесь с Лицензионным соглашением на использование операционных систем Astra Linux.
3. Если вы принимаете условия Лицензионного соглашения на использование операционных систем Astra Linux, нажмите на кнопку **Yes**.

   Откроется окно с текстом Лицензионного соглашения АО "Лаборатория Касперского".
4. Ознакомьтесь с Лицензионным соглашением АО "Лаборатория Касперского".
5. Если вы принимаете условия Лицензионного соглашения, нажмите на кнопку **Yes**.

   Откроется окно с текстом Политики конфиденциальности.
6. Ознакомьтесь с Политикой конфиденциальности.
7. Если вы принимаете условия Политики конфиденциальности, нажмите на кнопку **Yes**.

Мастер установки перейдет к следующему шагу.

Шаг 3. Выбор диска для установки компонента

► *Чтобы выбрать диск для установки компонента:*

1. Выберите один из предложенных дисков для установки компонента и нажмите на клавишу **Enter**.

   Отобразится окно подтверждения.
2. Выберите **Yes** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 4. Выбор внешнего сетевого интерфейса

Внешний сетевой интерфейс используется для доступа к серверу по протоколу SSH, работы в веб-интерфейсе Kaspersky Anti Targeted Attack Platform и других внешних подключений.

► *Чтобы выбрать внешний сетевой интерфейс:*

1. Выберите строку с сетевым интерфейсом, который используется для внешней сети.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 5. Подключение к серверу с компонентом Central Node

► *Чтобы подключиться к серверу, на котором вы установили компонент Central Node:*

1. В поле Central Node введите IP-адрес или URL-адрес сервера с компонентом Central Node.

   Если компонент Central Node развернут в виде кластера, вы можете ввести IP-адрес любого сервера кластера.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 6. Создание учетной записи администратора

Учетная запись администратора используется для работы с компонентом Sensor в меню администратора приложения и в режиме Technical Support Mode.

По умолчанию в качестве имени пользователя для учетной записи администратора используется *admin*. Вам требуется задать пароль для этой учетной записи.

► *Чтобы задать пароль для учетной записи администратора:*

1. В поле **password** введите пароль учетной записи администратора.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. В поле **confirm** введите пароль повторно.
3. Выберите кнопку **Ok** и нажмите на клавишу **Enter**.

Установка будет завершена.

Настройка Kaspersky Anti Targeted Attack Platform на базе операционной системы Astra Linux

Для достижения расчетных характеристик производительности Kaspersky Anti Targeted Attack Platform на базе операционной системы Astra Linux вам необходимо произвести настройку приложения.

► *Чтобы настроить Kaspersky Anti Targeted Attack Platform на базе операционной системы Astra Linux:*

1. Перейдите в режим Technical Support Mode (см. раздел "Начало работы с приложением в режиме Technical Support Mode" на стр. 189).
2. Выполните команды:

   ```
   sudo -s
   astra-modeswitch set 0
   mv /lib/modules/$(uname -r)/misc/parsec.ko ./parsec.ko.backup
   update-initramfs -u -k all
   cp /lib/systemd/system/docker.service /lib/systemd/system/docker.service.backup
   ```

3. Отредактируйте файл docker.service в директории /lib/systemd/system/ следующим образом:
   c. Измените значение строки

      ```
      After=network-online.target docker.socket firewalld.service \
            docker-parsec-init.service
      ```

      на значение `After=network-online.target docker.socket firewalld.service`
   d. Измените значение строки `Requires=docker.socket docker-parsec-init.service` на значение `Requires=docker.socket`
4. Перезагрузите сервер и снова перейдите в режим Technical Support Mode.
5. Выполните команду:

   ```
   lsmod | grep parsec
   ```

   В консоли отобразится пустая строка.

Приложение Kaspersky Anti Targeted Attack Platform на базе операционной системы Astra Linux будет настроено.

Функции безопасности модуля Parsec не требуются и не используются при работе приложения Kaspersky Anti Targeted Attack Platform.

Установка пакета обновления приложения до версии 6.0.2

Перед установкой пакета обновления приложения рекомендуется предварительно создать резервную копию текущего состояния каждого обновляемого сервера Central Node и загрузить ее на жесткий диск из меню администратора приложения. В случае сбоя при установке пакета обновления приложения или при необходимости переустановить Kaspersky Anti Targeted Attack Platform вы сможете воспользоваться сохраненной копией приложения.

Обновление поставляется в виде пакета обновления. Пакет входит в комплект поставки приложения.

Пакет обновления приложения до версии 6.0.2 устанавливается на серверы Central Node, Sensor и Sandbox версий 6.0 или 6.0.1. Установка пакета обновления на серверы Central Node и Sensor зависит от способа развертывания и использования приложения:

- Если вы используете приложение в виде отказоустойчивого кластера, вам необходимо установить пакет обновления на сервер кластера с ролью manager в Docker swarm. Для просмотра роли используйте команду `$ docker node ls`.
- Если вы используете режим распределенного решения и мультитенатности, вам необходимо установить пакет обновления на каждый сервер Central Node и Sensor, установленных на отдельных серверах. Вам не требуется отключать серверы SCN от PCN для установки пакета обновления.
- В остальных случаях для установки пакета обновления вам необходимо подключиться к каждому серверу Central Node и Sensor по протоколу SSH или через терминал (см. раздел "Начало работы с приложением в режиме Technical Support Mode" на стр. 189) и войти в консоль управления. Вам не требуется отключать Sandbox и Sensor от Central Node для установки пакета обновления.

Для установки пакета обновления до версии 6.0.2 на серверах Sandbox следуйте отдельной инструкции, расположенной ниже.

► *Чтобы установить пакет обновления на серверах Central Node и Sensor:*

1. Поместите пакет обновления компонентов Central Node и Sensor *kata-cn-upgrade-6.0.2-x86_64_en-ru.tar.gz* на сервер в директорию `/data`. Если у вас включена функция сохранения сетевого трафика. убедитесь, что размер свободного дискового пространства составляет более 100 ГБ.
2. Войдите в консоль управления сервера, на котором вы хотите установить пакет обновления, по протоколу SSH или через терминал (см. раздел "Начало работы с приложением в режиме Technical Support Mode" на стр. 189).
3. Убедитесь, что размер свободного дискового пространства в файловой системе /dev/sda2 составляет более 100 ГБ.
4. Распакуйте архив с обновлением, выполнив команду `tar xvf /data/kata-cn-upgrade-6.0.2-x86_64_en-ru.tar.gz -C /data/`.
5. Повысьте привилегии пользователя, выполнив команду `sudo -i`.
6. Установите пакет с обновлением, выполнив следующие команды:

   ```
   cd /data/upgrade/
   chmod +x ./install_kata_upgrade.sh
   ```

```
./install_kata_upgrade.sh
```

7. Установите обновление, выполнив команды:

   ```
   kata-upgrade --data-dir /data/upgrade/ --password <пароль пользователя admin>.
   ```

   Если пароль содержит служебные символы, переменная password должна быть указана в следующем формате: --password '<пароль>'.

8. Выполните повторный вход в консоль управления обновленного сервера по протоколу SSH или через терминал.

9. Установите значение параметра **Максимальный размер хранилища**, если используете Sensor с компонентом Central Node на сервере (см. раздел "Включение и настройка параметров записи сырого сетевого трафика на сервере с установленными компонентами Sensor и Central Node" на стр. 273) или значение параметра **Traffic storage size**, если используете Sensor на отдельном сервере (см. раздел "Включение и настройка параметров записи сырого сетевого трафика на отдельном сервере с компонентом Sensor" на стр. 274). После обновления будет установлено значение по умолчанию - 100 ГБ.

Пакет обновления будет установлен на серверах Central Node и Sensor.

► *Чтобы установить пакет обновления на серверах Sandbox:*

1. Поместите пакет обновления компонента Sandbox *kata-sb-upgrade-6.0.2-x86_64_en-ru.tar.gz* на сервер в директорию `/tmp`.

2. Войдите в консоль управления сервера, на котором вы хотите установить пакет обновления, по протоколу SSH или через терминал (см. раздел "Начало работы с приложением в режиме Technical Support Mode" на стр. 189).

3. Распакуйте архив с обновлением, выполнив команду `tar xzvf /tmp/kata-sb-upgrade-6.0.2-x86_64_en-ru.tar.gz -C /tmp/`.

4. Повысьте привилегии пользователя, выполнив команду `sudo -i`.

5. Установите пакет с обновлением, выполнив следующие команды:

   ```
   cd /tmp/kata-sb-upgrade-6.0.2-x86_64_en-ru
   ./patch.sh
   ```

6. Дождитесь успешной установки пакета обновления.

Пакет обновления будет установлен на серверах Sandbox.

Подключение и настройка внешнего хранилища для компонента Sensor

Kaspersky Anti Targeted Attack Platform сохраняет трафик, полученный от сетевых интерфейсов, в виде файлов дампа сетевого трафика. Если вы хотите обеспечить долговременное хранение файлов дампа сетевого трафика, вы можете подключить и настроить внешнее хранилище. Файлы дампа сетевого трафика, хранящиеся во внешнем хранилище, можно использовать для выгрузки сетевого трафика в файлы формата PCAP.

► *Чтобы подключить и настроить внешнее хранилище для файлов дампа сетевого трафика на сервере с установленными компонентами Sensor и Central Node:*

1. Подключите диск, который будет использоваться в качестве внешнего хранилища, объемом не менее 100 ГБ.
2. Перейдите в режим Technical Support Mode (см. раздел "Начало работы с приложением в режиме Technical Support Mode" на стр. 189).
3. Выполните команды:

   ```
   sudo -i
   fdisk -l
   ```

   Убедитесь, что диск, подключенный для использования в качестве внешнего хранилища, отобразился в консоли.
4. Выполните команды:

   ```
   mke2fs -t ext4 -L DATA -m 0 /dev/<имя подключенного диска>
   sudo nano etc/fstab
   ```

   Откроется файл fstab в текстовом редакторе.
5. Добавьте в конец файла запись:

   ```
   /dev/<имя подключенного диска>                /data/volumes/dumps/
   ext4    defaults        0 0
   ```
6. Закройте текстовый редактор.
7. Выполните команды:

   ```
   mount
   rm -r /data/volumes/dumps/*
   ```

   > В результате выполнения команд с подключенного диска будут удалены все данные.

   Подключенный диск будет настроен для использования в качестве внешнего хранилища.
8. Выполните команды:

   ```
   chown kluser:klusers /data/volumes/dumps/
   ls -lah /data/volumes/dumps/
   lsblk
   ```

   Убедитесь, что напротив имени подключенного диска в столбце **TYPE MOUNTPOINTS** отображается значение **/data/volumes/dumps**.
9. Выполните команды:

   ```
   docker stop $(docker ps | grep preprocessor_span | awk '{print $1}')
   docker ps | grep preprocessor_span
   ```

   Дождитесь, когда в консоли появится статус **Up 2 seconds**.
10. Выполните команды:

```
docker exec -it $(docker ps | grep preprocessor_span | awk '{print
$1}') bash
```

```
lsblk
```

Убедитесь, что напротив имени подключенного диска в столбце **TYPE MOUNTPOINTS** отображается значение **/mnt/kaspersky/nta/dumps**.

Внешнее хранилище для файлов дампа сетевого трафика на сервере с установленными Sensor и Central Node будет подключено и настроено.

► *Чтобы подключить и настроить внешнее хранилище для файлов дампа сетевого трафика на отдельном сервере с установленным компонентом Sensor:*

1. Подключите диск, который будет использоваться в качестве внешнего хранилища, объемом не менее 100 ГБ.
2. Перейдите в режим Technical Support Mode (см. раздел "Начало работы с приложением в режиме Technical Support Mode" на стр. 189).
3. Выполните команды:

   ```
   sudo -i
   ```

   ```
   fdisk -l
   ```

   Убедитесь, что диск, подключенный для использования в качестве внешнего хранилища, отобразился в консоли.
4. Выполните команды:

   ```
   mke2fs -t ext4 -L DATA -m 0 /dev/<имя подключенного диска>
   ```

   ```
   sudo nano etc/fstab
   ```

   Откроется файл fstab в текстовом редакторе.
5. Добавьте в конец файла запись:

   ```
   /dev/<имя подключенного диска>                /data/volumes/dumps/
   ext4    defaults        0 0
   ```
6. Закройте текстовый редактор.
7. Выполните команду:

   ```
   rm -r /data/volumes/dumps/*
   ```

   В результате выполнения команд с подключенного диска будут удалены все данные.

Внешнее хранилище для файлов дампа сетевого трафика на отдельном сервере с установленным компонентом Sensor будет подключено и настроено.

Процедура приемки

Перед вводом приложения в эксплуатацию проводится процедура приемки, включающая проверку правильной установки (см. раздел "Проверка целостности файлов Kaspersky Anti Targeted Attack Platform" на стр. 151), работоспособности (см. раздел "Проверка безопасности и работоспособности Kaspersky Anti Targeted Attack Platform" на стр. 153) и соответствия безопасной (сертифицированной) конфигурации (см. раздел "Безопасное состояние" на стр. 150).

В этом разделе

Безопасное состояние 150

Проверка целостности файлов Kaspersky Anti Targeted Attack Platform 151

Проверка безопасности и работоспособности Kaspersky Anti Targeted Attack Platform 153

Безопасное состояние

Приложение находится в безопасном состоянии (сертифицированной конфигурации), если параметры приложения находятся в рамках допустимых значений, приведенных в приложении к этому документу (см. раздел "Приложение. Значения параметров приложения в сертифицированной конфигурации" на стр. 674).

Вам необходимо использовать коммерческую лицензию для того, чтобы приложение находилось в безопасном состоянии. NFR лицензия ограничивает функциональность приложения.

Проверка целостности файлов Kaspersky Anti Targeted Attack Platform

Вы можете проверить целостность файлов Kaspersky Anti Targeted Attack Platform с помощью утилиты kata-product-verification.

Проверка целостности файлов компонентов Sensor и Central Node выполняется на серверах с компонентом Sensor или Central Node (для этих серверов используется один и тот же установочный файл программы) с использованием эталонного файла с контрольной суммой файлов этих компонентов.

Проверка целостности файлов компонента Sandbox выполняется на сервере с компонентом Sandbox с использованием эталонного файла с контрольной суммой файлов компонента Sandbox.

Для проверки целостности файлов Kaspersky Anti Targeted Attack Platform требуется предварительно установить утилиту kata-product-verification на сервер, на котором вы хотите выполнить проверку.

► *Чтобы установить утилиту для проверки целостности файлов на сервере с компонентами Central Node и Sensor или с компонентом Sandbox, выполните следующие действия:*

1. Загрузите архив с утилитой на сервер, выполнив команду:

   ```
   scp <имя архива с утилитой и манифестами>.tar.gz <имя пользователя с правами администратора сервера Central Node и/или Sandbox>@<IP-адрес сервера>:/tmp
   ```

   Например, вы можете выполнить команду `scp kata-6.0.0-product-manifests.tar.gz admin@10.10.10.1:/tmp`

   Архив будет загружен.
2. Войдите в консоль управления сервера с компонентом Central Node, Sensor или Sandbox по протоколу SSH или через терминал.
3. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке программы.
4. В отобразившемся меню администратора программы выберите режим **Technical Support Mode**.
5. Нажмите на клавишу **ENTER**.
6. В окне подтверждения выберите **Yes** и нажмите на клавишу **ENTER**.
7. Распакуйте архив, выполнив команду:

   ```
   tar xvf /tmp/kata-6.0.0-product-manifests.tar.gz --directory /tmp
   ```
8. Установите утилиту kata-product-verification и необходимые пакеты, выполнив команды:

   ```
   sudo dpkg -i /tmp/apt_integrity_check_tool_6.0.0.7_Release_amd64.deb
   ```

   ```
   sudo chmod +x /opt/kaspersky/apt-integrity-check-tool/bin/integrity_check_tool
   ```

   ```
   sudo kata-run.sh pip install --force-reinstall --no-deps /tmp/product_verification-1.0-py3-none-any.whl /tmp/split_delivery_tool-1.0-py3-none-any.whl
   ```

Утилита будет установлена. Вы можете перейти к проверке целостности файлов Kaspersky Anti Targeted Attack Platform.

► *Чтобы проверить целостность файлов компонентов Central Node и Sensor, выполните следующие действия:*

1. Выполните команду:

   sudo kata-run.sh kata-product-verification verify --node-type <node_type> --report <имя эталонного файла>.json, где `node_type` *принимает значение* `CN` *для компонента Central Node,* `Sensor` *для компонента Sensor.*

Например, вы можете выполнить команду `sudo kata-run.sh kata-product-verification verify --node-type CN --report /tmp/kata-cnode-astra-6.0.0.200.json`

► *Чтобы проверить целостность файлов компонента Sandbox, выполните следующие действия:*

1. Выполните команду:

   sudo kata-product-verification verify --node-type SB --report <имя эталонного файла>.json

При успешной проверке целостности файлов в консоли будет выведено сообщение Product files verification finished! При неуспешной проверке целостности файлов в консоли будет выведено сообщение об ошибке *Product files verification failed!*, а также будет создан отчет, содержащий список файлов, контрольные суммы которых не совпали с эталонными. По умолчанию отчет будет создан в `/tmp/report_of_changed_files.json`

Проверка безопасности и работоспособности Kaspersky Anti Targeted Attack Platform

Для того, чтобы работа с Kaspersky Anti Targeted Attack Platform была безопасной, программа сохраняет зараженные и возможно зараженные файлы в специальном изолированном хранилище. Файлы защищены паролем и не представляют опасности для IT-инфраструктуры организации.

Для проверки безопасности и работоспособности в Kaspersky Anti Targeted Attack Platform вы можете использовать следующую информацию:

- графическое отображение работоспособности компонентов на странице мониторинга веб-интерфейса приложения;
- записи о работоспособности компонентов в журнале Kaspersky Anti Targeted Attack Platform (см. раздел "О журналах Kaspersky Anti Targeted Attack Platform" на стр. 153).

В этом разделе

О журналах Kaspersky Anti Targeted Attack Platform 153

Просмотр журнала работоспособности сервера с компонентом Central Node 154

Просмотр журнала работоспособности сервера с компонентом Sandbox 154

Просмотр журнала аудита безопасности сервера с компонентом Central Node 154

Просмотр журнала аудита безопасности сервера с компонентом Sandbox 155

О журналах Kaspersky Anti Targeted Attack Platform

Во время работы Kaspersky Anti Targeted Attack Platform возникают различного рода события. Они отражают изменения состояния приложения. Для того, чтобы администратор программы мог самостоятельно проанализировать ход работы приложения и возникающие ошибки, а также для того, чтобы специалисты "Лаборатории Касперского" могли оказать эффективную техническую поддержку, Kaspersky Anti Targeted Attack Platform записывает информацию о работе приложения в журналах каждые 10 минут.

В журналах содержится, например, следующая информация:

- о запуске приложения;
- о входе в систему каждого пользователя;
- о состоянии работы серверов с компонентами приложения;
- об обнаружении событий компонентами Kaspersky Anti Targeted Attack Platform.

Просмотр журнала работоспособности сервера с компонентом Central Node

► *Чтобы просмотреть журнал работоспособности сервера с компонентом Central Node, выполните следующие действия:*

1. Подключитесь к серверу с компонентом Central Node по протоколу SSH под учетной записью администратора.

   Откроется меню администратора.
2. В меню администратора программы выберите режим **Technical Support Mode**.
3. Нажмите на клавишу **ENTER**.

   Отобразится окно подтверждения входа в режим **Technical Support Mode**.
4. Выберите **Yes** и нажмите на клавишу **ENTER**.
5. Выполните команду:

   ```
   sudo kata-run.sh kata-collect-siem-logs log-audit --no-compress --output-dir /tmp
   ```

   Журнал будет скачен в директорию /tmp.
6. Выполните команду:
7. `cat /tmp/log-audit.log | head -n 1`

В консоли меню администратора вы сможете просмотреть журнал работоспособности сервера с компонентом Central Node.

Просмотр журнала работоспособности сервера с компонентом Sandbox

► *Чтобы просмотреть журнал работоспособности сервера с компонентом Sandbox, выполните следующие действия:*

1. Подключитесь к серверу с компонентом Sandbox по протоколу SSH под учетной записью администратора для работы в консоли управления сервером.
2. В консоли управления сервером выполните команду:

   ```
   sudo /opt/kaspersky/sandbox/libexec/utilities/checker.py -l /var/log/kaspersky/sandbox/checker/checker.log
   ```

Вы сможете просмотреть журнал работоспособности сервера с компонентом Sandbox.

Просмотр журнала аудита безопасности сервера с компонентом Central Node

Вы можете просмотреть журнал аудита безопасности сервера с компонентом Central Node следующими способами:

- Включить запись информации о действиях пользователей в веб-интерфейсе приложения (см. раздел "Включение и отключение записи информации в журнал активности" на стр. 313) в журнал и

просмотреть эту информацию, скачав файлы журнала (см. раздел "Скачивание файлов журнала активности" на стр. 313).

- Просмотреть журнал аудита безопасности через меню администратора.

► *Чтобы просмотреть журнал аудита безопасности сервера с компонентом Central Node через меню администратора:*

1. Подключитесь к серверу с компонентом Central Node по протоколу SSH под учетной записью администратора.

   Откроется меню администратора.

2. В меню администратора программы выберите режим **Technical Support Mode**.
3. Нажмите на клавишу **ENTER**.

   Отобразится окно подтверждения входа в режим **Technical Support Mode**.

4. Выберите **Yes** и нажмите на клавишу **ENTER**.
5. Выполните команду:

   ```
   sudo kata-run.sh kata-collect-siem-logs log-audit --no-compress --output-dir /tmp
   ```

   Журнал будет скачен в директорию /tmp.

6. Выполните команду:

   ```
   cat /tmp/log-audit.log | head -n 1
   ```

В консоли меню администратора вы сможете просмотреть журнал аудита безопасности сервера с компонентом Central Node.

Просмотр журнала аудита безопасности сервера с компонентом Sandbox

► *Чтобы просмотреть журнал аудита безопасности сервера с компонентом Sandbox:*

1. Подключитесь к серверу с компонентом Sandbox по протоколу SSH под учетной записью администратора для работы в консоли управления сервером.
2. В консоли управления сервером выполните команду:

   ```
   sudo less /var/log/kaspersky/apt-audit.log
   ```

Вы сможете просмотреть журнал аудита безопасности сервера с компонентом Sandbox.

Лицензирование приложения

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием приложения Kaspersky Anti Targeted Attack Platform.

В этом разделе

О Лицензионном соглашении 156
О лицензии 157
О лицензионном сертификате 157
О ключе 158
О файле ключа 158
Просмотр информации о лицензии и добавленных ключах в веб-интерфейсе Central Node 158
Просмотр текста Лицензионного соглашения в веб-интерфейсе Central Node 159
Просмотр текста Политики конфиденциальности в веб-интерфейсе Central Node 159
Просмотр информации о стороннем коде, используемом в приложении 160
Просмотр текста Лицензионного соглашения в веб-интерфейсе Sandbox 160
Просмотр текста Лицензионного соглашения компонента Endpoint Agent 160
Добавление ключа 161
Замена ключа 161
Удаление ключа 161
Режимы работы приложения в соответствии с лицензией 162

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать приложение.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с приложением.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки Kaspersky Anti Targeted Attack Platform.
- Прочитав документ /EULA/License.<язык>.

  Этот документ включен в комплект поставки приложения.
- В веб-интерфейсе приложения в разделе **Параметры**, подразделе **Лицензия** по кнопке **Лицензионное соглашение**.

- В веб-интерфейсе компонента Sandbox в меню по ссылке **Лицензионное соглашение**.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки приложения. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку приложения и не должны использовать его.

О лицензии

Лицензия – это ограниченное по времени право на использование приложения, предоставляемое вам на основе Лицензионного соглашения.

Лицензия включает в себя право на получение следующих видов услуг:

- использование приложения в соответствии с условиями Лицензионного соглашения;
- получение технической поддержки.

Объем предоставляемых услуг и срок использования приложения зависят от типа лицензии, по которой было активировано приложение.

В Kaspersky Anti Targeted Attack Platform предусмотрены следующие типы лицензий:

- NFR (not for resale / не для перепродажи) – бесплатная лицензия на определенный период, предназначенная для ознакомления с приложением и тестовых развертываний приложения.
- Коммерческая – платная лицензия, предоставляемая при приобретении приложения.

По истечении срока действия лицензии приложение продолжает работу, но с ограниченной функциональностью. Чтобы использовать приложение в режиме полной функциональности, вам нужно приобрести коммерческую лицензию или продлить срок действия коммерческой лицензии.

В текущей версии Kaspersky Anti Targeted Attack Platform функциональность приложения также зависит от типа установленного ключа.

О лицензионном сертификате

Лицензионный сертификат – это документ, который передается вам вместе с файлом ключа или кодом активации.

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- лицензионный ключ или номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о приложении, которое можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать приложение по предоставляемой лицензии);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

О ключе

Лицензионный ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать приложение в соответствии с условиями Лицензионного соглашения. Лицензионный ключ создается специалистами "Лаборатории Касперского".

Чтобы добавить ключ в приложение, загрузите файл ключа.

Ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если ключ заблокирован, для работы приложения требуется добавить другой ключ.

В текущей версии Kaspersky Anti Targeted Attack Platform функциональность приложения зависит от типа добавленного лицензионного ключа:

- **Ключи KATA и KEDR**. Полная функциональность приложения.
- **Ключ KEDR**. Ограничен прием и обработка данных из сетевого и почтового трафика.
- **Ключ KATA**. Ограничена функциональность разделов веб-интерфейса **Поиск угроз**, **Задачи**, **Политики**, **Пользовательские правила**, **Хранилище**, **Endpoint Agents**.

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления лицензионного ключа, активирующего приложение.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения приложения или после заказа пробной версии приложения.

Чтобы активировать приложение с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации в Kaspersky CompanyAccount.

Для восстановления файла ключа обратитесь к продавцу лицензии.

Просмотр информации о лицензии и добавленных ключах в веб-интерфейсе Central Node

В режиме распределенного решения и мультитенантности вы можете просматривать информацию о лицензии и добавленных ключах в веб-интерфейсе серверов PCN и всех подключенных SCN под учетной записью локального администратора, администратора или пользователей веб-интерфейса приложения.

► *Чтобы просмотреть информацию о лицензии и добавленных ключах,*

в веб-интерфейсе сервера с компонентом Central Node выберите раздел **Параметры**, подраздел **Лицензия**.

В веб-интерфейсе отображается следующая информация о лицензии и добавленных ключах:

- серийный номер лицензии;
- дата активации приложения;
- дата окончания срока действия лицензии;
- количество дней до окончания срока действия лицензии.

За 30 дней до окончания срока действия лицензии в разделе **Мониторинг** появляется уведомление о необходимости продлить лицензию. Это уведомление отображается на всех серверах с компонентом Central Node (в режиме распределенного решения и мультитенантности – на PCN и всех подключенных SCN) для всех пользователей независимо от их роли.

Просмотр текста Лицензионного соглашения в веб-интерфейсе Central Node

В режиме распределенного решения и мультитенантности вы можете просматривать текст Лицензионного соглашения в веб-интерфейсе серверов PCN и всех подключенных SCN под учетной записью локального администратора, администратора или пользователей веб-интерфейса приложения.

► *Чтобы просмотреть текст Лицензионного соглашения, выполните следующие действия в веб-интерфейсе сервера с компонентом Central Node:*

1. Выберите раздел **Параметры**, подраздел **Лицензия**.
2. Нажмите на кнопку **Лицензионное соглашение** в правом верхнем углу рабочей области.
3. В открывшемся окне просмотрите текст Лицензионного соглашения.
4. По окончании просмотра нажмите на кнопку **Закрыть**.

Просмотр текста Политики конфиденциальности в веб-интерфейсе Central Node

В режиме распределенного решения и мультитенантности вы можете просматривать текст Политики конфиденциальности в веб-интерфейсе серверов PCN и всех подключенных SCN под учетной записью локального администратора, администратора или пользователей веб-интерфейса приложения.

► *Чтобы просмотреть текст Политики конфиденциальности, выполните следующие действия в веб-интерфейсе сервера с компонентом Central Node:*

1. Выберите раздел **Параметры**, подраздел **Лицензия**.
2. Нажмите на кнопку **Политика конфиденциальности** в правом верхнем углу рабочей области.
3. В открывшемся окне просмотрите текст Политики конфиденциальности.
4. По окончании просмотра нажмите на кнопку **Закрыть**.

Просмотр информации о стороннем коде, используемом в приложении

В режиме распределенного решения и мультитенантности вы можете просматривать информацию о стороннем коде, используемом в Kaspersky Anti Targeted Attack Platform, в веб-интерфейсе серверов PCN и всех подключенных SCN под учетной записью локального администратора, администратора или пользователей веб-интерфейса приложения.

► *Чтобы просмотреть информацию о стороннем коде, выполните следующие действия в веб-интерфейсе сервера с компонентом Central Node:*

1. Выберите раздел **Параметры**, подраздел **Лицензия**.
2. Нажмите на кнопку **Сторонний код** в правом верхнем углу рабочей области.
3. В открывшемся окне просмотрите информацию о стороннем коде.
4. По окончании просмотра нажмите на кнопку **Закрыть**.

Просмотр текста Лицензионного соглашения в веб-интерфейсе Sandbox

► *Чтобы просмотреть текст Лицензионного соглашения в веб-интерфейсе сервера с компонентом Sandbox (см. раздел "Компонент Sandbox" на стр. 68), выполните следующие действия:*

1. Войдите в веб-интерфейс Sandbox под учетными данными, которые вы задали при установке компонента Sandbox (см. раздел "Установка компонента Sandbox" на стр. 119).
2. Нажмите на кнопку в левой нижней части окна веб-интерфейса.
3. Откроется окно с информацией о компоненте Sandbox.
4. По ссылке **Лицензионное соглашение** раскройте окно с текстом Лицензионного соглашения приложения.
5. Просмотрите текст Лицензионного соглашения.
6. По окончании просмотра нажмите на кнопку .

Просмотр текста Лицензионного соглашения компонента Endpoint Agent

Вы можете просмотреть текст Лицензионного соглашения для приложения, которую используете в качестве компонента Endpoint Agent. Подробнее о том, как просмотреть текст Лицензионного соглашения, см. в справке соответствующего приложения.

Добавление ключа

В режиме распределенного решения добавление ключа доступно только на сервере PCN.

► *Чтобы добавить ключ:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Лицензия**.
2. Выберите тип ключа: **KATA** или **KEDR**.
3. В разделе с выбранным типом ключа нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.
4. Выберите файл ключа, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

Ключ будет добавлен в приложение.

Замена ключа

В режиме распределенного решения замена ключа доступна только на сервере PCN.

► *Чтобы заменить активный ключ приложения другим ключом:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Лицензия**.
2. Выберите тип ключа: **KATA** или **KEDR**.
3. В разделе с выбранным типом ключа нажмите на кнопку **Заменить**.

   Откроется окно выбора файлов.
4. Выберите файл ключа, которым вы хотите заменить активный ключ, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

Загруженный ключ заменит активный ключ приложения.

Удаление ключа

В режиме распределенного решения удаление ключа доступно только на сервере PCN.

► *Чтобы удалить ключ, выполните следующие действия:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Лицензия**.

2. Выберите тип ключа: **KATA** или **KEDR**.
3. В разделе с выбранным типом ключа нажмите на кнопку **Удалить**.

   Откроется окно подтверждения удаления ключа.
4. Нажмите на кнопку **Да**.

   Окно подтверждения удаления ключа закроется.

Ключ будет удален.

Режимы работы приложения в соответствии с лицензией

В Kaspersky Anti Targeted Attack Platform предусмотрены различные режимы работы приложения в зависимости от добавленных ключей.

Без лицензии

В этом режиме приложения работает с момента установки приложения и запуска веб-интерфейса до тех пор, пока вы не добавите ключ.

В режиме Без лицензии действуют следующие ограничения:

- Не обновляются базы приложения.
- Отсутствует подключение к базе знаний Kaspersky Security Network.
- Ограничен прием и обработка данных из сетевого и почтового трафика.
- Ограничена функциональность разделов веб-интерфейса **Поиск угроз**, **Задачи**, **Политики**, **Пользовательские правила**, **Хранилище**, **Endpoint Agents**.

Коммерческая лицензия

В этом режиме приложения подключается к базе знаний Kaspersky Security Network и обновляет базы.

По истечении срока годности ключа для коммерческой лицензии приложения прекращает обновление баз и не подключается к базе знаний Kaspersky Security Network.

Для возобновления работы приложения необходимо заменить ключ или добавить новый ключ для коммерческой лицензии.

В текущей версии Kaspersky Anti Targeted Attack Platform функциональность приложения также зависит от типа добавленного лицензионного ключа:

- **Ключи KATA и KEDR**. Полная функциональность приложения.
- **Ключ KEDR**. Ограничен прием и обработка данных из сетевого и почтового трафика.
- **Ключ KATA**. Ограничена функциональность разделов веб-интерфейса **Поиск угроз**, **Задачи**, **Политики**, **Пользовательские правила**, **Хранилище**, **Endpoint Agents**.

Настройка интеграции Kaspersky Anti Targeted Attack Platform с компонентом Endpoint Agent

В этом разделе содержится информация о том, как настроить интеграцию Kaspersky Anti Targeted Attack Platform с приложением Kaspersky Endpoint Agent для Windows, если оно используется в роли компонента Endpoint Agent.

Вам понадобится выполнить действия и на стороне Kaspersky Anti Targeted Attack Platform через веб-интерфейс (см. раздел "Начало работы в веб-интерфейсе приложения под учетной записью локального администратора" на стр. 186) и меню администратора приложения (см. раздел "Начало работы в меню администратора приложения" на стр. 188), и на стороне приложения, которое используется в качестве компонента Endpoint Agent, через Консоль администрирования (MMC).

Если вы используете в роли компонента Endpoint Agent приложения Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Mac, более подробную информацию по интеграции с Kaspersky Anti Targeted Attack Platform см. в разделах *Управление приложением Kaspersky Endpoint Security для Windows (на стр. 606), Управление приложением Kaspersky Endpoint Security для Linux (на стр. 607) и Управление приложением Kaspersky Endpoint Security для Mac (на стр. 608).*

kaspersky

В этом разделе

Настройка доверенного соединения Kaspersky Anti Targeted Attack Platform с приложением Kaspersky Endpoint Agent 164

Скачивание TLS-сертификата сервера Central Node на компьютер 169

Генерация TLS-сертификата сервера Central Node в веб-интерфейсе Kaspersky Anti Targeted Attack Platform 169

Загрузка самостоятельно подготовленного TLS-сертификата сервера Central Node через веб-интерфейс Kaspersky Anti Targeted Attack Platform 170

Загрузка TLS-сертификата сервера Central Node или Sensor в Kaspersky Endpoint Agent 171

Включение проверки TLS-сертификата Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform 172

Генерация TLS-сертификата Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform и скачивание крипто-контейнера 173

Загрузка самостоятельно подготовленного TLS-сертификата Kaspersky Endpoint Agent через веб-интерфейс Kaspersky Anti Targeted Attack Platform 173

Просмотр таблицы TLS-сертификатов Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform 174

Фильтрация и поиск TLS-сертификатов Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform 175

Удаление TLS-сертификатов Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform 176

Настройка проверки TLS-сертификата Kaspersky Endpoint Agent сервером Central Node и загрузка крипто-контейнера в Kaspersky Endpoint Agent 176

Настройка перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor 177

Генерация TLS-сертификата сервера Sensor в меню администратора сервера Sensor 179

Загрузка самостоятельно подготовленного TLS-сертификата сервера Sensor через меню администратора сервера Sensor 180

Скачивание TLS-сертификата сервера Sensor на компьютер 181

Настройка интеграции и доверенного соединения с Kaspersky Anti Targeted Attack Platform на стороне Kaspersky Endpoint Agent 181

Настройка доверенного соединения Kaspersky Anti Targeted Attack Platform с приложением Kaspersky Endpoint Agent

Вам понадобится настроить доверенное соединение Kaspersky Anti Targeted Attack Platform с Kaspersky Endpoint Agent и на стороне Kaspersky Anti Targeted Attack Platform через веб-интерфейс (см. раздел "Начало работы в веб-интерфейсе приложения под учетной записью локального администратора" на стр. 186) и меню администратора приложения (см. раздел "Начало работы в меню администратора приложения" на стр. 188), и на стороне Kaspersky Endpoint Agent через консоль администрирования KSC.

Вы можете использовать один из следующих вариантов доверенного соединения:

1. С использованием TLS-сертификата Kaspersky Anti Targeted Attack Platform. Без проверки TLS-сертификата Kaspersky Endpoint Agent на стороне Kaspersky Anti Targeted Attack Platform.

   a. Настройка соединения с сервером Central Node без проверки TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform (на стр. 166)

      Kaspersky Endpoint Agent устанавливает доверенное соединение с Kaspersky Anti Targeted Attack Platform с использованием TLS-сертификата сервера Central Node. Kaspersky Anti Targeted Attack Platform не проверяет TLS-сертификат Kaspersky Endpoint Agent при попытке подключения Kaspersky Endpoint Agent.

   b. Настройка соединения с сервером Sensor без проверки TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform (см. раздел "Настройка соединения с сервером Central Node с проверкой TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform" на стр. 166)

      В Kaspersky Anti Targeted Attack Platform настроено перенаправление трафика на сервер Sensor (см. раздел "Настройка перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor" на стр. 177). Kaspersky Endpoint Agent устанавливает доверенное соединение с Kaspersky Anti Targeted Attack Platform с использованием TLS-сертификата сервера Sensor. Kaspersky Anti Targeted Attack Platform не проверяет TLS-сертификат Kaspersky Endpoint Agent при попытке подключения Kaspersky Endpoint Agent.

2. С использованием TLS-сертификатов Kaspersky Anti Targeted Attack Platform и Kaspersky Endpoint Agent. С проверкой TLS-сертификата Kaspersky Endpoint Agent на стороне Kaspersky Anti Targeted Attack Platform.

   a. Настройка соединения с сервером Central Node с проверкой TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform (см. раздел "Настройка соединения с сервером Sensor без проверки TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform" на стр. 167)

      Kaspersky Endpoint Agent устанавливает доверенное соединение с Kaspersky Anti Targeted Attack Platform с использованием TLS-сертификата сервера Central Node. В Kaspersky Endpoint Agent настроена дополнительная защита соединения и загружен TLS-сертификат Kaspersky Endpoint Agent. Kaspersky Anti Targeted Attack Platform проверяет TLS-сертификат Kaspersky Endpoint Agent при попытке подключения Kaspersky Endpoint Agent.

   b. Настройка соединения с сервером Sensor с проверкой TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform (на стр. 168)

      В Kaspersky Anti Targeted Attack Platform настроено перенаправление трафика на сервер Sensor (см. раздел "Настройка перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor" на стр. 177). Kaspersky Endpoint Agent устанавливает доверенное соединение с Kaspersky Anti Targeted Attack Platform с использованием TLS-сертификата сервера Sensor. В Kaspersky Endpoint Agent настроена дополнительная защита соединения и загружен TLS-сертификат Kaspersky Endpoint Agent. Kaspersky Anti Targeted Attack Platform проверяет TLS-сертификат Kaspersky Endpoint Agent при попытке подключения Kaspersky Endpoint Agent.

kaspersky

В этом разделе

Настройка соединения с сервером Central Node без проверки TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform 166

Настройка соединения с сервером Central Node с проверкой TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform 166

Настройка соединения с сервером Sensor без проверки TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform 167

Настройка соединения с сервером Sensor с проверкой TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform 168

Настройка соединения с сервером Central Node без проверки TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform

Kaspersky Endpoint Agent устанавливает доверенное соединение с Kaspersky Anti Targeted Attack Platform с использованием TLS-сертификата сервера Central Node. Kaspersky Anti Targeted Attack Platform не проверяет TLS-сертификат Kaspersky Endpoint Agent при попытке подключения Kaspersky Endpoint Agent.

Если вы используете этот вариант настройки доверенного соединения, настройка состоит из следующих этапов:

a. **Генерация (см. раздел "Генерация TLS-сертификата сервера Central Node в веб-интерфейсе Kaspersky Anti Targeted Attack Platform" на стр. 169) или загрузка самостоятельно подготовленного TLS-сертификата сервера Central Node в веб-интерфейсе Central Node (см. раздел "Загрузка самостоятельно подготовленного TLS-сертификата сервера Central Node через веб-интерфейс Kaspersky Anti Targeted Attack Platform" на стр. 170) (если TLS-сертификат сервера Central Node не был создан ранее)**

b. **Скачивание TLS-сертификата сервера Central Node на компьютер (на стр. 169)**

c. **Загрузка TLS-сертификата сервера Central Node в Kaspersky Endpoint Agent через Консоль администрирования (MMC) (см. раздел "Загрузка TLS-сертификата сервера Central Node или Sensor в Kaspersky Endpoint Agent" на стр. 171)**

Настройка соединения с сервером Central Node с проверкой TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform

Kaspersky Endpoint Agent устанавливает доверенное соединение с Kaspersky Anti Targeted Attack Platform с использованием TLS-сертификата сервера Central Node. В Kaspersky Endpoint Agent настроена дополнительная защита соединения и загружен TLS-сертификат Kaspersky Endpoint Agent. Kaspersky Anti Targeted Attack Platform проверяет TLS-сертификат Kaspersky Endpoint Agent при попытке подключения Kaspersky Endpoint Agent.

Если вы используете этот вариант настройки доверенного соединения, настройка состоит из следующих этапов:

a. **Генерация (см. раздел "Генерация TLS-сертификата сервера Central Node в веб-интерфейсе Kaspersky Anti Targeted Attack Platform" на стр. 169) или загрузка самостоятельно подготовленного TLS-сертификата сервера Central Node в веб-интерфейсе Central Node (см. раздел "Загрузка самостоятельно подготовленного TLS-сертификата сервера Central Node через веб-интерфейс Kaspersky Anti Targeted Attack Platform" на стр. 170) (если TLS-сертификат сервера Central Node не был создан ранее)**

b. **Скачивание TLS-сертификата сервера Central Node на компьютер (на стр. 169)**

c. **Загрузка TLS-сертификата сервера Central Node в Kaspersky Endpoint Agent через Консоль администрирования (MMC) (см. раздел "Настройка интеграции и доверенного соединения с Kaspersky Anti Targeted Attack Platform на стороне Kaspersky Endpoint Agent" на стр. 181)**

d. **Включение проверки TLS-сертификата Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform (на стр. 172)**

e. **Генерация и скачивание крипто-контейнера с TLS-сертификатом Kaspersky Endpoint Agent (см. раздел "Генерация TLS-сертификата Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform и скачивание крипто-контейнера" на стр. 173) или загрузка самостоятельно подготовленного TLS-сертификата Kaspersky Endpoint Agent через веб-интерфейс Kaspersky Anti Targeted Attack Platform (на стр. 173)**

> Если вы подготавливаете TLS-сертификат Kaspersky Endpoint Agent самостоятельно, вам нужно создать крипто-контейнер формата PFX с этим сертификатом. Подробнее о работе с TLS-сертификатами см. в документации OpenSSL.

f. **Загрузка крипто-контейнера с сертификатом Kaspersky Endpoint Agent в Kaspersky Endpoint Agent через Консоль администрирования (MMC) (см. раздел "Загрузка TLS-сертификата сервера Central Node или Sensor в Kaspersky Endpoint Agent" на стр. 171)**

Настройка соединения с сервером Sensor без проверки TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform

В Kaspersky Anti Targeted Attack Platform настроено перенаправление трафика на сервер Sensor (см. раздел "Настройка перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor" на стр. 177). Kaspersky Endpoint Agent устанавливает доверенное соединение с Kaspersky Anti Targeted Attack Platform с использованием TLS-сертификата сервера Sensor. Kaspersky Anti Targeted Attack Platform не проверяет TLS-сертификат Kaspersky Endpoint Agent при попытке подключения Kaspersky Endpoint Agent.

Если вы используете этот вариант настройки доверенного соединения, настройка состоит из следующих этапов:

a. **Включение перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor (см. раздел "Включение и отключение перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor" на стр. 178)**

b. **Авторизация компонента Sensor на сервере Central Node (на стр. 178)**

c. **Генерация (см. раздел "Генерация TLS-сертификата сервера Sensor в меню администратора сервера Sensor" на стр. 179) или загрузка самостоятельно подготовленного TLS-сертификата сервера Sensor через меню администратора сервера Sensor (на стр. 180)**

d. **Скачивание TLS-сертификата сервера Sensor на компьютер (на стр. 181)**

e. **Загрузка TLS-сертификата сервера Sensor в Kaspersky Endpoint Agent через Консоль администрирования (MMC) (см. раздел "Загрузка TLS-сертификата сервера Central Node или Sensor в Kaspersky Endpoint Agent" на стр. 171)**

Настройка соединения с сервером Sensor с проверкой TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform

В Kaspersky Anti Targeted Attack Platform настроено перенаправление трафика на сервер Sensor (см. раздел "Настройка перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor" на стр. 177). Kaspersky Endpoint Agent устанавливает доверенное соединение с Kaspersky Anti Targeted Attack Platform с использованием TLS-сертификата сервера Sensor. В Kaspersky Endpoint Agent настроена дополнительная защита соединения и загружен TLS-сертификат Kaspersky Endpoint Agent. Kaspersky Anti Targeted Attack Platform проверяет TLS-сертификат Kaspersky Endpoint Agent при попытке подключения Kaspersky Endpoint Agent.

Если вы используете этот вариант настройки доверенного соединения, настройка состоит из следующих этапов:

a. **Включение перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor (см. раздел "Включение и отключение перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor" на стр. 178)**

b. **Авторизация компонента Sensor на сервере Central Node (на стр. 178)**

c. **Генерация (см. раздел "Генерация TLS-сертификата сервера Sensor в меню администратора сервера Sensor" на стр. 179) или загрузка самостоятельно подготовленного TLS-сертификата сервера Sensor через меню администратора сервера Sensor (на стр. 180)**

d. **Скачивание TLS-сертификата сервера Sensor на компьютер (на стр. 181)**

e. **Загрузка TLS-сертификата сервера Sensor в Kaspersky Endpoint Agent через Консоль администрирования (MMC) (см. раздел "Загрузка TLS-сертификата сервера Central Node или Sensor в Kaspersky Endpoint Agent" на стр. 171)**

f. **Включение проверки TLS-сертификата Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform (на стр. 172)**

g. **Генерация и скачивание крипто-контейнера с TLS-сертификатом Kaspersky Endpoint Agent (см. раздел "Генерация TLS-сертификата Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform и скачивание крипто-контейнера" на стр. 173) или загрузка самостоятельно подготовленного TLS-сертификата Kaspersky Endpoint Agent через веб-интерфейс Kaspersky Anti Targeted Attack Platform (на стр. 173)**

> Если вы подготавливаете TLS-сертификат Kaspersky Endpoint Agent самостоятельно, вам нужно создать крипто-контейнер формата PFX с этим сертификатом. Подробнее о работе с TLS-сертификатами см. в документации OpenSSL.

h. **Загрузка крипто-контейнера с сертификатом Kaspersky Endpoint Agent в Kaspersky Endpoint Agent через консоль администрирования KSC (см. раздел "Настройка проверки TLS-сертификата Kaspersky Endpoint Agent сервером Central Node и загрузка крипто-контейнера в Kaspersky Endpoint Agent" на стр. 176)**

Скачивание TLS-сертификата сервера Central Node на компьютер

Чтобы скачать TLS-сертификат сервера на компьютер:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Сертификаты**.
2. В разделе **Сертификат сервера** нажмите на кнопку **Скачать**.

Файл сертификата сервера будет сохранен в папке загрузки браузера.

Генерация TLS-сертификата сервера Central Node в веб-интерфейсе Kaspersky Anti Targeted Attack Platform

Если вы уже используете TLS-сертификат сервера Central Node и сгенерируете новый сертификат, сертификат, который используется в приложении, будет удален и заменен на сгенерированный сертификат.
Вам потребуется указать данные нового сертификата везде, где использовался старый.

Если вы замените TLS-сертификат на новый, вам потребуется:

- Повторно авторизовать почтовые сенсоры (KSMG, KLMS) на Central Node (см. раздел "Настройка интеграции с внешними системами" на стр. 300).
- Повторно настроить соединение Central Node, PCN и SCN с Sandbox (см. раздел "Настройка интеграции с компонентом Sandbox" на стр. 297).
- Повторно настроить перенаправление трафика от Endpoint Agent на Sensor и доверенное соединение с Endpoint Agent (см. раздел "Настройка перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor" на стр. 177).
- Загрузить новый сертификат в Active Directory (если вы используете Active Directory).

Удалите все правила изоляции хостов Endpoint Agent. Соединение с изолированными хостами будет разорвано, вы не сможете ими управлять.

► *Чтобы сгенерировать TLS-сертификат сервера Central Node:*

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform (см. раздел "Начало работы в веб-интерфейсе приложения под учетной записью локального администратора" на стр. 186) под учетной записью администратора (см. раздел "Создание учетной записи администратора веб-интерфейса приложения" на стр. 194).
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Сертификаты**.
3. В разделе **Сертификат сервера** нажмите на кнопку **Сгенерировать**.

   Откроется окно подтверждения действия.
4. Нажмите на кнопку **Да**.

Kaspersky Anti Targeted Attack Platform сгенерирует новый TLS-сертификат. Страница автоматически обновится.

Загрузка самостоятельно подготовленного TLS-сертификата сервера Central Node через веб-интерфейс Kaspersky Anti Targeted Attack Platform

Вы можете самостоятельно подготовить TLS-сертификат и загрузить его через веб-интерфейс Kaspersky Anti Targeted Attack Platform.

Файл TLS-сертификата, предназначенный для загрузки, должен удовлетворять следующим требованиям:

- Файл должен содержать сам сертификат и закрытый ключ шифрования соединения.
- Файл должен иметь формат PEM.

  Приложение не работает с сертификатами другого формата.

  Если вы подготовили сертификат в другом формате, вам нужно конвертировать его в формат PEM.
- Длина закрытого ключа должна быть 2048 бит или более.

Подробнее о подготовке TLS-сертификатов к импорту см. в документации Open SSL.

Если вы уже используете TLS-сертификат сервера Central Node и загрузите новый сертификат, сертификат, который используется в приложении, будет удален и заменен на загруженный сертификат.
Вам потребуется указать данные нового сертификата везде, где использовался старый.

Если вы замените TLS-сертификат на новый, вам потребуется:

- Повторно авторизовать почтовые сенсоры (KSMG, KLMS) на Central Node (см. раздел "Настройка интеграции с внешними системами" на стр. 300).
- Повторно настроить соединение Central Node, PCN и SCN с Sandbox (см. раздел "Настройка интеграции с компонентом Sandbox" на стр. 297).
- Повторно настроить перенаправление трафика от Endpoint Agent на Sensor и доверенное соединение с Endpoint Agent (см. раздел "Настройка перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor" на стр. 177).

Удалите все правила изоляции хостов Endpoint Agent. Соединение с изолированными хостами будет разорвано, вы не сможете ими управлять.

► *Чтобы загрузить самостоятельно подготовленный TLS-сертификат через веб-интерфейс Kaspersky Anti Targeted Attack Platform:*

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform (см. раздел "Начало работы в веб-интерфейсе приложения под учетной записью локального администратора" на стр. 186) под учетной записью администратора (см. раздел "Создание учетной записи администратора веб-интерфейса приложения" на стр. 194).
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Сертификаты**.
3. В разделе **Сертификат сервера** нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.
4. Выберите файл TLS-сертификата, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

   TLS-сертификат будет добавлен в Kaspersky Anti Targeted Attack Platform.

   Повторно настроить перенаправление трафика от Endpoint Agent на Sensor и доверенное соединение с Endpoint Agent (см. раздел "Настройка перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor" на стр. 177).

Удалите все правила изоляции хостов Endpoint Agent. Соединение с изолированными хостами будет разорвано, вы не сможете ими управлять.

Загрузка TLS-сертификата сервера Central Node или Sensor в Kaspersky Endpoint Agent

► *Чтобы загрузить TLS-сертификат сервера Central Node или Sensor в Kaspersky Endpoint Agent:*

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Политики**.
3. В блоке политик Kaspersky Endpoint Agent выберите нужную политику и откройте ее свойства двойным щелчком мыши.

   Откроются свойства выбранной политики.
4. В разделе **Интеграция с KATA** выберите подраздел **Параметры интеграции с KATA**.
5. Установите флажок **Включить интеграцию с KATA**.
6. В поле **Адрес** введите адрес сервера Central Node программы Kaspersky Anti Targeted Attack Platform, с которым вы хотите настроить интеграцию, и выберите порт подключения. По умолчанию используется порт 443.
7. Установите флажок **Использовать закрепленный сертификат для защиты соединения**.
8. Нажмите на кнопку **Добавить TLS-сертификат...**.

   Откроется окно **Добавление TLS-сертификата**.

9. Выполните одно из следующих действий по добавлению TLS-сертификата, созданного на стороне Kaspersky Anti Targeted Attack Platform и скачанного на компьютер:
   - Добавьте файл сертификата. Для этого нажмите на кнопку **Обзор...**, в открывшемся окне выберите файл сертификата и нажмите на кнопку **Open**.
   - Скопируйте содержание файла сертификата в поле **Вставьте данные TLS-сертификата**.

   В Kaspersky Endpoint Agent может быть только один TLS-сертификат сервера Kaspersky Anti Targeted Attack Platform. Если вы добавляли TLS-сертификат ранее и снова добавили TLS-сертификат, только последний добавленный сертификат будет актуальным.
   Если вы настроили перенаправление трафика на сервер с компонентом Sensor, вам нужно загрузить TLS-сертификат сервера Sensor, предварительно скачанный на компьютер (см. раздел "Скачивание TLS-сертификата сервера Sensor на компьютер" на стр. 181).

10. Нажмите на кнопку **Добавить**.

    Информация о добавленном TLS-сертификате отобразится в разделе интеграции с Kaspersky Anti Targeted Attack Platform.

11. Убедитесь, что переключатель в правом верхнем углу блока параметров находится в положении **Политика применяется**.
12. Нажмите на кнопку **OK**.

TLS-сертификат сервера Central Node будет загружен в Endpoint Agent.

Включение проверки TLS-сертификата Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform

► *Чтобы включить использование доверенного соединения с Kaspersky Endpoint Agent:*

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform (см. раздел "Начало работы в веб-интерфейсе приложения под учетной записью локального администратора" на стр. 186) под учетной записью администратора (см. раздел "Создание учетной записи администратора веб-интерфейса приложения" на стр. 194).
2. В окне веб-интерфейса Kaspersky Anti Targeted Attack Platform выберите раздел **Параметры**, подраздел **Сертификаты**.
3. В разделе **Сертификаты Endpoint Agent** включите переключатель **Проверять TLS-сертификаты Endpoint Agent**.

Kaspersky Anti Targeted Attack Platform будет проверять данные TLS-сертификата при попытках подключения Kaspersky Endpoint Agent к Kaspersky Anti Targeted Attack Platform.

Генерация TLS-сертификата Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform и скачивание крипто-контейнера

► *Чтобы сгенерировать TLS-сертификат соединения Kaspersky Anti Targeted Attack Platform с Kaspersky Endpoint Agent:*

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform (см. раздел "Начало работы в веб-интерфейсе приложения под учетной записью локального администратора" на стр. 186) под учетной записью администратора (см. раздел "Создание учетной записи администратора веб-интерфейса приложения" на стр. 194).
2. В окне веб-интерфейса Kaspersky Anti Targeted Attack Platform выберите раздел **Параметры**, подраздел **Сертификаты**.
3. В разделе **Сертификаты Endpoint Agent** нажмите на кнопку **Сгенерировать**.

Новый TLS-сертификат отобразится в таблице TLS-сертификатов. На ваш локальный компьютер в папку загрузки браузера будет загружен файл крипто-контейнера с сертификатом Kaspersky Endpoint Agent в формате PFX.

Вы можете использовать крипто-контейнер для настройки проверки TLS-сертификата Kaspersky Endpoint Agent сервером Central Node при попытке подключения к Kaspersky Anti Targeted Attack Platform (см. раздел "Настройка проверки TLS-сертификата Kaspersky Endpoint Agent сервером Central Node и загрузка крипто-контейнера в Kaspersky Endpoint Agent" на стр. 176).

По умолчанию крипто-контейнер не защищен паролем. Вы можете установить пароль крипто-контейнера. Подробнее о работе с TLS-сертификатами см. в документации OpenSSL.

> В крипто-контейнере содержится только файл сертификата и не содержится файл закрытого ключа. Kaspersky Anti Targeted Attack Platform не хранит закрытые ключи TLS-шифрования соединения.

Загрузка самостоятельно подготовленного TLS-сертификата Kaspersky Endpoint Agent через веб-интерфейс Kaspersky Anti Targeted Attack Platform

Вы можете самостоятельно подготовить TLS-сертификат и загрузить его через веб-интерфейс Kaspersky Anti Targeted Attack Platform.

Файл TLS-сертификата, предназначенный для загрузки, должен удовлетворять следующим требованиям:

- Файл должен содержать сам сертификат и закрытый ключ шифрования соединения.
- Файл должен иметь формат PEM.
- Длина закрытого ключа должна быть 2048 бит или более.

Подробнее о подготовке TLS-сертификатов к импорту см. в документации Open SSL.

Если вы подготавливаете TLS-сертификат Kaspersky Endpoint Agent самостоятельно, вам нужно создать крипто-контейнер формата PFX с этим сертификатом и загрузить крипто-контейнер в Kaspersky Endpoint

Agent (см. раздел "Настройка проверки TLS-сертификата Kaspersky Endpoint Agent сервером Central Node и загрузка крипто-контейнера в Kaspersky Endpoint Agent" на стр. 176).

Вы можете использовать крипто-контейнер для настройки проверки TLS-сертификата Kaspersky Endpoint Agent сервером Central Node при попытке подключения к Kaspersky Anti Targeted Attack Platform (см. раздел "Настройка проверки TLS-сертификата Kaspersky Endpoint Agent сервером Central Node и загрузка крипто-контейнера в Kaspersky Endpoint Agent" на стр. 176).

Подробнее о работе с TLS-сертификатами см. в документации OpenSSL.

В крипто-контейнере должен содержится только файл сертификата и не должен содержится файл закрытого ключа. Kaspersky Anti Targeted Attack Platform не хранит закрытые ключи TLS-шифрования соединения.

► *Чтобы загрузить самостоятельно подготовленный TLS-сертификат Kaspersky Endpoint Agent через веб-интерфейс Kaspersky Anti Targeted Attack Platform:*

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform (см. раздел "Начало работы в веб-интерфейсе приложения под учетной записью локального администратора" на стр. 186) под учетной записью администратора (см. раздел "Создание учетной записи администратора веб-интерфейса приложения" на стр. 194).
2. В окне веб-интерфейса Kaspersky Anti Targeted Attack Platform выберите раздел **Параметры**, подраздел **Сертификаты**.
3. В разделе **Сертификаты Endpoint Agent** нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.
4. Выберите файл TLS-сертификата, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

TLS-сертификат будет добавлен в Kaspersky Anti Targeted Attack Platform.

Просмотр таблицы TLS-сертификатов Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform

► *Чтобы просмотреть список TLS-сертификатов соединения с Kaspersky Endpoint Agent через веб-интерфейс Kaspersky Anti Targeted Attack Platform:*

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform (см. раздел "Начало работы в веб-интерфейсе приложения под учетной записью локального администратора" на стр. 186) под учетной записью администратора (см. раздел "Создание учетной записи администратора веб-интерфейса приложения" на стр. 194).
2. В окне веб-интерфейса Kaspersky Anti Targeted Attack Platform выберите раздел **Параметры**, подраздел **Сертификаты**.
3. В разделе **Сертификаты Endpoint Agent** отобразится список TLS-сертификатов со следующими данными по каждому сертификату:

- **TLS-сертификат** - отпечаток сертификата.
- **Серийный номер** - серийный номер сертификата.
- **Истекает** - дата истечения срока действия сертификата.

Фильтрация и поиск TLS-сертификатов Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform

Вы можете отфильтровать TLS-сертификаты для отображения в таблице по одной или обеим столбцам **TLS-сертификат** и **Серийный номер** или выполнить поиск TLS-сертификатов по этим столбцам таблицы по указанным вами показателям.

► *Чтобы выполнить фильтрацию и поиск TLS-сертификатов в таблице:*

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform (см. раздел "Начало работы в веб-интерфейсе приложения под учетной записью локального администратора" на стр. 186) под учетной записью администратора (см. раздел "Создание учетной записи администратора веб-интерфейса приложения" на стр. 194).
2. В окне веб-интерфейса Kaspersky Anti Targeted Attack Platform выберите раздел **Параметры**, подраздел **Сертификаты**.
3. В разделе **Сертификаты Endpoint Agent** отобразится список TLS-сертификатов со следующими данными по каждому сертификату:
   - **TLS-сертификат** - отпечаток сертификата.
   - **Серийный номер** - серийный номер сертификата.
   - **Истекает** - дата истечения срока действия сертификата.
4. Если вы хотите отфильтровать или найти TLS-сертификаты по отпечатку сертификата:
   a. По ссылке **TLS-сертификат** откройте окно настройки фильтрации.
   b. В поле **TLS-сертификат** введите несколько символов отпечатка сертификата.
   c. Нажмите на кнопку **Применить**.
5. Если вы хотите отфильтровать или найти TLS-сертификаты по серийному номеру:
   a. По ссылке **Серийный номер** откройте окно настройки фильтрации.
   b. В поле **Серийный номер** введите несколько символов серийного номера.
   c. Нажмите на кнопку **Применить**.

В таблице отобразятся только TLS-сертификаты, соответствующие заданным вами условиям.

► *Чтобы сбросить фильтр по одному или нескольким условиям фильтрации,*

нажмите на кнопку ☒ справа от того заголовка столбца таблицы, условия фильтрации по которому вы хотите сбросить.

Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

Удаление TLS-сертификатов Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform

► *Чтобы удалить один или несколько TLS-сертификатов соединения с Kaspersky Endpoint Agent через веб-интерфейс Kaspersky Anti Targeted Attack Platform:*

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform (см. раздел "Начало работы в веб-интерфейсе приложения под учетной записью локального администратора" на стр. 186) под учетной записью администратора (см. раздел "Создание учетной записи администратора веб-интерфейса приложения" на стр. 194).
2. В окне веб-интерфейса Kaspersky Anti Targeted Attack Platform выберите раздел **Параметры**, подраздел **Сертификаты Endpoint Agent**.

   В разделе **Сертификаты Endpoint Agent** отобразится список TLS-сертификатов.
3. Установите флажки рядом с одним или несколькими TLS-сертификатами, которые вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.
5. Нажмите на кнопку **Да**.

Выбранные TLS-сертификаты будут удалены.

Настройка проверки TLS-сертификата Kaspersky Endpoint Agent сервером Central Node и загрузка крипто-контейнера в Kaspersky Endpoint Agent

► *Чтобы настроить проверку TLS-сертификата Kaspersky Endpoint Agent сервером Central Node и загрузить крипто-контейнер с сертификатом Kaspersky Endpoint Agent в Kaspersky Endpoint Agent:*

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Политики**.
3. В блоке политик Kaspersky Endpoint Agent выберите нужную политику и откройте ее свойства двойным щелчком мыши.

   Откроются свойства выбранной политики.
4. В разделе **Интеграция с KATA** выберите подраздел **KATA Central Node**.
5. Нажмите на кнопку **Настроить дополнительную защиту**.

6. В открывшемся окне установите флажок **Защита подключения с помощью клиентского сертификата**.
7. Нажмите на кнопку **Загрузить**.

   Откроется окно выбора файла на вашем локальном компьютере.
8. Выберите файл крипто-контейнера сертификата Kaspersky Endpoint Agent, сгенерированного на сервере Kaspersky Anti Targeted Attack Platform и скачанного на жесткий диск вашего компьютера.
9. Нажмите на кнопку **OK**.

   Окно закроется.
10. Убедитесь, что переключатель в правом верхнем углу блока параметров находится в положении **Политика применяется**.
11. Нажмите на кнопку **OK**.

Крипто-контейнер с сертификатом Kaspersky Endpoint Agent будет загружен в Kaspersky Endpoint Agent. Kaspersky Anti Targeted Attack Platform будет проверять TLS-сертификат Kaspersky Endpoint Agent при попытке подключения.

Настройка перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor

Вы можете использовать сервер с компонентом Sensor в качестве прокси-сервера при обмене данными между приложением Kaspersky Endpoint Agent и компонентом Central Node, чтобы снизить нагрузку на компонент Central Node.

При настройке перенаправления трафика учитывайте следующие ограничения:

- Максимальный объем входящего трафика для компонента Sensor не должен превышать 1 Гбит/с.
- Рекомендуемая ширина канала между серверами с компонентами Central Node и Sensor составляет 15% от трафика на SPAN-порте.
- Максимально допустимые потери пакетов, пересылаемых между серверами с компонентами Sensor и Central Node, составляют 10% при задержке отправки пакетов до 100 мс.

Вы можете использовать компонент Sensor в качестве прокси-сервера, только если компоненты Sensor и Central Node расположены на разных серверах.
Если вы используете компонент Sensor в качестве прокси-сервера, убедитесь, что при интеграции Kaspersky Anti Targeted Attack Platform с приложением Kaspersky Endpoint Agent на стороне Kaspersky Endpoint Agent вместо IP-адреса Central Node вы указали IP-адрес компонента Sensor.

В этом разделе

Включение и отключение перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor178

Авторизация компонента Sensor на сервере Central Node 178

Включение и отключение перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor

► *Чтобы включить или отключить использование компонента Sensor в качестве прокси-сервера при обмене данными между приложением Kaspersky Endpoint Agent и компонентом Central Node, выполните следующие действия в меню администратора сервера с компонентом Sensor (см. раздел "Начало работы в меню администратора приложения" на стр. 188):*

1. В главном окне меню администратора выберите пункт **Program settings**.
2. Нажмите на клавишу **ENTER**.

   Откроется следующее окно меню администратора.
3. Выберите пункт **Configure Central Node**.
4. Нажмите на клавишу **ENTER**.
5. В открывшемся окне укажите IP-адрес сервера с компонентом Central Node.
6. Нажмите на кнопку **Ok**.

   Откроется окно с информацией о сертификате компонента Central Node.
7. Убедитесь, что отображаемый сертификат совпадает с сертификатом компонента Central Node, который вы скачали.
8. Нажмите на кнопку **Accept**.
9. Если соединение с компонентом Central Node уже установлено или запрос на авторизацию отправлен, в открывшемся окне подтверждения действия нажмите на кнопку **Yes**.

Использование компонента Sensor в качестве прокси-сервера будет отключено после подтверждения авторизации на сервере с компонентом Central Node.

Авторизация компонента Sensor на сервере Central Node

► *Чтобы авторизовать компонент Sensor на сервере с компонентом Central Node, выполните следующие действия в меню администратора сервера с компонентом Central Node (см. раздел "Начало работы в меню администратора приложения" на стр. 188):*

1. В главном окне меню администратора выберите пункт **Program settings**.
2. Нажмите на клавишу **ENTER**.

   Откроется следующее окно меню администратора.
3. Выберите пункт **Configure Sensor connections**.

   Откроется окно со списком запросов на авторизацию от серверов с компонентом Sensor.
4. В нижней части окна выберите IP-адрес сервера с компонентом Sensor, запрос на авторизацию от которого вы хотите подтвердить или отклонить.

   Откроется окно подтверждения авторизации.
5. Если вы хотите авторизовать выбранный сервер с компонентом Sensor, выберите пункт **Accept Sensor**.

Запрос на авторизацию будет подтвержден.

6. Если вы хотите отклонить авторизацию выбранного сервера с компонентом Sensor, выберите пункт **Reject Sensor**.

   Запрос на авторизацию будет отклонен.

Генерация TLS-сертификата сервера Sensor в меню администратора сервера Sensor

► *Чтобы сгенерировать TLS-сертификат сервера с компонентом Sensor, выполните следующие действия в меню администратора сервера с компонентом Sensor (см. раздел "Начало работы в меню администратора приложения" на стр. 188):*

1. В главном окне меню администратора выберите пункт **Program settings**.
2. Нажмите на клавишу **ENTER**.

   Откроется следующее окно меню администратора.
3. Выберите пункт **Manage server certificate**.
4. Нажмите на клавишу **ENTER**.

   Откроется окно **Certificate management**.
5. В нижней части окна выберите пункт **New**.
6. Нажмите на клавишу **ENTER**.

   Откроется окно с информацией о новом сертификате.
7. Нажмите на кнопку **Continue**.

   Откроется окно подтверждения действия.
8. Нажмите на кнопку **Generate**.

   Начнется создание сертификата.
9. По окончании создания сертификата нажмите на клавишу **ENTER**.

   Откроется окно с информацией об установленном сертификате.
10. Нажмите на кнопку **Continue**.

    Откроется окно подтверждения действия.
11. Нажмите на кнопку **Ok**.

Сертификат будет создан. Данные сертификатов, установленных ранее, будут перезаписаны.

Загрузка самостоятельно подготовленного TLS-сертификата сервера Sensor через меню администратора сервера Sensor

Вы можете самостоятельно подготовить TLS-сертификат и загрузить его на сервер с компонентом Sensor по протоколу SCP. Подробнее о способах загрузки файлов по протоколу SCP см. в документации к операционной системе, установленной на том компьютере, с которого вы хотите загрузить TLS-сертификат.

Файл TLS-сертификата, предназначенный для загрузки на сервер, должен удовлетворять следующим требованиям:

- Файл должен содержать сам сертификат и закрытый ключ шифрования соединения.
- Файл должен иметь формат PEM.
- Имя файла должно быть kata.pem.
- Длина закрытого ключа должна быть 2048 бит или более.

Подробнее о подготовке TLS-сертификатов к импорту см. в документации Open SSL.

► *Чтобы загрузить самостоятельно подготовленный TLS-сертификат на сервер с компонентом Sensor по протоколу SCP, выполните следующие действия в интерфейсе работы по протоколу SCP вашего компьютера (на примере операционной системы Linux):*

1. Выполните команду `scp kata.pem admin@<IP-адрес сервера с компонентом Sensor>:`
2. На приглашение ввести пароль введите пароль администратора для работы в меню администратора сервера с компонентом Sensor, заданный при установке (см. раздел "Установка и первоначальная настройка приложения" на стр. 110).

TLS-сертификат будет загружен на сервер с компонентом Sensor.

► *Чтобы применить загруженный TLS-сертификат на сервере с компонентом Sensor, выполните следующие действия в меню администратора сервера с компонентом Sensor (см. раздел "Начало работы в меню администратора приложения" на стр. 188):*

1. В главном окне меню администратора выберите пункт **Program settings**.
2. Нажмите на клавишу **ENTER**.

   Откроется следующее окно меню администратора.
3. Выберите пункт **Manage server certificate**.
4. Нажмите на клавишу **ENTER**.

   Откроется окно **Certificate management**.
5. В нижней части окна выберите пункт **kata.pem**.
6. Нажмите на клавишу **ENTER**.

   Откроется окно **Uploaded certificate**.
7. Выберите пункт **Install certificate**.
8. Нажмите на клавишу **ENTER**.

   Откроется окно подтверждения действия.

9. Нажмите на кнопку **Yes**.

   Откроется окно с информацией о сертификате.

10. Нажмите на кнопку **Continue**.

    Откроется окно подтверждения действия.

11. Нажмите на кнопку **Install**.

    Начнется установка сертификата.

12. По окончании установки сертификата нажмите на клавишу **ENTER**.

    Откроется окно с информацией о примененном сертификате.

13. Нажмите на кнопку **Continue**.

    Откроется окно подтверждения действия.

14. Нажмите на кнопку **Ok**.

Сертификат будет применен. Данные сертификатов, установленных ранее, будут перезаписаны.

Скачивание TLS-сертификата сервера Sensor на компьютер

Вы можете скачать TLS-сертификат с сервера Sensor на любой компьютер, имеющий доступ к серверу с компонентом Sensor, по протоколу SCP. Подробнее о способах загрузки файлов по протоколу SCP см. в документации к операционной системе, установленной на том компьютере, на который вы хотите скачать TLS-сертификат.

► *Чтобы скачать TLS-сертификат с сервера с компонентом Sensor по протоколу SCP, выполните следующие действия в интерфейсе работы по протоколу SCP вашего компьютера (на примере операционной системы Linux):*

1. Выполните команду `scp admin@<IP-адрес сервера с компонентом Sensor>:ssl/kata.crt`.
2. На приглашение ввести пароль введите пароль администратора для работы в меню администратора сервера с компонентом Sensor, заданный при установке.

TLS-сертификат будет загружен с сервера с компонентом Sensor в текущую директорию.

Настройка интеграции и доверенного соединения с Kaspersky Anti Targeted Attack Platform на стороне Kaspersky Endpoint Agent

► *Чтобы настроить интеграцию с Kaspersky Anti Targeted Attack Platform на стороне Kaspersky Endpoint Agent:*

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Политики**.

3. В блоке политик Kaspersky Endpoint Agent выберите нужную политику и откройте ее свойства двойным щелчком мыши.

   Откроются свойства выбранной политики.

4. В разделе **Интеграция с KATA** выберите подраздел **Параметры интеграции с KATA**.

5. Установите флажок **Включить интеграцию с KATA**.

6. В поле **Адрес** введите адрес сервера Central Node программы Kaspersky Anti Targeted Attack Platform, с которым вы хотите настроить интеграцию, и выберите порт подключения. По умолчанию используется порт 443.

7. Установите флажок **Использовать закрепленный сертификат для защиты соединения**.

8. Нажмите на кнопку **Добавить TLS-сертификат...**.

   Откроется окно **Добавление TLS-сертификата**.

9. Выполните одно из следующих действий по добавлению TLS-сертификата, созданного на стороне Kaspersky Anti Targeted Attack Platform и скачанного на компьютер:

   - Добавьте файл сертификата. Для этого нажмите на кнопку **Обзор...**, в открывшемся окне выберите файл сертификата и нажмите на кнопку **Open**.
   - Скопируйте содержание файла сертификата в поле **Вставьте данные TLS-сертификата**.

   В Kaspersky Endpoint Agent может быть только один TLS-сертификат сервера Kaspersky Anti Targeted Attack Platform. Если вы добавляли TLS-сертификат ранее и снова добавили TLS-сертификат, только последний добавленный сертификат будет актуальным.
   Если вы настроили перенаправление трафика на сервер с компонентом Sensor, вам нужно загрузить TLS-сертификат сервера Sensor, предварительно скачанный на компьютер (см. раздел "Скачивание TLS-сертификата сервера Sensor на компьютер" на стр. 181).

10. Нажмите на кнопку **Добавить**.

    Информация о добавленном TLS-сертификате отобразится в разделе интеграции с Kaspersky Anti Targeted Attack Platform.

11. Нажмите на кнопку **Добавить сертификат клиента...**.

12. В открывшемся окне установите флажок **Защита подключения с помощью сертификата клиента**.

13. Нажмите на кнопку **Загрузить**.

    Откроется окно выбора файла на вашем локальном компьютере.

14. Выберите файл крипто-контейнера сертификата Kaspersky Endpoint Agent, сгенерированного на сервере Kaspersky Anti Targeted Attack Platform и скачанного на жесткий диск вашего компьютера.

15. Нажмите на кнопку **OK**.

    Окно закроется.

16. В поле **Время ожидания (сек.):** укажите максимальное время ожидания ответа сервера Central Node приложения Kaspersky Anti Targeted Attack Platform в секундах.

17. В поле **Отправлять запрос на синхронизацию на сервер KATA каждые (мин.)** укажите интервал в минутах.

18. Если вы хотите, чтобы Kaspersky Endpoint Agent не отправлял на сервер Kaspersky Anti Targeted Attack Platform информацию о процессах, которые запускаются повторно, установите флажок

Использовать период TTL при отправке событий. Kaspersky Endpoint Agent не считает запуск процесса повторным, если запуск происходит после окончания очередного периода TTL.

19. Если вы установили флажок Использовать период TTL при отправке событий, укажите время в поле **Период TTL (мин.)**.
20. Убедитесь, что переключатель в правом верхнем углу блока параметров находится в положении **Политика применяется**.
21. Нажмите на кнопку **OK**.

Интеграция с Kaspersky Anti Targeted Attack Platform на стороне Kaspersky Endpoint Agent будет настроена.

Разделение доступа к функциям приложения по пользовательским ролям

В зависимости от назначенной роли пользователю будут доступны определенные разделы веб-интерфейса и функционал приложения. Информация о возможных ролях и функциональности, доступной пользователям с этими ролями, приведена в таблице ниже.

Таблица 31. Функциональность, доступная для пользователей в зависимости от роли

Роль	Функциональность
Старший сотрудник службы безопасности	• Мониторинг работы компонентов приложения. • Работа с обнаружениями: просмотр таблицы обнаружений, фильтрация и поиск обнаружений, просмотр и работа с каждым обнаружением, выполнение рекомендаций по оценке и расследованию инцидентов. • Просмотр таблицы событий, зарегистрированных на компьютерах и серверах, входящих в IT-инфраструктуру организации, поиск угроз, фильтрация, просмотр и работа с каждым событием, выполнение рекомендаций по оценке и расследованию инцидентов. • Включение и отключение автоматической отправки файлов с хостов с компонентом Endpoint Agent на проверку компоненту Sandbox. • Просмотр информации о хостах с компонентом Endpoint Agent. • Выполнение задач на хостах с компонентом Endpoint Agent: запуск программы и остановка процессов, экспорт и удаление файлов, помещение объектов на карантин на хостах с компонентом Endpoint Agent и копий файлов в Хранилище программы, восстановление файлов из карантина, проверка хостов с помощью правил YARA, управление службами, сбор данных с хостов (список файлов, процессов и точек автозапуска). • Настройка политик запрета запуска файлов и процессов, которые могут быть небезопасными, на выбранных хостах с компонентом Endpoint Agent. • Изоляция отдельных хостов с компонентом Endpoint Agent от сети. • Работа с правилами TAA (IOA) для классификации и анализа событий. • Работа с пользовательскими правилами Targeted Attack Analyzer TAA (IOA), Intrusion Detection System (IDS) и YARA: загрузка правил, по которым программа будет проверять события и создавать обнаружения. • Работа с файлами открытого стандарта описания индикаторов компрометации OpenIOC (IOC-файлами) для поиска признаков целевых атак, зараженных и возможно зараженных объектов на хостах с компонентом Endpoint Agent и в базе обнаружений. • Добавление правил TAA (IOA) и правила IDS, предоставленные специалистами "Лаборатории Касперского", в исключения из проверки. • Работа с объектами на карантине и копиями объектов в Хранилище. • Управление отчетами о работе приложения и отчетами об обнаружениях. • Настройка отправки уведомлений об обнаружениях и о проблемах в работе приложения на адреса электронной почты пользователей. • Работа со списком обнаружений со статусом VIP, со списком данных, исключенных из проверки, наполнение локальной репутационной базы KPSN. • Создание списка паролей для архивов. • Выгрузка копий сырого сетевого трафика для анализа во внешних системах.

Сотрудник службы безопасности	• Просмотр пользовательских правил Targeted Attack Analyzer TAA (IOA) и YARA. • Просмотр списка импортированных IOC-файлов. • Просмотр списка данных, исключенных из проверки. • Мониторинг работы приложения. • Работа с обнаружениями: просмотр таблицы обнаружений, фильтрация и поиск обнаружений, просмотр и работа с каждым обнаружением, выполнение рекомендаций по оценке и расследованию инцидентов. • Просмотр таблицы событий, зарегистрированных на компьютерах и серверах, входящих в IT-инфраструктуру организации, поиск угроз, фильтрация, просмотр и работа с каждым событием, выполнение рекомендаций по оценке и расследованию инцидентов. • Просмотр информации о хостах с компонентом Endpoint Agent. • Работа с правилами TAA (IOA) для классификации и анализа событий. • Работа с объектами на карантине и копиями объектов в Хранилище. • Настройка отправки уведомлений об обнаружениях и о проблемах в работе приложения на адреса электронной почты пользователей. • Выгрузка копий сырого сетевого трафика для анализа во внешних системах.
Аудитор	• Мониторинг работы программы. • Просмотр таблицы обнаружений, фильтрация и поиск обнаружений, просмотр данных каждого обнаружения. • Просмотр таблицы событий, происходящих на компьютерах и серверах, входящих в IT-инфраструктуру организации, поиск угроз, фильтрация и просмотр каждого события. • Просмотр списка хостов с компонентом Endpoint Agent и информации о выбранных хостах. • Просмотр пользовательских правил Targeted Attack Analyzer TAA (IOA), Intrusion Detection System (IDS) и YARA. • Просмотр списка импортированных IOC-файлов. • Просмотр исключенных из проверки правил TAA (IOA) и правил IDS, предоставленных специалистами "Лаборатории Касперского". • Просмотр отчетов о работе приложения и отчетов об обнаружениях. • Просмотр списка обнаружений со статусом VIP, списка данных, исключенных из проверки. • Просмотр всех настроек, производимых в веб-интерфейсе приложения. • Выгрузка копий сырого сетевого трафика для анализа во внешних системах.
Локальный администратор и Администратор	• Настройка параметров работы приложения. • Настройка серверов для работы в режиме распределенного решения и multitenancy. • Настройка интеграции приложения с другими программами и системами. • Работа с TLS-сертификатами и настройка доверенного соединения сервера Central Node с сервером Sandbox, а также серверов Kaspersky Anti Targeted Attack Platform с компонентом Endpoint Agent и с внешними системами. • Управление учетными записями пользователей приложения. • Мониторинг работоспособности приложения. • Сохранение копий сырого сетевого трафика для анализа во внешних системах.

kaspersky

Начало работы с приложением

Этот раздел содержит информацию о том, как начать работу с приложением в веб-интерфейсе, в меню администратора и в режиме Technical Support Mode.

В этом разделе

Начало работы в веб-интерфейсе приложения под учетной записью локального администратора 186

Начало работы в веб-интерфейсе для управления масштабированием 187

Начало работы в меню администратора приложения 188

Начало работы с приложением в режиме Technical Support Mode 189

Начало работы в веб-интерфейсе приложения под учетной записью локального администратора

Веб-интерфейс Kaspersky Anti Targeted Attack Platform защищен от *CSRF-атак* и работает только в том случае, если браузер пользователя веб-интерфейса приложения предоставляет заголовок Referrer HTTP-запроса POST. Убедитесь, что браузер, который вы используете для работы с веб-интерфейсом Kaspersky Anti Targeted Attack Platform, не модифицирует заголовок Referrer HTTP-запроса POST. Если соединение с веб-интерфейсом Kaspersky Anti Targeted Attack Platform осуществляется через прокси-сервер вашей организации, убедитесь, что прокси-сервер не модифицирует заголовок Referrer HTTP-запроса POST.

После установки (см. раздел "Установка и первоначальная настройка приложения" на стр. 110) Kaspersky Anti Targeted Attack Platform вам требуется настроить параметры масштабирования приложения в веб-интерфейсе для управления масштабированием (см. раздел "Начало работы в веб-интерфейсе для управления масштабированием" на стр. 187).

Если параметры масштабирования Kaspersky Anti Targeted Attack Platform не настроены, вход в веб-интерфейс под учетной записью локального администратора недоступен.

► *Чтобы начать работу в веб-интерфейсе приложения под учетной записью локального администратора:*

1. В браузере на любом компьютере, на котором разрешен доступ к серверу Central Node, в адресной строке браузера введите IP-адрес сервера с компонентом Central Node.

   Если вы используете отказоустойчивую версию приложения, вы можете ввести IP-адрес любого сервера кластера Central Node или полное доменное имя (FQDN) кластера.

   Откроется окно ввода учетных данных пользователя Kaspersky Anti Targeted Attack Platform.

2. Введите имя учетной записи Administrator и пароль Administrator.

Пароль Administrator используется по умолчанию. Настоятельно рекомендуется изменить пароль (см. раздел "Изменение пароля учетной записи администратора или пользователя приложения" на стр. 201) для этой учетной записи после входа в веб-интерфейс приложения.

3. Установите флажок **Локальный администратор**.
4. Нажмите на кнопку **Войти**.

   Откроется страница **Мониторинг** веб-интерфейса приложения.

Вы можете начать работу с приложением под учетной записью локального администратора.

Количество одновременных сеансов работы с приложением под одной учетной записью ограничено одним IP-адресом. При попытке входа в приложение под этим же именем пользователя с другого IP-адреса, первый сеанс работы с приложением завершается.

Начало работы в веб-интерфейсе для управления масштабированием

В веб-интерфейсе для управления масштабированием вы можете выполнять следующие действия:

- Управлять серверами кластера Central Node (см. раздел "Управление кластером" на стр. 277).
- Настраивать конфигурацию серверов с компонентом Central Node.

Веб-интерфейс Kaspersky Anti Targeted Attack Platform для управления масштабированием защищен от *CSRF-атак* и работает только в том случае, если браузер пользователя веб-интерфейса приложения предоставляет заголовок Referrer HTTP-запроса POST. Убедитесь, что браузер, который вы используете для работы с веб-интерфейсом Kaspersky Anti Targeted Attack Platform, не модифицирует заголовок Referrer HTTP-запроса POST. Если соединение с веб-интерфейсом Kaspersky Anti Targeted Attack Platform осуществляется через прокси-сервер вашей организации, убедитесь, что прокси-сервер не модифицирует заголовок Referrer HTTP-запроса POST.

Веб-интерфейс для управления масштабированием расположен на сервере с компонентом Central Node.

► *Чтобы начать работу в веб-интерфейсе для управления масштабированием:*

1. В браузере на любом компьютере, на котором разрешен доступ к серверу Central Node, в адресной строке браузера введите IP-адрес сервера с компонентом Central Node.

   Если вы используете отказоустойчивую версию приложения, вы можете ввести IP-адрес любого сервера кластера Central Node или полное доменное имя (FQDN) кластера.

   Откроется окно ввода учетных данных пользователя Kaspersky Anti Targeted Attack Platform.
2. Введите имя учетной записи администратора admin и пароль, заданный при установке приложения (см. раздел "Установка и первоначальная настройка приложения" на стр. 110).

Вы можете начать работу в веб-интерфейсе для управления масштабированием.

Для отказоустойчивой версии приложения в веб-интерфейсе отображаются разделы **Кластер** и **Конфигурация серверов**.

Если вы используете неотказоустойчивую версию приложения, в веб-интерфейсе отображается только раздел **Конфигурация серверов**.

Количество одновременных сеансов работы с приложением под одной учетной записью ограничено одним IP-адресом. При попытке входа в приложение под этим же именем пользователя с другого IP-адреса, первый сеанс работы с приложением завершается.

Начало работы в меню администратора приложения

Вы можете работать с параметрами каждого из компонентов приложения Sensor, Central Node и Sandbox в меню администратора в консоли управления каждого сервера, на котором установлен компонент приложения.

Убедитесь что доступ к меню администратора и консоли управления серверами Kaspersky Anti Targeted Attack Platform есть только с тех компьютеров, которым вы разрешили этот доступ. Убедитесь, что компьютеры, которым вы разрешаете доступ, находятся в защищенном периметре вашей сети.
Вы можете настроить доступ к меню администратора и консоли управления серверами Kaspersky Anti Targeted Attack Platform с определенных компьютеров, с помощью утилиты командной строки iptables. Подробнее о работе с iptables см. документацию к iptables.

► *Чтобы начать работу в меню администратора компонента Sandbox, Sensor или Central Node в консоли управления сервером с нужным компонентом:*

1. Войдите в консоль управления того сервера, параметры которого вы хотите изменить, по протоколу SSH или через терминал.

   Отобразится меню администратора компонента приложения.

2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке приложения (см. раздел "Установка и первоначальная настройка приложения" на стр. 110).

   Отобразится меню администратора компонента приложения.

Вы можете начать работу в меню администратора компонента Sensor или Sandbox.

Начало работы с приложением в режиме Technical Support Mode

Не рекомендуется выполнять действия с Kaspersky Anti Targeted Attack Platform в режиме Technical Support Mode без консультации или указания сотрудников Службы технической поддержки.

Вы можете работать с компонентами приложения Sensor, Central Node и Sandbox в режиме Technical Support Mode.

Режим Technical Support Mode предоставляет администратору Kaspersky Anti Targeted Attack Platform неограниченные права (root) доступа к приложении и всем данным (в том числе персональным), которые в ней хранятся.

Работа с Kaspersky Anti Targeted Attack Platform из консоли управления в режиме Technical Support Mode с правами учетной записи суперпользователя позволяет выполнять следующие действия:

- Управлять параметрами работы приложения с помощью конфигурационных файлов.

  При этом могут быть изменены параметры шифрования данных при передаче между узлами приложения, параметры хранения и обработки объектов проверки.

  В этом случае данные передаются в открытом виде. Администратору Kaspersky Anti Targeted Attack Platform необходимо обеспечить безопасность серверов с этими данными самостоятельно. Администратор Kaspersky Anti Targeted Attack Platform несет ответственность за изменение конфигурационных файлов приложения.

- Управлять параметрами журнала трассировки.

  Файлы трассировки могут содержать конфиденциальные данные пользователя. Такие файлы хранятся бессрочно и могут быть удалены администратором Kaspersky Anti Targeted Attack Platform вручную. Путь к папке для записи файлов трассировки указывает администратор Kaspersky Anti Targeted Attack Platform.

► *Чтобы начать работу с компонентами Central Node, Sensor или Sandbox в режиме Technical Support Mode:*

1. Войдите в консоль управления того сервера, параметры которого вы хотите изменить, по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке компонента (см. раздел "Установка и первоначальная настройка приложения" на стр. 110).

   Отобразится меню администратора компонента приложения.
3. В меню администратора приложения выберите режим **Technical Support Mode**.
4. Нажмите на клавишу **ENTER**.

Отобразится окно подтверждения входа в режим Technical Support Mode.

5. Подтвердите, что хотите выполнять действия с приложением в режиме Technical Support Mode. Для этого выберите **Yes** и нажмите на клавишу **ENTER**.

Вы можете начать работу с компонентами Sensor или Sandox в режиме Technical Support Mode.

Управление учетными записями администраторов и пользователей приложения

В Kaspersky Anti Targeted Attack Platform предусмотрены учетные записи для серверов со следующими компонентами:

- Sensor. Учетная запись администратора для работы в меню администратора приложения и в консоли управления сервером (в режиме Technical Support Mode).

  По умолчанию используется учетная запись admin.

- Sandbox. Учетная запись администратора для работы в меню администратора приложения, в консоли управления сервером (в режиме Technical Support Mode) и в веб-интерфейсе Sandbox.

  По умолчанию используется учетная запись admin.

- Central Node. Следующие учетные записи:
  - Учетная запись администратора для работы в меню администратора приложения и в консоли управления сервером (в режиме Technical Support Mode).

    По умолчанию используется учетная запись admin, созданная при установке приложения.

  - Учетная запись локального администратора веб-интерфейса приложения.

    По умолчанию используется учетная запись Administrator, созданная при установке приложения. Вы можете создать другие учетные записи администратора веб-интерфейса приложения (см. раздел "Создание учетной записи администратора веб-интерфейса приложения" на стр. 194) после установки.

  - Учетная запись администратора веб-интерфейса приложения.
  - Учетные записи пользователей веб-интерфейса приложения с ролями **Аудитор**, **Сотрудник службы безопасности** и **Старший сотрудник службы безопасности**.

Данные каждой из этих учетных записей хранятся на том сервере с компонентом приложения, к которому она относится.

В режиме распределенного решения и мультитенантности данные каждой из этих учетных записей хранятся на PCN и на том сервере с компонентом приложения, к которому она относится.

Учетная запись администратора для работы в консоли управления сервером обладает неограниченными правами на управление сервером с компонентом приложения, к которому она относится (правами суперпользователя). Под этой учетной записью вы можете выключить или перезагрузить сервер, а также изменить параметры приложения в режиме Technical Support Mode в консоли управления сервером.

Учетная запись администратора для работы в консоли управления сервером (admin) имеет неограниченный доступ к данным на этом сервере. Пароль учетной записи администратора для работы в консоли управления сервером должен быть надежным. Администратору требуется обеспечить безопасность серверов самостоятельно. Администратор несет ответственность за доступ к данным, хранящимся на серверах.

Под учетной записью с ролью **Администратор** вы можете добавлять, включать и отключать учетные записи пользователей приложения, а также изменять пароли учетных записей администраторов и пользователей веб-интерфейса приложения. В режиме режиме распределенного решения и мультитенантности управление учетными записями пользователей осуществляется на PCN.

Учетная запись локального администратора веб-интерфейса приложения предназначена для сотрудников вашей организации, в чьи обязанности входит управление Kaspersky Anti Targeted Attack Platform. При входе в приложение под этой учетной записью отображаются все разделы веб-интерфейса, доступные пользователю с ролью **Администратор** (см. раздел "**Интерфейс Kaspersky Anti Targeted Attack Platform**" на стр. 243).

Под учетной записью администратора веб-интерфейса приложения можно управлять приложением, но, в отличие от локального администратора веб-интерфейса приложения, этой учетной записи недоступно управление серверами PCN и SCN, а также тенантами в разделе **Режим работы**.

Под учетной записью с ролью **Аудитор** вы можете просматривать все разделы веб-интерфейса, доступные локальному администратору и сотрудникам службы безопасности. Пользователь с ролью **Аудитор** может просматривать данные без возможности редактирования.

Роли **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** предназначены для сотрудников вашей организации, в чьи обязанности входит работа с событиями (см. раздел "Информация о событиях" на стр. 378) и задачами (см. раздел "Работа с задачами" на стр. 456) Kaspersky Anti Targeted Attack Platform. При входе в приложение под учетными записями с этими ролями отображаются все разделы веб-интерфейса, доступные сотрудникам службы безопасности (см. раздел "Интерфейс Kaspersky Anti Targeted Attack Platform" на стр. 322). Пользователи с ролью **Старший сотрудник службы безопасности** доступны все операции. Ограничения доступа для пользователей с ролями **Сотрудник службы безопасности** представлены в таблице ниже.

*Таблица 32. Ограничения доступа для пользователей приложения с ролью **Сотрудник службы безопасности***

Функциональная область / Раздел веб-интерфейса	Ограничения
Мониторинг	Недоступны виджеты событий группы VIP. Нет возможности перейти по ссылке на виджет в раздел **Обнаружения**.
Обнаружения	Недоступны следующие действия: • просмотр информации об обнаружении; • отметка о завершении обработки обнаружения группы VIP; • операции над несколькими обнаружениями; • экспорт списка всех обнаружений.
Поиск угроз	Недоступны события, которые относятся к хостам из обнаружений группы VIP.
Задачи	Нет доступа.
Политики	Нет доступа.
Пользовательские правила	Доступ на чтение.

Функциональная область / Раздел веб-интерфейса	Ограничения
Хранилище	Нет доступа к объектам, помещенным в Хранилище в результате выполнения задач. Полный доступ к объектам, загруженным пользователем вручную.
Endpoint Agents	Доступ к просмотру таблиц компьютеров с Kaspersky Endpoint Agent, ограничения по просмотру данных о задачах, политиках и сетевой изоляции.
Сетевая изоляция хостов	Нет доступа.
Отчеты	Нет доступа.
Параметры: Расписание IOC-проверки	Доступ на чтение.
Параметры: Endpoint Agents	Доступ на чтение.
Параметры: Репутационная база KPSN	Нет доступа.
Параметры: Правила уведомлений	Нет доступа к правилам для отправки уведомлений об обнаружениях. Полный доступ к правилам для отправки уведомлений о проблемах в работе приложения.
Параметры: Статус VIP	Доступ на чтение.
Пользовательские правила: YARA	Доступ только на экспорт правил.
Параметры: Исключение TAA (IOA)	Доступ на чтение и экспорт.
Параметры: Пароли к архивам	Нет доступа.
Параметры: Лицензия	Доступ на чтение.

Если вы используете режим распределенного решения и мультитенантности, то для каждой учетной записи вы можете разрешить или запретить доступ к тенантам и веб-интерфейсу сервера SCN.

kaspersky

В этом разделе

Создание учетной записи администратора веб-интерфейса приложения 194

Создание учетной записи пользователя веб-интерфейса приложения 196

Настройка отображения таблицы учетных записей пользователей 197

Просмотр таблицы учетных записей пользователей 198

Фильтрация учетных записей 199

Сброс фильтра учетных записей 199

Изменение прав доступа учетной записи пользователя веб-интерфейса приложения 200

Включение и отключение учетной записи администратора или пользователя веб-интерфейса приложения 200

Изменение пароля учетной записи администратора или пользователя приложения 201

Изменение пароля своей учетной записи 202

Создание учетной записи администратора веб-интерфейса приложения

Под учетной записью администратора веб-интерфейса приложения можно управлять приложением, но, в отличие от локального администратора веб-интерфейса приложения, этой учетной записи недоступно управление серверами PCN и SCN, а также тенантами в разделе **Режим работы**.

► *Чтобы создать учетную запись администратора веб-интерфейса приложения:*

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Пользователи**.
3. Нажмите на кнопку **Добавить**.

   Откроется окно **Новый пользователь**.
4. Если вы хотите включить учетную запись, включите переключатель **Состояние**.

   По умолчанию учетная запись включена.

   > Если учетная запись включена, доступ к веб-интерфейсу приложения разрешен. Если учетная запись отключена, доступ к веб-интерфейсу приложения запрещен.
5. В раскрывающемся списке **Роль** выберите **Администратор**.
6. В блоке параметров **Тип аутентификации** выберите один из вариантов:
   - **Учетная запись KATA**.

     В этом случае для подключения к веб-интерфейсу приложения пользователю потребуется ввести имя пользователя и пароль, которые были указаны при создании учетной записи.
   - **Доменная учетная запись**.

В этом случае для подключения к веб-интерфейсу приложения пользователю не требуется вводить имя пользователя и пароль: аутентификация осуществляется с помощью доменной учетной записи пользователя.

Поля **Учетная запись KATA** и **Доменная учетная запись** доступны, если настроена интеграция с Active Directory (см. раздел "Настройка интеграции с Active Directory" на стр. 206).

7. Если вы выбрали **Учетная запись KATA**, выполните следующие действия:
   a. В поле **Имя пользователя** введите имя пользователя, учетную запись которого вы хотите создать.

      Имя пользователя должно удовлетворять следующим требованиям:

      - должно быть уникальным в списке имен пользователей (регистр имеет значение);
      - должно содержать максимум 32 символа;
      - может содержать буквы A–Z, a–z, цифры 0–9, дефис (-) или символ подчеркивания (_);
      - должно начинаться с буквы (A–Z или a–z).

   b. В поле **Новый пароль** введите пароль доступа пользователя к веб-интерфейсу.

      Пароль должен удовлетворять следующим требованиям:

      - не должен совпадать с именем пользователя;
      - не должен содержать словарные слова, распространенные сочетания букв или примеры раскладки клавиатуры (например, Qwerty или passw0rd);
      - должен содержать минимум 8 символов;
      - должен содержать символы минимум трех типов:
        - символ верхнего регистра (A–Z);
        - символ нижнего регистра (a–z);
        - цифру;
        - специальный символ.

   c. В поле **Подтвердите пароль** повторно введите пароль доступа пользователя к веб-интерфейсу.
8. Если вы выбрали **Доменная учетная запись**, в поле **Имя пользователя** укажите доменное имя пользователя.
9. Нажмите на кнопку **Добавить**.

Учетная запись администратора веб-интерфейса приложения будет создана.

Если вы используете режим распределенного решения и мультитенантности, учетная запись администратора веб-интерфейса сервера PCN имеет доступ к данным всех тенантов, связанных с этим сервером.

Создание учетной записи пользователя веб-интерфейса приложения

Вы можете создавать учетные записи пользователей с ролями **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности** и **Аудитор**.

► *Чтобы создать учетную запись пользователя веб-интерфейса приложения:*

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Пользователи**.
3. Нажмите на кнопку **Добавить**.

   Откроется окно **Новый пользователь**.
4. При необходимости с помощью переключателя **Состояние** отключите учетную запись пользователя.

   По умолчанию учетная запись включена.

   Если учетная запись включена, доступ к веб-интерфейсу приложения разрешен. Если учетная запись отключена, доступ к веб-интерфейсу приложения запрещен.
5. В блоке параметров **Тип аутентификации** выберите один из вариантов:
   - **Учетная запись KATA**.

     В этом случае для подключения к веб-интерфейсу приложения пользователю потребуется ввести имя пользователя и пароль, которые были указаны при создании учетной записи.
   - **Доменная учетная запись**.

     В этом случае для подключения к веб-интерфейсу приложения пользователю не требуется вводить имя пользователя и пароль: аутентификация осуществляется с помощью доменной учетной записи пользователя.

     Если вы выбрали тип аутентификации **Доменная учетная запись**, требуется учитывать, что пользователь не сможет войти в веб-интерфейс приложения под другой учетной записью.

   Поля **Учетная запись KATA** и **Доменная учетная запись** доступны, если настроена интеграция с Active Directory (см. раздел "Настройка интеграции с Active Directory" на стр. 206).
6. В раскрывающемся списке **Роль** выберите одну из следующих ролей:
   - **Старший сотрудник службы безопасности**.
   - **Сотрудник службы безопасности**.
   - **Аудитор**.
7. Если вы выбрали **Учетная запись KATA**, выполните следующие действия:
   a. В поле **Имя пользователя** введите имя пользователя, учетную запись которого вы хотите создать.

Имя пользователя должно удовлетворять следующим требованиям:

- должно быть уникальным в списке имен пользователей (регистр имеет значение);
- должно содержать максимум 32 символа;
- может содержать буквы A–Z, a–z, цифры 0–9, дефис (-) или символ подчеркивания (_);
- должно начинаться с буквы (A–Z или a–z).

b. В поле **Новый пароль** введите пароль доступа пользователя к веб-интерфейсу.

Пароль должен удовлетворять следующим требованиям:

- не должен совпадать с именем пользователя;
- не должен содержать словарные слова, распространенные сочетания букв или примеры раскладки клавиатуры (например, Qwerty или passw0rd);
- должен содержать минимум 8 символов;
- должен содержать символы минимум трех типов:
  - символ верхнего регистра (A–Z);
  - символ нижнего регистра (a–z);
  - цифру;
  - специальный символ.

c. В поле **Подтвердите пароль** повторно введите пароль доступа пользователя к веб-интерфейсу.

8. Если вы выбрали **Доменная учетная запись**, в поле **Имя пользователя** укажите доменное имя пользователя.
9. В разделе **Доступ** настройте права доступа:

   a. С помощью переключателя включите параметр **Веб-интерфейс SCN**, если вы хотите предоставить пользователю доступ не только к веб-интерфейсу этого сервера PCN, но и к веб-интерфейсам всех доступных серверов SCN.

   b. Справа от названия параметра **Тенанты** установите флажки рядом с названиями одного или нескольких тенантов, к веб-интерфейсам серверов которых вы хотите предоставить доступ.

   Вы можете использовать ссылки **Выбрать все** и **Отменить выбор** для выбора или отмены выбора всех тенантов.

10. Нажмите на кнопку **Добавить**.

Настройка отображения таблицы учетных записей пользователей

Вы можете настроить отображение столбцов, а также порядок их следования в таблице учетных записей пользователей.

► *Чтобы настроить отображение таблицы учетных записей пользователей:*

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Пользователи**.

3. В заголовочной части таблицы нажмите на кнопку .

   Отобразится окно **Настройка таблицы**.

4. Если вы хотите включить отображение столбца в таблице, установите флажок рядом с названием того параметра, который должен отображаться в таблице.

   Если вы не хотите, чтобы параметр отображался в таблице, снимите флажок.

   Должен быть установлен хотя бы один флажок.

5. Если вы хотите изменить порядок отображения столбцов в таблице, наведите курсор мыши на строку с нужным параметром, нажмите на кнопку и переместите строку с параметром в нужное место.

6. Если вы хотите восстановить параметры отображения таблицы по умолчанию, нажмите на ссылку **По умолчанию**.

7. Нажмите на кнопку **Применить**.

Отображение таблицы учетных записей пользователей будет настроено.

Просмотр таблицы учетных записей пользователей

Таблица событий отображается в разделе **Параметры**, подразделе **Пользователи** окна веб-интерфейса приложения. Вы можете сортировать события в таблице по столбцам **Имя пользователя**, **Роль**, **Тенанты** и **Состояние**.

В таблице содержится следующая информация:

1. **Имя пользователя** – имя пользователя, заданное при создании учетной записи.
2. **Тип аутентификации** – тип аутентификации пользователя. Может иметь следующие значения:
   - **Учетная запись KATA**.

     Если выбран этот тип аутентификации, для подключения к веб-интерфейсу приложения пользователю потребуется ввести имя пользователя и пароль, которые были указаны при создании учетной записи.
   - **Доменная учетная запись**.

     Если выбран этот тип аутентификации, для подключения к веб-интерфейсу приложения пользователю не требуется вводить имя пользователя и пароль: аутентификация осуществляется с помощью доменной учетной записи пользователя.
3. **Роль** – роль, назначенная пользователю.
4. **Тенанты** – тенанты, к которым пользователь имеет доступ.

   Столбец отображается только в режиме распределенного решения и мультитенантности.
5. **Состояние** – статус учетной записи. может иметь следующие значения:
   - **Включено**.

     Если учетная запись включена, доступ к веб-интерфейсу приложения разрешен.
   - **Выключено**.

Если учетная запись отключена, доступ к веб-интерфейсу приложения запрещен.

Фильтрация учетных записей

► *Чтобы отфильтровать или найти учетные записи пользователей по требуемым критериям:*

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Пользователи**.
3. Выполните следующие действия в зависимости от критерия фильтрации:
   - **По имени пользователя**
   - **По типу аутентификации**
   - **По роли**
   - **По названию тенантов, к которым у пользователя есть доступ**
   - **По состоянию**

   В таблице отобразятся учетные записи, соответствующие заданным критериям фильтрации.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра учетных записей

► *Чтобы сбросить фильтр правил YARA по одному или нескольким условиям фильтрации:*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **YARA**.

   Откроется таблица правил YARA.
2. Нажмите на кнопку ☒ справа от того заголовка столбца таблицы правил, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице отобразятся только правила, соответствующие заданным условиям.

Изменение прав доступа учетной записи пользователя веб-интерфейса приложения

Вы можете изменить права доступа пользователей с ролями **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** к данным серверов PCN и SCN, а также тенантов, связанных с этими серверами.

► *Чтобы изменить права доступа учетной записи пользователя веб-интерфейса приложения, выполните следующие действия в веб-интерфейсе PCN:*

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Пользователи**.Выберите учетную запись, права доступа которой вы хотите изменить.

   Откроется окно **Изменить учетную запись**.
3. Если вы хотите включить или отключить учетную запись, измените положение переключателя **Состояние**.
4. Если нужно, в разделе **Доступ** измените положение переключателя **Веб-интерфейс SCN**:
   - Переведите переключатель в положение **Включено**, если вы хотите предоставить пользователю доступ не только к веб-интерфейсу этого сервера PCN, но и к веб-интерфейсам всех доступных серверов SCN.
   - Переведите переключатель в положение **Выключено**, если вы хотите предоставить пользователю доступ только к веб-интерфейсу этого сервера PCN.
5. Справа от названия параметра **Тенанты** установите или снимите флажки рядом с названиями тенантов, к веб-интерфейсам серверов которых вы хотите изменить доступ.

   Вы можете использовать ссылки **Выбрать все** и **Отменить выбор** для выбора или отмены выбора всех тенантов.
6. Нажмите на кнопку **Сохранить**.

Права доступа учетной записи будут изменены.

Включение и отключение учетной записи администратора или пользователя веб-интерфейса приложения

► *Чтобы включить или отключить учетную запись администратора или пользователя веб-интерфейса приложения, выполните следующие действия в веб-интерфейсе PCN:*

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Пользователи**.
3. В списке учетных записей выберите учетную запись пользователя, которую вы хотите включить или отключить.
4. Выполните одно из следующих действий в столбце **Состояние**:

- Включите переключатель рядом с именем учетной записи, если вы хотите включить учетную запись.
- Выключите переключатель рядом с именем учетной записи, если вы хотите отключить учетную запись.

Отобразится окно подтверждения действия.

5. Нажмите на кнопку **Да**.

Состояние учетной записи будет изменено.

Изменение пароля учетной записи администратора или пользователя приложения

Изменение пароля учетной записи доступно только для пользователей с типом аутентификации **Учетная запись KATA**.

► *Чтобы изменить пароль учетной записи администратора или пользователя приложения, выполните следующие действия в веб-интерфейсе PCN:*

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Пользователи**.В списке учетных записей выберите учетную запись, пароль которой вы хотите изменить.

   Откроется окно **Изменить учетную запись**.
3. В поле **Новый пароль** введите новый пароль доступа к веб-интерфейсу приложения.

   Пароль должен удовлетворять следующим требованиям:

   - не должен совпадать с именем пользователя;
   - не должен содержать словарные слова, распространенные сочетания букв или примеры раскладки клавиатуры (например, Qwerty или passw0rd);
   - должен содержать минимум 8 символов;
   - должен содержать символы минимум трех типов:
     - символ верхнего регистра (A–Z);
     - символ нижнего регистра (a–z);
     - цифру;
     - специальный символ.
4. В поле **Подтвердите пароль** повторно введите новый пароль.
5. Нажмите на кнопку **Сохранить**.

Пароль учетной записи администратора или пользователя приложения будет изменен.

Изменение пароля своей учетной записи

Изменение пароля учетной записи доступно только для пользователей с типом аутентификации **Учетная запись KATA**.

► *Чтобы изменить пароль своей учетной записи:*

1. Войдите в веб-интерфейс под своей учетной записью.
2. В нижней части окна веб-интерфейса программы по ссылке с именем вашей учетной записи раскройте список действий.
3. Выберите действие **Изменить пароль**.

   Откроется окно **Изменить пароль**.
4. В поле **Старый пароль** введите текущий пароль доступа к веб-интерфейсу приложения.
5. В поле **Новый пароль** введите новый пароль доступа к веб-интерфейсу приложения.

   Пароль должен удовлетворять следующим требованиям:

   - не должен совпадать с именем пользователя;
   - не должен содержать словарные слова, распространенные сочетания букв или примеры раскладки клавиатуры (например, Qwerty или passw0rd);
   - должен содержать минимум 8 символов;
   - должен содержать символы минимум трех типов:
     - символ верхнего регистра (A–Z);
     - символ нижнего регистра (a–z);
     - цифру;
     - специальный символ.
6. В поле **Подтвердите пароль** повторно введите новый пароль.
7. Нажмите на кнопку **Изменить пароль**.

Пароль доступа к веб-интерфейсу приложения вашей учетной записи будет изменен.

Аутентификация с помощью доменных учетных записей

Если аутентификация с помощью доменных учетных записей настроена, пользователям не требуется вводить данные учетной записи Kaspersky Anti Targeted Attack Platform для подключения к веб-интерфейсу приложения.

Для включения аутентификации с помощью доменных учетных записей вам требуется:

1. Настроить интеграцию с Active Directory (см. раздел "Настройка интеграции с Active Directory" на стр. 206).

   Для настройки интеграции с Active Directory требуется создать keytab-файл (см. раздел "Создание keytab-файла" на стр. 203), содержащий имя субъекта-службы (далее также "SPN") для сервера Central Node, на котором выполняется настройка интеграции.

2. Выбрать для пользователя тип аутентификации **Доменная учетная запись** при создании учетной записи (см. раздел "Управление учетными записями администраторов и пользователей приложения" на стр. 191).

В этом разделе

Создание keytab-файла 203

Настройка интеграции с Active Directory 206

Отключение интеграции с Active Directory 207

Создание keytab-файла

Вы можете использовать одну учетную запись для аутентификации на нескольких серверах Central Node. Для этого требуется создать keytab-файл, содержащий *имена субъекта-службы (далее также "SPN")* для каждого из этих серверов. При создании keytab-файла потребуется использовать атрибут для генерации *соли* (salt, модификатор входа хеш-функции).

Сгенерированную соль необходимо сохранить любым удобным способом для дальнейшего добавления новых SPN в keytab-файл.

Вы также можете создать отдельную учетную запись Active Directory для каждого сервера Central Node, для которого вы хотите настроить Kerberos-аутентификацию.

► *Чтобы создать keytab-файл, используя одну учетную запись:*

1. На сервере контроллера домена в оснастке **Active Directory Users and Computers** создайте учетную запись пользователя (например, с именем `control-user`).
2. Если вы хотите использовать алгоритм шифрования AES256-SHA1, то в оснастке **Active Directory Users and Computers** выполните следующие действия:

a. Откройте свойства созданной учетной записи.

b. На закладке **Account** установите флажок **This account supports Kerberos AES 256 bit encryption**.

3. Создайте keytab-файл для пользователя `control-user` с помощью утилиты ktpass. Для этого в командной строке выполните следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) сервера Central Node>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * +dumpsalt -out <путь к файлу>\<имя файла>.keytab
```

Утилита запросит пароль пользователя `control-user` в процессе выполнения команды.

В созданный keytab-файл будет добавлено SPN выбранного сервера. На экране отобразится сгенерированная соль: `Hashing password with salt "<хеш-значение>".`

4. Добавьте в keytab-файл запись SPN для каждого следующего сервера Central Node. Для этого выполните следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) сервера Central Node>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in <путь и имя ранее созданного файла>.keytab -out <путь и новое имя>.keytab -setupn -setpass -rawsalt "<хеш-значение соли, полученное при создании keytab-файла на шаге 3>"
```

Утилита запросит пароль пользователя `control-user` в процессе выполнения команды.

Keytab-файл будет создан. Этот файл будет содержать все добавленные SPN выбранных серверов.

Пример:

Например, вам нужно создать keytab-файл, содержащий SPN-имена 3 серверов: `control-01.test.local`, `secondary-01.test.local` и `secondary-02.test.local`.

Чтобы создать в папке C:\keytabs\ файл под названием `filename1.keytab`, содержащий SPN сервера, требуется выполнить команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/control-01.test.local@TEST.LOCAL
-mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype
KRB5_NT_PRINCIPAL -pass * +dumpsalt -out C:\keytabs\filename1.keytab
```

Допустим, вы получили соль `"TEST.LOCALHTTPcontrol-01.test.local"`.

Для добавления еще одного SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-
01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-
SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename1.keytab -out
C:\keytabs\filename2.keytab -setupn -setpass -rawsalt
"TEST.LOCALHTTPcontrol-01.test.local"
```

Для добавления третьего SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-
02.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-
SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename2.keytab -out
C:\keytabs\filename3.keytab -setupn -setpass -rawsalt
"TEST.LOCALHTTPcontrol-01.test.local"
```

В результате будет создан файл с именем `filename3.keytab`, содержащий все три добавленные SPN.

► *Чтобы создать keytab-файл, используя отдельную учетную запись для каждого сервера Central Node:*

1. На сервере контроллера домена в оснастке **Active Directory Users and Computers** создайте отдельную учетную запись пользователя для каждого сервера (например, учетные записи с именами `control-user`, `secondary1-user`, `secondary2-user` и т.д.).
2. Если вы хотите использовать алгоритм шифрования AES256-SHA1, то в оснастке **Active Directory Users and Computers** выполните следующие действия:
   a. Откройте свойства созданной учетной записи.
   b. На закладке **Account** установите флажок **This account supports Kerberos AES 256 bit encryption**.
3. Создайте keytab-файл для пользователя `control-user` с помощью утилиты ktpass. Для этого в командной строке выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN)
   сервера Central Node>@<realm имя домена Active Directory в верхнем
   регистре> -mapuser control-user@<realm имя домена Active Directory в
   верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass *
   -out <путь к файлу>\<имя файла>.keytab
   ```

Утилита запросит пароль пользователя `control-user` в процессе выполнения команды.

В созданный keytab-файл будет добавлено SPN выбранного сервера.

4. Добавьте в keytab-файл запись SPN для каждого следующего сервера Central Node. Для этого выполните следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) сервера Central Node>@<realm имя домена Active Directory в верхнем регистре> -mapuser secondary1-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in <путь и имя ранее созданного файла>.keytab -out <путь и новое имя>.keytab
```

Утилита запросит пароль пользователя `secondary1-user` в процессе выполнения команды.

Keytab-файл будет создан. Этот файл будет содержать все добавленные SPN выбранных серверов.

Пример:

Например, вам нужно создать keytab-файл, содержащий SPN-имена 3 серверов: `control-01.test.local`, `secondary-01.test.local` и `secondary-02.test.local`.

Чтобы создать в папке C:\keytabs\ файл под названием `filename1.keytab`, содержащий SPN сервера, требуется выполнить команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/control-01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -out C:\keytabs\filename1.keytab
```

Для добавления еще одного SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-01.test.local@TEST.LOCAL -mapuser secondary1-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename1.keytab -out C:\keytabs\filename2.keytab
```

Для добавления третьего SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-02.test.local@TEST.LOCAL -mapuser secondary2-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename2.keytab -out C:\keytabs\filename3.keytab
```

В результате будет создан файл с именем `filename3.keytab`, содержащий все три добавленные SPN.

Настройка интеграции с Active Directory

► *Чтобы настроить интеграцию с Active Directory:*

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Пользователи**.

3. Перейдите на закладку **Интеграция с Active Directory**.
4. Установите флажок **Интеграция**, если вы хотите включить интеграцию с Active Directory.
5. Нажмите на кнопку **Обзор**, чтобы загрузить keytab-файл.
6. Выберите keytab-файл и нажмите на кнопку **Открыть**.

   После загрузки файла отобразятся следующие поля:

   - **Статус keytab-файла**. Может принимать следующие значения:
     - **Файл содержит SPN-идентификатор для этого сервера** – в загруженном keytab-файле есть SPN для этого сервера Kaspersky Anti Targeted Attack Platform.
     - **Отсутствует SPN-идентификатор для этого сервера** – в загруженном keytab-файле отсутствует SPN для этого сервера Kaspersky Anti Targeted Attack Platform.
   - **Файл содержит** – список SPN, которые содержит файл.
7. Нажмите на кнопку **Применить**.

Интеграция с Active Directory будет настроена.

В режиме распределенного решения и мультитенантности настройки интеграции с Active Directory, заданные на сервере PCN, **не** распространяются на подключенные к нему серверы SCN. Если вы хотите настроить интеграцию с Active Directory на серверах SCN, вам требуется выполнить описанные выше шаги на каждом выбранном сервере SCN.

Отключение интеграции с Active Directory

При отключении интеграции с Active Directory аутентификация пользователей с помощью доменных учетных данных будет недоступна.

Чтобы отключить интеграцию с Active Directory:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Пользователи**.
3. Перейдите на закладку **Интеграция с Active Directory**.
4. Снимите флажок **Интеграция**.
5. Нажмите на кнопку **Применить**.

Интеграция с Active Directory будет отключена. Загруженный keytab-файл будет удален без возможности восстановления.

В режиме распределенного решения и мультитенантности настройки интеграции с Active Directory, заданные на сервере PCN, **не** распространяются на подключенные к нему серверы SCN. Если вы хотите отключить интеграцию с Active Directory на отдельных серверах SCN, вам требуется выполнить описанные выше шаги на каждом выбранном сервере SCN.

Участие в Kaspersky Security Network и использование Kaspersky Private Security Network

Использование Kaspersky Security Network приводит к выходу приложения из сертифицированного состояния. Рекомендуется использовать Kaspersky Private Security Network или отказаться от использования KSN.

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Anti Targeted Attack Platform использует данные, полученные от пользователей во всем мире. Для получения этих данных предназначена сеть *Kaspersky Security Network*.

Kaspersky Security Network (далее также "KSN") – это инфраструктура облачных служб, предоставляющая пользователям доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Anti Targeted Attack Platform на объекты, информация о которых еще не вошла в базы антивирусных программ, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Участие пользователей в Kaspersky Security Network позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках объектов, данные о которых еще не вошли в базы антивирусных программ, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний программы, а также помогает другим пользователям Kaspersky Security Network оперативно получать информацию об угрозах IT-инфраструктуре предприятий.

Когда вы участвуете в Kaspersky Security Network, Kaspersky Anti Targeted Attack Platform отправляет в Kaspersky Security Network запросы о репутации файлов, интернет-ресурсов и программного обеспечения и получает ответ, содержащий данные о репутации этих объектов.

Участие в Kaspersky Security Network добровольное. Решение об участии в Kaspersky Security Network принимается на этапе установки Kaspersky Anti Targeted Attack Platform, его можно изменить в любой момент.

Подробнее об участии в Kaspersky Security Network вы можете прочитать в Положении о Kaspersky Security Network.

Если вы не хотите участвовать в KSN, вы можете использовать Kaspersky Private Security Network (далее также "KPSN") – решение, позволяющее пользователям получать доступ к репутационным базам Kaspersky Security Network, а также другим статистическим данным, не отправляя данные в Kaspersky Security Network со своих компьютеров.

По вопросам приобретения программы Kaspersky Private Security Network вы можете связаться со специалистами компании-партнера "Лаборатории Касперского" в вашем регионе.

Настройка участия в KSN производится на сервере Central Node и распространяется на все подключаемые серверы Sensor.
Если вы используете режим распределенного решения и multitenancy, настраивайте участие в KSN на сервере PCN. Настройка участия в KSN распространится на все серверы SCN, подключаемые к PCN.

В этом разделе

Просмотр Положения о KSN и настройка участия в KSN 210
Включение использования KPSN 210
Настройка подключения к локальной репутационной базе KPSN 211
Настройка сохранения информации в локальную репутационную базу KPSN 211
Отказ от участия в KSN и использования KPSN 212

Просмотр Положения о KSN и настройка участия в KSN

► *Чтобы настроить участие в Kaspersky Security Network:*

1. Войдите в веб-интерфейс приложения под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **KSN/KPSN и MDR**.
3. Справа от названия параметра **Тип подключения** нажмите на кнопку **KSN**.
4. Ознакомьтесь с Положением о Kaspersky Security Network и выберите один из следующих вариантов:
   - **Я согласен участвовать в KSN**, если вы согласны с условиями Положения о KSN и хотите участвовать в KSN.
   - **Я не согласен участвовать в KSN**, если вы не согласны с условиями Положения о KSN и не хотите участвовать в KSN.

     Если вы не согласны с условиями Положения, использование Kaspersky Security Network не будет включено.
5. Нажмите на кнопку **Применить**.

Участие в Kaspersky Security Network будет настроено.

Включение использования KPSN

► *Чтобы включить использование KPSN:*

1. Войдите в веб-интерфейс приложения под учетной записью администратора.

2. Выберите раздел **Параметры**, подраздел **KSN/KPSN и MDR**.
3. Справа от названия параметра **Тип подключения** нажмите на кнопку **KPSN**.
4. В блоке **Конфигурационные файлы KPSN** загрузите файлы kc_private.xms, kh_private.xms и ksncli_private.dat с помощью кнопки **Обзор**.
5. Нажмите на кнопку **Применить**.

Использование Kaspersky Private Security Network будет включено.

Настройка подключения к локальной репутационной базе KPSN

Приложение может сохранять информацию об обнаружениях компонента Sandbox в локальную репутационную базу KPSN. В этом случае объектам присваивается статус *Недоверенный*. Данные локальных репутационных баз доступны только для компьютеров локальной сети организации.

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить подключение Kaspersky Anti Targeted Attack Platform к локальной репутационной базе KPSN:*

1. Войдите в веб-интерфейс приложения под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **Репутационная база KPSN**.
3. В поле **Хост** укажите IP-адрес сервера KPSN, на котором хранится локальная репутационная база KPSN.
4. Нажмите на кнопку **Обзор** справа от поля **TLS-сертификат**.

   Откроется окно выбора файлов.
5. Выберите файл сертификата для аутентификации пользователей в KPSN и нажмите на кнопку **Открыть**.
6. Нажмите на кнопку **Обзор** справа от поля **TLS-ключ шифрования**.

   Откроется окно выбора файлов.
7. Выберите файл, содержащий закрытый ключ шифрования, и нажмите на кнопку **Открыть**.

Подключение к локальной репутационной базе KPSN будет настроено.

Настройка сохранения информации в локальную репутационную базу KPSN

Приложение может сохранять MD5- и SHA256-хеши объектов, обнаруженных компонентом Sandbox, в локальную репутационную базу KPSN. В этом случае объектам присваивается статус *Недоверенный*. Данные локальных репутационных баз доступны только для компьютеров локальной сети организации.

► *Чтобы настроить сохранение информации об обнаружениях в локальную репутационную базу KPSN:*

1. Войдите в веб-интерфейс приложения под учетной записью старшего сотрудника службы безопасности.
2. Выберите раздел **Параметры**, подраздел **Репутационная база KPSN**.
3. Выполните одно из следующих действий:
   - Включите переключатель **Присваивать объектам статус "Недоверенный"**, если вы хотите, чтобы приложение присваивало обнаружениям статус *Недоверенный* и сохраняла информацию об обнаружениях компонента Sandbox в локальную репутационную базу KPSN.
   - Выключите переключатель **Присваивать объектам статус "Недоверенный"**, если вы не хотите сохранять информацию об обнаружениях компонента Sandbox в локальную репутационную базу KPSN.
4. Нажмите на кнопку **Сохранить**.

Настройка сохранения информации в локальную репутационную базу KPSN будет выполнена.

Отказ от участия в KSN и использования KPSN

► *Чтобы отказаться от участия в Kaspersky Security Network и использования KPSN:*

1. Войдите в веб-интерфейс приложения под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **KSN/KPSN и MDR**.
3. Справа от названия параметра **Тип подключения** нажмите на кнопку **Не подключен**.
4. Нажмите на кнопку **Применить**.

Вы не будете участвовать в KSN и использовать KPSN.

Работа с компонентом Sandbox через веб-интерфейс

Веб-интерфейс Sandbox расположен на сервере с компонентом Sandbox.

Веб-интерфейс Sandbox защищен от *CSRF-атак* и работает только в том случае, если браузер пользователя веб-интерфейса предоставляет заголовок Referrer HTTP-запроса POST. Убедитесь, что браузер, который вы используете для работы с веб-интерфейсом Sandbox, не модифицирует заголовок Referrer HTTP-запроса POST. Если соединение с веб-интерфейсом осуществляется через прокси-сервер вашей организации, проверьте параметры и убедитесь, что прокси-сервер не модифицирует заголовок Referrer HTTP-запроса POST.

► *Чтобы начать работу в веб-интерфейсе Sandbox:*

1. В браузере на любом компьютере, на котором разрешен доступ к серверу с компонентом Sandbox, введите IP-адрес сервера с компонентом Sandbox.

   Откроется окно ввода учетных данных администратора компонента Sandbox.

2. Введите имя пользователя и пароль администратора компонента Sandbox, который вы задали при установке компонента Sandbox.

Вы можете начать работу в веб-интерфейсе Sandbox.

Если вы используете несколько серверов с компонентом Sandbox, производите настройку параметров каждого компонента Sandbox из веб-интерфейса Sandbox этого сервера.

kaspersky

В этом разделе

Обновление баз компонента Sandbox 214

Настройка соединения компонентов Sandbox и Central Node 216

Настройка сетевых интерфейсов компонента Sandbox 218

Установка даты и времени системы Sandbox 221

Установка и настройка образов операционных систем и приложений для работы компонента Sandbox 221

Работа с образами операционных систем и приложений в Хранилище Sandbox 223

Работа с шаблонами виртуальных машин 226

Управление виртуальными машинами 232

Установка максимального количества одновременно запускаемых виртуальных машин 239

Изменение количества лицензионных ключей для виртуальной машины с пользовательским образом операционной системы 239

Загрузка журнала системы Sandbox на жесткий диск 240

Экспорт параметров Sandbox 240

Импорт параметров Sandbox 241

Перезагрузка сервера Sandbox 242

Выключение сервера Sandbox 242

Изменение пароля учетной записи администратора Sandbox 242

Обновление баз компонента Sandbox

Базы компонента Sandbox представляют собой файлы с записями, которые позволяют обнаруживать в проверяемых объектах вредоносный код и признаки подозрительного поведения объектов.

Вирусные аналитики "Лаборатории Касперского" ежедневно обнаруживают множество новых угроз, создают для них идентифицирующие записи и включают их в *пакет обновлений баз* (далее также "пакет обновлений"). Пакет обновлений представляет собой один или несколько файлов с записями, идентифицирующими угрозы, которые были выявлены за время, истекшее с момента выпуска предыдущего пакета обновлений. Рекомендуется регулярно получать пакеты обновлений.

В течение срока действия лицензии вы можете получать пакеты обновлений автоматически один раз в час или обновлять базы вручную.

kaspersky

В этом разделе

Запуск обновления баз вручную 215
Выбор источника обновления баз 215
Включение и отключение использования прокси-сервера для обновления баз 216
Настройка параметров соединения с прокси-сервером для обновления баз 216

Запуск обновления баз вручную

► *Чтобы запустить обновление баз вручную:*

1. В окне веб-интерфейса Sandbox выберите раздел **Обновление баз**.

   В блоке параметров **Последнее обновление** отобразятся время и статус последней попытки обновления баз Sandbox.

2. Нажмите на кнопку **Запустить**.

Выбор источника обновления баз

► *Чтобы выбрать источник обновления баз:*

1. В окне веб-интерфейса Sandbox выберите раздел **Обновление баз**.
2. В блоке параметров **Источник обновлений** выберите источник, из которого вы хотите получать пакет обновлений:
   - **Сервер обновлений "Лаборатории Касперского"**.

     Программа будет подключаться к серверу обновлений "Лаборатории Касперского" по протоколу HTTP и загружать актуальные базы.
   - **Сервер обновлений "Лаборатории Касперского" (безопасное подключение)**.

     Программа будет подключаться к серверу обновлений "Лаборатории Касперского" по протоколу HTTPS и загружать актуальные базы. Рекомендуется выполнять обновления баз по протоколу HTTPS.
   - **Другой сервер**.

     Программа будет подключаться к вашему FTP- или HTTP-серверу или к папке с базами программы на вашем компьютере и загружать актуальные базы.
3. Если вы выбрали **Другой сервер**, в поле под названием этого параметра укажите полный путь к папке с пакетом обновлений баз приложения.
4. Нажмите на кнопку **Применить** в нижней части окна.

Включение и отключение использования прокси-сервера для обновления баз

► *Чтобы включить или отключить использование прокси-сервера для обновления баз компонента Sandbox:*

1. В окне веб-интерфейса Sandbox выберите раздел **Обновление баз**.
2. В рабочей области выполните одно из следующих действий:
   - Включите переключатель рядом с названием блока параметров **Прокси-сервер**, если вы хотите использовать прокси-сервер при обновлении баз компонента Sandbox.
   - Выключите переключатель рядом с названием блока параметров **Прокси-сервер**, если вы не хотите использовать прокси-сервер при обновлении баз компонента Sandbox.

Настройка параметров соединения с прокси-сервером для обновления баз

► *Чтобы настроить параметры соединения с прокси-сервером для обновления баз компонента Sandbox:*

1. В окне веб-интерфейса Sandbox выберите раздел **Обновление баз**.
2. Включите переключатель рядом с названием блока параметров **Прокси-сервер**.
3. В поле **Адрес** введите адрес прокси-сервера.
4. В поле **Порт** укажите номер порта прокси-сервера.
5. В поле **Имя пользователя** введите имя пользователя прокси-сервера.
6. В поле **Пароль** введите пароль подключения к прокси-серверу.
7. Выполните одно из следующих действий:
   - Установите флажок **Не использовать прокси-сервер для локальных адресов**, если вы не хотите использовать прокси-сервер для внутренних адресов электронной почты вашей организации.
   - Снимите флажок **Не использовать прокси-сервер для локальных адресов**, если вы хотите использовать прокси-сервер независимо от принадлежности адресов электронной почты к вашей организации.
8. Нажмите на кнопку **Применить** в нижней части окна.

Настройка соединения компонентов Sandbox и Central Node

Предусмотрен следующий порядок настройки соединения компонента Sandbox с компонентом Central Node:

1. В веб-интерфейсе приложения (см. раздел "Начало работы с приложением" на стр. 186) создается запрос на подключение к компоненту Sandbox (см. раздел "Создание запроса на подключение к серверу с компонентом Sandbox" на стр. 299).
2. В веб-интерфейсе Sandbox отображаются запросы на подключение.

Вы можете принять или отклонить запрос (см. раздел "Обработка запросов на подключение от серверов Central Node в веб-интерфейсе Sandbox" на стр. 217).

После настройки соединения серверу Sandbox требуется 5–10 минут для подготовки к работе. В течение этого времени в окне **Работоспособность системы** (см. раздел "**Просмотр состояния работоспособности модулей и компонентов приложения**" на стр. 251) веб-интерфейса приложения отображается предупреждение *Возникла проблема со стандартной конфигурацией. Переустановите компонент Central Node*. Когда сервер будет готов к работе, предупреждение исчезнет.

В этом разделе

Обработка запросов на подключение от серверов Central Node в веб-интерфейсе Sandbox 217

Обработка запросов на подключение от серверов Central Node в веб-интерфейсе Sandbox

Вы можете принять, отклонить или отозвать ранее принятый запрос на подключение от серверов Central Node в веб-интерфейсе Sandbox (см. раздел "Работа с компонентом Sandbox через веб-интерфейс" на стр. 213).

► *Чтобы принять, отклонить или отозвать запрос на подключение от серверов Central Node:*

1. В окне веб-интерфейса Sandbox выберите раздел **Авторизация**.

   В разделе **Запросы на подключение от Central Node** отобразится список запросов на подключение от компонентов Central Node.

   В каждом запросе на подключение содержится следующая информация:

   - **IP** – IP-адрес сервера Central Node.
   - **Отпечаток сертификата** – отпечаток TLS-сертификата Cental Node, с помощью которого устанавливается шифрованное соединение между серверами.
   - **Состояние** – состояние запроса на подключение.

     Может иметь значения **Ожидание** или **Принят**.

2. Убедитесь, что отпечаток сертификата Cental Node соответствует отпечатку сертификата на стороне Cental Node.

   Вы можете проверить отпечаток сертификата Central Node в меню администратора сервера Central Node в разделе **Manage server certificate**.

3. Нажмите на одну из следующих кнопок в строке с запросом на подключение от компонента Central Node:

   - **Принять**, если вы хотите принять запрос на подключение.
   - **Отклонить**, если вы хотите отклонить запрос на подключение.

- **Отозвать**, если вы хотите отозвать ранее принятый запрос на подключение.

4. Нажмите на кнопку **Применить** в нижней части окна.

Настройка сетевых интерфейсов компонента Sandbox

В этом разделе содержится информация о настройке сетевых интерфейсов компонента Sandbox.

В этом разделе

Настройка параметров DNS 218
Настройка параметров управляющего сетевого интерфейса 218
Настройка параметров сетевого интерфейса для доступа обрабатываемых объектов в интернет 219
Добавление, изменение и удаление статических сетевых маршрутов 220

Настройка параметров DNS

► *Чтобы настроить параметры DNS:*

1. В окне веб-интерфейса Sandbox выберите раздел **Сетевые интерфейсы**.
2. В поле **Имя хоста** введите имя сервера, на который вы устанавливаете компонент Sandbox, в формате FQDN (например, sandbox).
3. Справа от названия параметра **DNS-серверы** нажмите на кнопку **Добавить**.

   Добавится пустое поле ввода IP-адреса DNS-сервера.
4. Введите IP-адрес основного DNS-сервера в формате IPv4.
5. Нажмите на кнопку ✔ справа от поля ввода.

   DNS-сервер будет добавлен.
6. Если вы хотите добавить дополнительный DNS-сервер, повторите действия 2-5.
7. Если вы хотите удалить добавленный DNS-сервер, нажмите на кнопку 🗑 справа от строки с IP-адресом DNS-сервера.

   Вы можете удалить только дополнительные DNS-серверы. Вы не можете удалить основной DNS-сервер. Если вы добавили 2 и более DNS-сервера, вы можете удалить любой из них, при этом оставшийся DNS-сервер будет использоваться в качестве основного.

Настройка параметров управляющего сетевого интерфейса

Управляющий сетевой интерфейс предназначен для доступа к серверу с компонентом Sandbox по протоколу SSH, также через этот интерфейс компонент Sandbox будет принимать объекты от компонента Central Node.

Вы можете настроить управляющий сетевой интерфейс во время установки компонента Sandbox (см. раздел "Установка компонента Sandbox" на стр. 119).

Вы также можете настроить управляющий сетевой интерфейс в веб-интерфейсе Sandbox.

► *Чтобы настроить управляющий сетевой интерфейс в веб-интерфейсе Sandbox:*

1. В окне веб-интерфейса Sandbox выберите раздел **Сетевые интерфейсы**.
2. В группе параметров **Управляющий интерфейс** в раскрывающемся списке **Интерфейс** выберите сетевой интерфейс, который вы хотите использовать в качестве управляющего.
3. В поле **IP** введите IP-адрес, который вы хотите назначить этому сетевому интерфейсу, если IP-адрес не назначен.
4. В поле **Маска** введите маску сети, в которой вы хотите использовать этот сетевой интерфейс.
5. Нажмите на кнопку **Применить** в нижней части окна.

Настройка параметров сетевого интерфейса для доступа обрабатываемых объектов в интернет

Объекты, которые обрабатывает компонент Sandbox, могут предпринимать попытки действий в интернете через сетевой интерфейс для доступа обрабатываемых объектов в интернет. Компонент Sandbox может анализировать поведение этих объектов.

Если вы запретите доступ в интернет, компонент Sandbox не сможет анализировать поведение объектов в интернете, и будет анализировать поведение объектов без доступа в интернет.

Сетевой интерфейс для доступа обрабатываемых объектов в интернет должен быть изолирован от локальной сети вашей организации.

Если в соответствии с политикой безопасности вашей организации с компьютеров пользователей локальной сети запрещен доступ в интернет, и вы настроили сетевой интерфейс Sandbox для доступа обрабатываемых объектов в интернет, есть риск возникновения следующего сценария: Злоумышленник может прикрепить вредоносное приложение к произвольному файлу и запустить Sandbox-проверку этого файла с компьютера пользователя локальной сети. Этот файл будет выведен за пределы локальной сети через сетевой интерфейс для доступа обрабатываемых объектов в интернет в процессе проверки файла компонентом Sandbox.

Отсутствие сетевого интерфейса Sandbox для доступа обрабатываемых объектов в интернет исключает риски подобной передачи информации, однако снижает качество обнаружений.

► *Чтобы настроить сетевой интерфейс для доступа обрабатываемых объектов в интернет:*

1. В окне веб-интерфейса Sandbox выберите раздел **Сетевые интерфейсы**.

2. В группе параметров **Интерфейс для выхода в интернет** в списке **Интерфейс** выберите сетевой интерфейс, который вы хотите использовать для доступа обрабатываемых объектов в интернет.

   Управляющий сетевой интерфейс, которые вы настроили ранее, недоступен для выбора в этом списке сетевых интерфейсов.

3. В поле **IP** введите IP-адрес, который вы хотите назначить этому сетевому интерфейсу.
4. В поле **Маска** введите маску сети, в которой вы хотите использовать этот сетевой интерфейс.
5. В поле **Шлюз по умолчанию** введите адрес шлюза сети, в которой вы хотите использовать этот сетевой интерфейс.
6. Нажмите на кнопку **Применить** в нижней части окна.

Добавление, изменение и удаление статических сетевых маршрутов

Вы можете настроить статические сетевые маршруты во время установки компонента Sandbox (см. раздел "Установка компонента Sandbox" на стр. 119).

Вы также можете добавить, удалить или изменить статические сетевые маршруты в веб-интерфейсе Sandbox.

► *Чтобы добавить статический сетевой маршрут:*

1. В окне веб-интерфейса Sandbox выберите раздел **Сетевые интерфейсы**.
2. В группе параметров **Статические маршруты** нажмите на кнопку **Добавить**.

   В списке статических сетевых маршрутов добавится строка с пустыми полями.

3. В поле **IP** введите IP-адрес сервера, для которого вы хотите настроить статический сетевой маршрут.
4. В поле **Маска** введите маску подсети.
5. В поле **Шлюз** введите IP-адрес шлюза.
6. В списке **Интерфейс** выберите сетевой интерфейс, для которого вы хотите добавить статический сетевой маршрут.
7. Нажмите на кнопку ✓.
8. Нажмите на кнопку **Применить** в нижней части окна.

► *Чтобы удалить статический сетевой маршрут, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Сетевые интерфейсы**.
2. В группе параметров **Статические маршруты** в строке со статическим сетевым маршрутом, который вы хотите удалить, нажмите на кнопку 🗑.
3. Нажмите на кнопку **Применить** в нижней части окна.

► *Чтобы изменить статический сетевой маршрут:*

1. В окне веб-интерфейса Sandbox выберите раздел **Сетевые интерфейсы**.
2. В группе параметров **Статические маршруты** в строке со статическим сетевым маршрутом, который вы хотите изменить, нажмите на кнопку .

   Строка статического сетевого маршрута станет доступна для редактирования. Вы можете изменить один или несколько параметров статического сетевого маршрута.
3. В поле **IP** измените IP-адрес сервера, для которого вы хотите настроить статический сетевой маршрут.
4. В поле **Маска** измените маску подсети.
5. В поле **Шлюз** измените IP-адрес шлюза.
6. В списке **Интерфейс** выберите сетевой интерфейс, для которого вы редактируете сетевой маршрут.
7. Нажмите на кнопку .
8. Нажмите на кнопку **Применить** в нижней части окна.

Установка даты и времени системы Sandbox

► *Чтобы установить дату и время сервера с компонентом Sandbox:*

1. В окне веб-интерфейса Sandbox выберите раздел **Дата и время**.
2. В раскрывающемся списке **Страна** выберите нужную страну.
3. В раскрывающемся списке **Часовой пояс** выберите нужный часовой пояс.
4. Если вы хотите синхронизировать время с NTP-сервером, включите переключатель справа от названия параметра **Синхронизация с NTP-серверами**.
5. Если вы хотите установить дату и время вручную, не включайте переключатель справа от названия параметра **Синхронизация с NTP-серверами** и выполните следующие действия:

   a. В поле **Дата** введите текущую дату или нажмите на кнопку и выберите дату в календаре.

   b. В поле **Время** введите текущее время.
6. Нажмите на кнопку **Применить** в нижней части окна.

Установка и настройка образов операционных систем и приложений для работы компонента Sandbox

Для проверки объектов вы можете использовать свои (далее также "пользовательские") образы операционных систем и преднастроенные образы из комплекта поставки. Если вы используете пользовательские образы, вы можете установить в этих операционных системах любые приложения. Набор приложений для образов из комплекта поставки невозможно изменить.

В комплекте поставки вы получаете преднастроенные ISO-образы операционных систем и приложений, необходимых для работы компонента Sandbox. Вам потребуется активировать (см. раздел "Активация

образов операционных систем и приложений в Хранилище Sandbox" на стр. 224) некоторые операционные системы и приложения.

Компонент Sandbox запускает объекты в выбранных операционных системах и анализирует поведение этих объектов для выявления вредоносной активности, признаков целевых атак и вторжений в IT-инфраструктуру организации.

Вы можете использовать пользовательские и преднастроенные образы операционных систем одновременно.

Чтобы использовать образ операционной системы для проверки объектов компонентом Sandbox, вам нужно создать виртуальную машину для этого образа.

Настоятельно рекомендуется на каждом сервере Sandbox использовать все необходимые вам и доступные преднастроенные образы операционных систем из комплекта поставки.

Если используется только часть образов из комплекта поставки или только пользовательские образы, качество проверки объектов может снизиться.

Создание виртуальных машин с преднастроенными образами операционных систем из комплекта поставки

Процесс создания виртуальных машин с преднастроенными образами операционных систем состоит из следующих этапов:

1. Импорт шаблона (на стр. 231).
2. Создание виртуальной машины (на стр. 232).
3. Установка виртуальной машины (на стр. 236).

Создание виртуальных машин с пользовательскими образами операционных систем

Процесс создания виртуальных машин с пользовательскими образами операционных систем состоит из следующих этапов:

1. Загрузка в Хранилище Sandbox образа операционной системы и приложений (см. раздел "Загрузка образов операционных систем и приложений в Хранилище" на стр. 224), которые вы хотите установить в этой операционной системе.

   Вы можете пропустить этот шаг и загрузить образы в процессе создания (см. раздел "Создание шаблона виртуальной машины" на стр. 226) и редактирования (см. раздел "Редактирование шаблона" на стр. 229) шаблона.
2. Создание или импорт пользовательского шаблона (см. раздел "Импорт шаблона" на стр. 231).
3. Создание виртуальной машины (на стр. 232).
4. Установка виртуальной машины (на стр. 236).

При возникновении проблем с активацией преднастроенных операционных систем или приложений в веб-интерфейсе компонента Sandbox отобразится сообщение об ошибке. В этом случае рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского".

Работа с образами операционных систем и приложений в Хранилище Sandbox

В Хранилище Sandbox помещаются пользовательские образы операционных систем и приложений, которые вы хотите установить в этих операционных системах.

Вы можете загрузить в Хранилище следующие пользовательские образы операционных систем:

- Windows XP SP3 и выше.
- Windows 7.
- Windows 8.1 64-разрядная.
- Windows 10 64-разрядная (до версии 1909).

Загружаемые файлы должны иметь расширение .ISO.

Загрузка пользовательских образов операционных систем семейства Linux не поддерживается.

Если вы хотите использовать в шаблоне пользовательские образы операционных систем, вам нужно настроить эти операционные системы (см. раздел "Настройка операционной системы и программного обеспечения" на стр. 229).

Просмотр таблицы образов операционных систем и приложений в Хранилище Sandbox

► *Чтобы просмотреть таблицу образов операционных систем и приложений в Хранилище Sandbox:*

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Хранилище**.

Отобразится таблица образов операционных систем и приложений в Хранилище Sandbox.

В таблице содержится следующая информация:

- **Загружено** – время загрузки образа.
- **Имя** – имя образа.
- **Размер** – размер образа.
- **Действия** – доступные для образа операции. Возможные значения:**Создать VM**, **Экспортировать**, **Удалить**.

Загрузка образов операционных систем и приложений в Хранилище

► *Чтобы загрузить в Хранилище пользовательские образы операционных систем и приложений, которые вы хотите установить в этих операционных системах:*

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Хранилище**.
3. Нажмите на кнопку **Загрузить**.
4. Откроется окно загрузки файла.
5. Выберите файл с расширением .ISO, который вы хотите загрузить в Хранилище.
6. Нажмите на кнопку **Open**.

   Если вы хотите загрузить несколько образов, повторите шаги 1–6 для каждого образа.

Образ будет загружен в Хранилище и отобразится в таблице объектов.

Активация образов операционных систем и приложений в Хранилище Sandbox

Вы можете создать виртуальную машину (см. раздел "Создание виртуальной машины" на стр. 232) с неактивированными образами операционных систем Windows 7 (64-разрядная), Windows 10 (64-разрядная) и приложений, необходимых для работы компонента Sandbox, и активировать их с помощью своего лицензионного кода после установки виртуальной машины.

Активация образов операционных систем Windows и пакета приложений Microsoft Office выполняется с помощью файла kata_images.py. Файл входит в комплект поставки.

Для корректной активации образов операционных систем Windows и пакета приложений Microsoft Office требуется доступ в интернет. Убедитесь в том, что вы правильно настроили доступ в интернет. (см. раздел "Настройка параметров сетевого интерфейса для доступа обрабатываемых объектов в интернет" на стр. 219)

Во время выполнения процедуры активации в разделе **Мониторинг** компонент Central Node проинформирует вас об ошибке самодиагностики компонента Sandbox. После успешной активации ошибка самодиагностики компонента Sandbox перестанет отображаться. Во время активации объекты на проверку не будут отправляться в компонент Sandbox.

► *Чтобы активировать образы операционных систем Windows и пакет приложений Microsoft Office:*

1. Убедитесь, что были созданы (см. раздел "Создание виртуальной машины" на стр. 232) и установлены (см. раздел "Установка виртуальной машины" на стр. 236) виртуальные машины с

неактивированными образами операционных систем Windows 7 (64-разрядная), Windows 10 (64-разрядная) и пакетом приложений Microsoft Office.

2. Поместите файл kata_images.py на сервер с компонентом Central Node по протоколу SSH, выполнив команду:

   ```
   scp ./kata_images.py admin@<IP-адрес сервера Sandbox>:
   ```

3. Войдите в консоль управления сервера с компонентом Sandbox по протоколу SSH или через терминал.
4. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке программы (см. стр. 110).

   Отобразится меню администратора компонента Sandbox.

5. В меню администратора программы выберите режим **Technical Support Mode**.
6. Нажмите на клавишу **ENTER**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.

7. Выберите **Yes** и нажмите на клавишу **ENTER**.
8. Активируйте образы операционных систем Windows и пакет приложений Microsoft Office, выполнив последовательность команд:

   c. `cd /var/opt/kaspersky/apt/files`

   d. `sudo -s`

   e. `./kata_images.py activate --vm_id Win7_x64 --component Win7 --key <код активации образа 64-разрядной операционной системы Windows 7>`

   f. `./kata_images.py activate --vm_id Win7_x64 --component Office2010 --key <код активации приложения Microsoft Office 2010>`

   g. `./kata_images.py activate --vm_id Win10_x64 --component Win10 --key <код активации образа 64-разрядной операционной системы Windows 10>`

   h. `./kata_images.py activate --vm_id Win10_x64 --component Office2016 --key <код активации приложения Microsoft Office 2016>`

   Код активации имеет следующий формат: XXXXX-XXXXX-XXXXX-XXXXX-XXXXX.

9. Создайте точки восстановления для виртуальных машин с установленными лицензионными ключами, выполнив команду:

   ```
   ./kata_images.py snapshot --vm_ids Win7_x64,Win10_x64
   ```

   Процесс может занять некоторое время.

10. Убедитесь, что в разделе **Мониторинг** веб-интерфейса приложения отсутствуют предупреждения о неработоспособности компонента Sandbox.

Образы операционных систем Windows и пакет приложений Microsoft Office будут активированы. Активацию образов операционных систем Windows и пакета приложений Microsoft Office необходимо провести на всех серверах с компонентом Sandbox.

Удаление образов операционных систем и приложений из Хранилища Sandbox

► *Чтобы удалить образ операционной системы или приложения из Хранилища Sandbox:*

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Хранилище**.
3. В столбце **Действие** напротив нужного образа нажмите на ссылку **Удалить**.

   Откроется окно подтверждения действия.
4. Нажмите на кнопку **Да**.

Образ будет удален.

Работа с шаблонами виртуальных машин

Виртуальные машины создаются на основе шаблонов. Чтобы создать виртуальную машину, вам нужно предварительно импортировать (см. раздел "Импорт шаблона" на стр. 231) или создать (см. раздел "Создание шаблона виртуальной машины" на стр. 226) для нее шаблон. На основе одного шаблона может быть создано (см. раздел "Создание виртуальной машины" на стр. 232) несколько виртуальных машин.

Вы можете выполнять с шаблонами следующие операции: просматривать таблицу шаблонов (см. раздел "Просмотр таблицы шаблонов" на стр. 227), включать и выключать шаблоны (см. раздел "Включение и выключение шаблона" на стр. 228), редактировать (см. раздел "Редактирование шаблона" на стр. 229), экспортировать (см. раздел "Экспорт шаблона" на стр. 230) и удалять (см. раздел "Удаление шаблона" на стр. 231) шаблоны.

Операции с шаблоном недоступны, если на основе этого шаблона создается или устанавливается виртуальная машина с пользовательским образом операционной системы. После завершения процесса создания и установки виртуальной машины вы снова сможете выполнять операции с шаблоном.

Создание шаблона виртуальной машины

Чтобы создать виртуальную машину с выбранной операционной системой, вам нужно предварительно создать для нее шаблон.

► *Чтобы создать шаблон для виртуальной машины:*

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Шаблоны**.
3. В раскрывающемся списке **Добавить** выберите **Создать шаблон**.

   Откроется окно создания шаблона.
4. На этапе **Подготовка образа** выполните следующие действия:

a. В поле **Имя** введите имя шаблона.

b. В поле **Описание** введите описание шаблона. Поле не является обязательным.

c. В раскрывающемся списке **Образ ОС** выполните одно из следующих действий:

- Выберите образ операционной системы, который вы хотите использовать для шаблона, в списке доступных образов.

  Чтобы образ отображался в списке, вам нужно загрузить его в Хранилище (см. раздел "Загрузка образов операционных систем и приложений в Хранилище" на стр. 224).

- Загрузите образ операционной системы, нажав на ссылку **Загрузить**, выберите нужный файл и нажмите на кнопку **Open**.

  Загружаемый файл должен иметь расширение ISO.

5. Нажмите на кнопку **Продолжить**.

6. На этапе **Настройка шаблона** выполните следующие действия:

a. В раскрывающемся списке **Подключить ISO** выберите образ приложения, которое вы хотите установить в операционной системе.

Чтобы образ отображался в списке, вам нужно выполнить одно из следующих действий:

- Загрузить образ в Хранилище (см. раздел "Загрузка образов операционных систем и приложений в Хранилище" на стр. 224).

- В раскрывающемся списке **Подключить ISO** нажать на ссылку **Загрузить**, выбрать нужный файл и нажать на кнопку **Open**.

  Загружаемый файл должен иметь расширение ISO.

b. Если вы хотите размонтировать установленный образ, в раскрывающемся списке **Подключить ISO** нажмите на значок напротив этого образа.

c. Настройте операционную систему и программное обеспечение, установленное в ней (см. раздел "Настройка операционной системы и программного обеспечения" на стр. 229).

d. В раскрывающемся списке **Выключить** вы можете выполнить одно из следующих действий:

- **Выключить**, если вы хотите завершить работу системы с сохранением результата работы запущенных приложений.

- **Отключить питание**, если вы хотите завершить работу системы без сохранения результатов работы.

> Если шаблон включен, на его основе нельзя создать виртуальную машину и нельзя экспортировать шаблон. Если вы хотите продолжить настройку шаблона, включите его.

Создание шаблона виртуальной машины будет завершено. Вы можете создать на его основе виртуальную машину (см. раздел "Создание виртуальной машины" на стр. 232).

Просмотр таблицы шаблонов

► *Чтобы просмотреть таблицу шаблонов:*

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.

2. Перейдите в раздел **Шаблоны**.

Отобразится таблица шаблонов.

В таблице содержится следующая информация:

- **Создано** – время создания шаблона.
- **Тип** – тип операционной системы: пользовательская или преднастроенная.
- **Имя** – имя шаблона.
- **Состояние** – состояние шаблона, например, **Включить** или **Выключено**.
- **Размер** – размер шаблона.
- **ОС** – версия операционной системы, которая используется для шаблона.
- **ВМ** – виртуальная машина, созданная на основе этого шаблона.
- **Действия** – доступные для шаблона операции. Доступны следующие операции: **Создать VM**, **Экспортировать** ( ), **Удалить** ( ).
- **Описание** – описание, заданное при создании шаблона.

Включение и выключение шаблона

Если шаблон выключен, вы можете выполнять с ним следующие операции: создать на его основе виртуальную машину, экспортировать (см. раздел "Экспорт шаблона" на стр. 230), удалить (см. раздел "Удаление шаблона" на стр. 231). Если шаблон включен, вы можете редактировать (см. раздел "Редактирование шаблона" на стр. 229) его.

► *Чтобы включить или выключить шаблон:*

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Шаблоны**.
3. Выберите нужный шаблон.
4. В разделе **Настройка шаблона** выполните одно из следующих действий:
   - Если вы хотите включить шаблон, в консоли управления шаблоном нажмите на кнопку **Включить**.
   - Если вы хотите выключить шаблон, в консоли управления шаблоном в раскрывающемся списке **Выключить** выберите один из вариантов:
     - **Выключить**, если вы хотите завершить работу системы с сохранением результата работы запущенных приложений.
     - **Отключить питание**, если вы хотите завершить работу системы без сохранения результатов работы.

Шаблон будет включен или выключен.

Редактирование шаблона

► *Чтобы отредактировать шаблон:*

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Шаблоны**.
3. Выберите нужный шаблон.
4. Если шаблон выключен, включите его, нажав на кнопку **Включить**.
5. Если вы хотите установить приложение в операционной системе, которая используется для шаблона, в раскрывающемся списке **Подключить ISO** выберите образ приложения.

   Чтобы образ отображался в списке, вам нужно загрузить образ в Хранилище (см. раздел "Загрузка образов операционных систем и приложений в Хранилище" на стр. 224).
6. Если вы хотите размонтировать установленный образ, в раскрывающемся списке **Подключить ISO** нажмите на значок **Размонтировать** напротив этого образа.
7. Настройте операционную систему и программное обеспечение, установленное в ней (см. раздел "Настройка операционной системы и программного обеспечения" на стр. 229).

Шаблон будет отредактирован.

Настройка операционной системы и программного обеспечения

Подготовка операционных систем к работе

При установке операционных систем Windows XP, 7, 8.1 или 10 выполните следующие требования:

- Отключите экранную заставку.
- Выберите схему питания *Всегда включено*.
- Отключите автоматическое обновление.
- Отключите брандмауэр Windows.

При использовании операционной системы Windows 7 требуется поддержка хеш-алгоритма SHA-2. Для поддержки этого хеш-алгоритма установите обновление Security Update for Windows 7 for x64-based Systems (KB3033929). Для 32-битных операционных систем Windows 7 также требуется установить обновление KB3033929.

> Не устанавливайте обновление KB4474419. Это обновление может вызвать сбой во время развертывания виртуальной машины.

При использовании операционных систем Windows 8.1 и 10 требуется отключить функцию быстрой загрузки (fast boot) и включить функцию автоматического входа в систему (автологин).

Настройка операционных систем

С установленной операционной системой требуется выполнить следующие действия:

- Убедиться, что включено использование командной оболочки по умолчанию.

- Активировать операционную систему и другое лицензионное программное обеспечение.

Вы можете выполнить с установленной операционной системой следующие действия:

- Присвоить статичное имя компьютеру.
- Создать учетные записи пользователей.

  В этом случае требуется настроить автоматический вход в систему.

- Выбрать локализацию.

  Полностью поддерживаются русская и английская локализация. При выборе другой локализации качество проверки объектов будет снижено.

- Установить программное обеспечение.

  Ограничения, действующие при установке программного обеспечения:

  - К одному шаблону единовременно можно подключить только один образ. После того как шаблон будет сохранен, вы можете отключить один образ и подключить другой.
  - Не поддерживаются версии Microsoft Office выше 2016.
  - Настоятельно не рекомендуется устанавливать программное обеспечение следующих типов:
    - программное обеспечение, внедряющее свой код в другой запущенный процесс.
    - Драйверы для защиты.
    - Антивирусные приложения, включая Защитник Windows.
  - Не гарантируется обнаружение вредоносной активности файлов, которые запускаются с помощью узкоспециального программного обеспечения.

Kaspersky Anti Targeted Attack Platform не уведомляет о проблемах с установленным в операционной системе программным обеспечением.

Экспорт шаблона

Вы можете экспортировать шаблон одним из следующих способов:

- В таблице шаблонов.
- При просмотре шаблона.

Шаблон должен быть выключен (см. раздел "Включение и выключение шаблона" на стр. 228).

► *Чтобы экспортировать шаблон в таблице шаблонов:*

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Шаблоны**.

3. В столбце **Действие** напротив нужного шаблона нажмите на значок .

Шаблон будет экспортирован. Загрузка файла начнется автоматически.

► *Чтобы экспортировать шаблон при просмотре шаблона:*

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Шаблоны**.
3. Выберите нужный шаблон.
4. В раскрывающемся списке **Действия** выберите **Экспортировать**.

Загрузка файла начнется автоматически. Загрузка файла начнется автоматически.

Импорт шаблона

Вы можете импортировать шаблон, созданный (см. раздел "Создание шаблона виртуальной машины" на стр. 226) ранее.

► *Чтобы импортировать шаблон:*

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Шаблоны**.
3. В раскрывающемся списке **Добавить** выберите **Импортировать шаблон**.
4. Откроется окно загрузки файла.
5. Выберите файл, который вы хотите импортировать.
6. Нажмите на кнопку **Open**.

Шаблон отобразится в списке шаблонов.

Вы можете отредактировать (см. раздел "Редактирование шаблона" на стр. 229) шаблон, создать из него виртуальную машину (см. раздел "Создание виртуальной машины" на стр. 232), экспортировать (см. раздел "Экспорт шаблона" на стр. 230) или удалить (см. раздел "Удаление шаблона" на стр. 231).

Удаление шаблона

При удалении шаблона удаляются все созданные на его основе виртуальные машины.

Вы можете удалить шаблон одним из следующих способов:

- В таблице шаблонов.
- При просмотре шаблона.

Шаблон должен быть выключен (см. раздел "Включение и выключение шаблона" на стр. 228).

► *Чтобы удалить шаблон в таблице шаблонов:*

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Шаблоны**.
3. В столбце **Действие** напротив нужного шаблона нажмите на значок .

   Откроется окно подтверждения действия.
4. Нажмите на кнопку **Да**.

Шаблон будет удален.

► *Чтобы удалить шаблон при просмотре шаблона:*

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Шаблоны**.
3. Выберите нужный шаблон.
4. В раскрывающемся списке **Действия** выберите **Удалить**.

   Откроется окно подтверждения действия.
5. Нажмите на кнопку **Да**.

Шаблон будет удален.

Управление виртуальными машинами

Вы можете создавать (см. раздел "Создание виртуальной машины" на стр. 232), устанавливать (см. раздел "Установка виртуальной машины" на стр. 236) и удалять (см. раздел "Удаление виртуальной машины" на стр. 237) установленные и ожидающие установки виртуальные машины. Также вы можете просматривать списки виртуальных машин с преднастроенными (см. раздел "Просмотр таблицы виртуальных машин с преднастроенными операционными системами" на стр. 236) и пользовательскими (см. раздел "Просмотр таблицы виртуальных машин с пользовательскими операционными системами" на стр. 236) операционными системами.

Создание виртуальной машины

Вы можете создать виртуальную машину одним из следующих способов:

- В разделе **Виртуальные машины**.
- В таблице шаблонов.
- В окне просмотра шаблона.

Шаблон для виртуальной машины должен быть выключен (см. раздел "Включение и выключение шаблона" на стр. 228). После создания виртуальную машину требуется установить (см. раздел "Установка виртуальной машины" на стр. 236).

Для создания виртуальной машины с пользовательским образом операционной системы требуется доступ в интернет.

Создание виртуальной машины в разделе Виртуальные машины

► *Чтобы создать виртуальную машину с преднастроенным образом операционной системы в разделе **Виртуальные машины**:*

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Виртуальные машины**.
3. Нажмите на кнопку **Создать VM**.

   Откроется окно создания виртуальной машины.
4. В раскрывающемся списке **Шаблон** выберите шаблон для виртуальной машины.

   Если в списке нет подходящего шаблона, вы можете импортировать (см. раздел "Импорт шаблона" на стр. 231) или создать шаблон (см. раздел "Создание шаблона виртуальной машины" на стр. 226) в разделе **Шаблоны** окна веб-интерфейса Sandbox.
5. В поле **Имя** введите имя виртуальной машины.
6. В поле **Описание** введите описание виртуальной машине. Поле необязательно для заполнения.
7. Нажмите на кнопку **Добавить**.
8. Для некоторых операционных систем из комплекта поставки необходимо принятие условий лицензионного соглашения. Ознакомьтесь с текстом лицензионного соглашения и нажмите на кнопку **Принять**.

Виртуальная машина с преднастроенным образом операционной системы будет создана.

► *Чтобы создать виртуальную машину с пользовательским образом операционной системы в разделе **Виртуальные машины**:*

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Виртуальные машины**.
3. Нажмите на кнопку **Создать VM**.

   Откроется окно создания виртуальной машины.
4. В раскрывающемся списке **Шаблон** выберите шаблон для виртуальной машины.

   Если в списке нет подходящего шаблона, вы можете импортировать (см. раздел "Импорт шаблона" на стр. 231) или создать шаблон (см. раздел "Создание шаблона виртуальной машины" на стр. 226) в разделе **Шаблоны** окна веб-интерфейса Sandbox.
5. В поле **Имя** введите имя виртуальной машины.
6. В поле **Описание** введите описание виртуальной машине. Поле необязательно для заполнения.
7. Нажмите на кнопку **Добавить**.
8. Если для сервера, на котором создается виртуальная машина, не настроен доступ в интернет, в окне **Шаблоны** отобразится окно с ошибкой *Нет доступа в интернет*. Для завершения создания

виртуальной машины вам нужно загрузить отладочные символы (см. раздел "Загрузка отладочных символов" на стр. 238).

Виртуальная машина с пользовательским образом операционной системы будет создана.

Создание виртуальной машины в таблице шаблонов

► *Чтобы создать виртуальную машину с преднастроенным образом операционной системы в таблице шаблонов:*

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.

   Перейдите в раздел **Шаблоны**.

2. В столбце **Действия** напротив нужно шаблона нажмите на ссылку **Создать VM**.

   Откроется окно создания виртуальной машины.

3. В раскрывающемся списке **Шаблон** выберите шаблон для виртуальной машины.

   Если в списке нет подходящего шаблона, вы можете импортировать (см. раздел "Импорт шаблона" на стр. 231) или создать шаблон (см. раздел "Создание шаблона виртуальной машины" на стр. 226) в разделе **Шаблоны** окна веб-интерфейса Sandbox.

4. В поле **Имя** введите имя виртуальной машины.
5. В поле **Описание** введите описание виртуальной машине. Поле необязательно для заполнения.
6. Нажмите на кнопку **Добавить**.
7. Для некоторых операционных систем из комплекта поставки необходимо принятие условий лицензионного соглашения. Ознакомьтесь с текстом лицензионного соглашения и нажмите на кнопку **Принять**.

Виртуальная машина с преднастроенным образом операционной системы будет создана.

► *Чтобы создать виртуальную машину с пользовательским образом операционной системы в таблице шаблонов:*

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.

   Перейдите в раздел **Шаблоны**.

2. В столбце **Действия** напротив нужно шаблона нажмите на ссылку **Создать VM**.

   Откроется окно создания виртуальной машины.

3. В раскрывающемся списке **Шаблон** выберите шаблон для виртуальной машины.

   Если в списке нет подходящего шаблона, вы можете импортировать (см. раздел "Импорт шаблона" на стр. 231) или создать шаблон (см. раздел "Создание шаблона виртуальной машины" на стр. 226) в разделе **Шаблоны** окна веб-интерфейса Sandbox.

4. В поле **Имя** введите имя виртуальной машины.
5. В поле **Описание** введите описание виртуальной машине. Поле необязательно для заполнения.
6. Нажмите на кнопку **Добавить**.
7. Если для сервера, на котором создается виртуальная машина, не настроен доступ в интернет, в окне **Шаблоны** отобразится окно с ошибкой *Нет доступа в интернет*. Для завершения создания виртуальной машины вам нужно загрузить отладочные символы (см. раздел "Загрузка отладочных символов" на стр. 238).

Виртуальная машина с пользовательским образом операционной системы будет создана.

Создание виртуальной машины в окне просмотра шаблона

1. Чтобы создать виртуальную машину с преднастроенным образом операционной системы в окне просмотра шаблона:
2. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
3. Перейдите в раздел **Шаблоны**.
4. Выберите нужный шаблон.
5. Нажмите на кнопку **Создать VM**.

   Откроется окно создания виртуальной машины.
6. В раскрывающемся списке **Шаблон** выберите шаблон для виртуальной машины.

   Если в списке нет подходящего шаблона, вы можете импортировать (см. раздел "Импорт шаблона" на стр. 231) или создать шаблон (см. раздел "Создание шаблона виртуальной машины" на стр. 226) в разделе **Шаблоны** окна веб-интерфейса Sandbox.
7. В поле **Имя** введите имя виртуальной машины.
8. В поле **Описание** введите описание виртуальной машине. Поле необязательно для заполнения.
9. Нажмите на кнопку **Добавить**.
10. Для некоторых операционных систем из комплекта поставки необходимо принятие условий лицензионного соглашения. Ознакомьтесь с текстом лицензионного соглашения и нажмите на кнопку **Принять**.

Виртуальная машина с преднастроенным образом операционной системы будет создана.

► *Чтобы создать виртуальную машину с пользовательским образом операционной системы в окне просмотра шаблона:*

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Шаблоны**.
3. Выберите нужный шаблон.
4. Нажмите на кнопку **Создать VM**.

   Откроется окно создания виртуальной машины.
5. В раскрывающемся списке **Шаблон** выберите шаблон для виртуальной машины.

   Если в списке нет подходящего шаблона, вы можете импортировать (см. раздел "Импорт шаблона" на стр. 231) или создать шаблон (см. раздел "Создание шаблона виртуальной машины" на стр. 226) в разделе **Шаблоны** окна веб-интерфейса Sandbox.
6. В поле **Имя** введите имя виртуальной машины.
7. В поле **Описание** введите описание виртуальной машине. Поле необязательно для заполнения.
8. Нажмите на кнопку **Добавить**.
9. Если для сервера, на котором создается виртуальная машина, не настроен доступ в интернет, в окне **Шаблоны** отобразится окно с ошибкой *Нет доступа в интернет*. Для завершения создания виртуальной машины вам нужно загрузить отладочные символы (см. раздел "Загрузка отладочных символов" на стр. 238).

Виртуальная машина с пользовательским образом операционной системы будет создана.

Просмотр таблицы виртуальных машин с преднастроенными операционными системами

► *Чтобы просмотреть список виртуальных машин с преднастроенными операционными системами:*

1. В окне веб-интерфейса Sandbox выберите раздел **Виртуальные машины**.
2. Выберите закладку **Преднастроенные**.

Отобразится таблица виртуальных машин с преднастроенными операционными системами.

В таблице содержится следующая информация:

- **Имя** – имя виртуальной машины.
- **Состояние** – состояние виртуальной машины, например, **Включено** или **Выключено**.
- **Действия** – доступные для виртуальной машины операции. Могут быть доступны следующие операции: **Удалить**.

В разделе **Не установленные виртуальные машины** отображаются готовые к установке, но еще не установленные виртуальные машины.

Просмотр таблицы виртуальных машин с пользовательскими операционными системами

► *Чтобы просмотреть список виртуальных машин с пользовательскими операционными системами:*

1. В окне веб-интерфейса Sandbox выберите раздел **Виртуальные машины**.
2. Выберите закладку **Пользовательские**.

Отобразится таблица виртуальных машин с пользовательскими операционными системами.

В таблице содержится следующая информация:

- **Создано** – время создания виртуальной машины.
- **Имя** – имя виртуальной машины.
- **Состояние** – состояние виртуальной машины, например, **Включено** или **Выключено**.
- **Действия** – доступные для виртуальной машины операции. Могут быть доступны следующие операции: **Удалить**.
- **Описание** – описание, заданное при создании виртуальной машины.

Установка виртуальной машины

После создания (см. раздел "Создание виртуальной машины" на стр. 232) виртуальной машины ее нужно установить.

► *Чтобы установить виртуальную машину с преднастроенным образом операционной системы:*

1. В окне веб-интерфейса Sandbox выберите раздел **Виртуальные машины**.
2. Выберите закладку **Преднастроенные**.
3. В разделе **Не установленные виртуальные машины** нажмите на кнопку **Установить готовые VM**.

Все виртуальные машины, ожидающие установки, будут установлены.

► *Чтобы установить виртуальную машину с пользовательским образом операционной системы:*

1. В окне веб-интерфейса Sandbox выберите раздел **Виртуальные машины**.
2. Выберите закладку **Пользовательские**.
3. Напротив нужной виртуальной машины в столбце **Действия** нажмите на ссылку **Установить**.
4. Когда виртуальная машина установится, в столбце **Действия** нажмите на ссылку **Включить**.

Виртуальная машина будет установлена и готова к работе.

Удаление виртуальной машины

► *Чтобы удалить установленную виртуальную машину:*

1. В окне веб-интерфейса Sandbox выберите раздел **Виртуальные машины**.
2. Выберите закладку **Преднастроенные** или **Пользовательские**.
3. В столбце **Действия** напротив нужной виртуальной машины нажмите на ссылку **Удалить**.

Виртуальная машина будет удалена.

► *Чтобы удалить еще не установленную виртуальную машину с преднастроенным образом операционной системы:*

1. В окне веб-интерфейса Sandbox выберите раздел **Виртуальные машины**.
2. В разделе **Не установленные виртуальные машины** нажмите на кнопку **Удалить все ожидающие VM**.

Все виртуальные машины с преднастроенными образами операционных систем, ожидающие установки, будут удалены.

► *Чтобы удалить еще не установленную виртуальную машину с пользовательским образом операционной системы:*

1. В окне веб-интерфейса Sandbox выберите раздел **Виртуальные машины**.
2. Выберите закладку **Пользовательские**.
3. Напротив нужной виртуальной машины в столбце **Действия** нажмите на ссылку **Удалить**.

Виртуальная машина с пользовательским образом операционной системы, ожидающая установки, будет удалена.

Загрузка отладочных символов

Если для сервера, на котором устанавливается виртуальная машина с пользовательским образом, не настроен доступ в интернет, для корректного завершения установки виртуальной машины вам нужно загрузить отладочные символы Microsoft.

Вы можете загрузить отладочные символы в процессе установки виртуальной машины в окне **Шаблоны** только после того, как виртуальная машина получит статус **Сбой** в списке виртуальных машин.

> Для корректной загрузки отладочных символов в операционной системе, которая используется для шаблона виртуальной машины (см. раздел "Работа с шаблонами виртуальных машин" на стр. 226), должны быть установлены средства для отладки Windows (Windows Debug Tools).

► *Чтобы загрузить отладочные символы в процессе установки виртуальной машины в окне **Шаблоны**:*

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Шаблоны**.
3. Выберите нужный шаблон.
4. В окне с ошибкой *Нет доступа в интернет* нажмите на кнопку **Скачать манифест**.

   > Кнопка **Скачать манифест** не будет доступна, пока виртуальная машина не получит статус **Сбой**.

   На ваш компьютер будет загружен архив.
5. Распакуйте скачанный архив.
6. Запустите файл sbsymtool.ps1 с помощью Windows PowerShell.

   Архив с отладочными символами будет загружен в папку с этим файлом.
7. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
8. Перейдите в раздел **Шаблоны**.
9. Выберите шаблон, для которого вы загрузили отладочные символы.
10. В раскрывающемся списке **Действия** выберите **Загрузить символы**.
11. В открывшемся окне выберите архив с отладочными символами и нажмите на кнопку **Open**.

Отладочные символы будут загружены. Виртуальная машина будет установлена и отобразится в списке виртуальных машин с пользовательскими операционными системами (см. раздел "Просмотр таблицы виртуальных машин с пользовательскими операционными системами" на стр. 236).

► *Чтобы загрузить отладочные символы после того, как виртуальная машина получила статус **Сбой** в списке виртуальных машин:*

1. В окне веб-интерфейса Sandbox выберите раздел **Шаблоны и Хранилище**.
2. Перейдите в раздел **Шаблоны**.
3. Выберите нужный шаблон.

4. В раскрывающемся списке **Действия** выберите **Скачать манифест**.

   На ваш компьютер будет загружен архив.

5. Распакуйте скачанный архив.
6. Запустите файл sbsymtool.ps1 с помощью Windows PowerShell.

   Архив с отладочными символами будет загружен в папку с этим файлом.

7. В окне **Шаблоны** раскройте список **Действия** и выберите **Загрузить символы**.
8. В открывшемся окне выберите архив с отладочными символами и нажмите на кнопку **Open**.

Отладочные символы будут загружены. Виртуальная машина будет установлена и отобразится в списке виртуальных машин с пользовательскими операционными системами (см. раздел "Просмотр таблицы виртуальных машин с пользовательскими операционными системами" на стр. 236).

Установка максимального количества одновременно запускаемых виртуальных машин

Задайте ограничение для количества одновременно запускаемых виртуальных машин с операционными системами, в которых компонент Sandbox будет обрабатывать объекты.

Количество одновременно запускаемых виртуальных машин не может превышать 200.

Рассчитывайте количество одновременно запускаемых виртуальных машин с образами операционных систем следующим образом: количество ядер процессора нужно умножить на 1,5.

► *Чтобы установить максимальное количество одновременно запускаемых виртуальных машин:*

1. В окне веб-интерфейса Sandbox выберите раздел **Администрирование**.
2. В блоке параметров **Гостевые виртуальные машины** в поле **Максимум VM одновременно** введите количество одновременно запускаемых виртуальных машин.

   Вы можете ввести число от 1 до 200.

3. Нажмите на кнопку **Сохранить**.

Изменение количества лицензионных ключей для виртуальной машины с пользовательским образом операционной системы

При создании виртуальной машины с пользовательским образом операционной системы Kaspersky Anti Targeted Attack Platform указывает количество лицензионных ключей для программного обеспечения, которое используется внутри этой виртуальной машины. По умолчанию количество лицензионных ключей равно количеству одновременно запускаемых виртуальных машин (см. раздел "Установка максимального количества одновременно запускаемых виртуальных машин" на стр. 239). Ваша лицензия должна

покрывать это число. При необходимости вы можете изменить количество лицензионных ключей для виртуальной машины.

Если количество лицензионных ключей, которое вы задали для виртуальной машины, меньше количества одновременно запускаемых виртуальных машин, то возможно снижение общей производительности сервера Sandbox.

Менять заданное количество одновременно запускаемых виртуальных машин не рекомендуется.

► *Чтобы изменить количество лицензионных ключей для виртуальной машины с пользовательским образом операционной системы:*

1. Войдите в консоль управления сервера Sandbox по протоколу SSH или через терминал (см. раздел "Начало работы с приложением в режиме Technical Support Mode" на стр. 189).
2. Получите список серверов, выполнив команду `sb-custom-images list-vm`.

   Отобразится таблица виртуальных машин, где `id` – идентификатор виртуальной машины, `name` – имя виртуальной машины, `licenses` – количество лицензионных ключей.
3. Задайте количество лицензионных ключей для выбранной виртуальной машины, выполнив команду `sb-custom-images licenses -id <идентификатор виртуальной машины> -ln <количество лицензий>`.

Количество лицензионных ключей будет изменено.

Вы можете вызвать справку скрипта, выполнив команду `sb-custom-images --help`.

Загрузка журнала системы Sandbox на жесткий диск

Данные в журнале системы Sandbox хранятся в открытом незашифрованном виде. Данные хранятся за последние 7 дней.

► *Чтобы загрузить журнал системы Sandbox на жесткий диск:*

1. В окне веб-интерфейса Sandbox выберите раздел **Администрирование**.
2. В группе параметров **Журнал системы** нажмите на кнопку **Скачать**.
3. Журнал системы Sandbox загрузится на жесткий диск вашего компьютера в ту директорию, которая указана в качестве директории загрузки файлов из интернета в параметрах браузера, который вы используете для работы с приложением.

Экспорт параметров Sandbox

► *Чтобы экспортировать параметры системы Sandbox:*

1. В окне веб-интерфейса Sandbox выберите раздел **Администрирование**.

2. В группе параметров **Параметры** нажмите на кнопку **Экспортировать**.

   Откроется окно **Предупреждение**, содержащее предупреждение об особенностях экспорта параметров системы.

   Параметры системы Sandbox зависят от аппаратных и программных параметров сервера, на котором установлен компонент Sandbox. Экспортируемые параметры системы Sandbox предназначены для импорта на этот же или строго идентичный по конфигурации сервер. Попытки восстановить конфигурацию системы Sandbox значениями параметров, сохраненными на другой системе Sandbox, могут нарушить работу системы Sandbox.

3. Нажмите на кнопку **Сохранить**.

Файл формата tar.gz загрузится на жесткий диск вашего компьютера в ту директорию, которая указана в качестве директории загрузки файлов из интернета в параметрах браузера, который вы используете для работы приложения. В файле содержатся все текущие параметры системы Sandbox.

Архивы с резервной копией параметров системы могут содержать такие конфиденциальные данные, как, например, пароли, закрытые ключи. Администратору Kaspersky Anti Targeted Attack Platform необходимо обеспечить безопасность этих данных самостоятельно.

Импорт параметров Sandbox

► *Чтобы импортировать параметры Sandbox:*

1. В окне веб-интерфейса Sandbox выберите раздел **Администрирование**.
2. В группе параметров **Параметры** нажмите на кнопку **Импортировать**.

   Откроется окно **Предупреждение**, содержащее предупреждение об особенностях импорта параметров системы.

   Параметры компонента Sandbox зависят от аппаратных и программных параметров сервера, на котором установлен Sandbox. Экспортируемые параметры Sandbox предназначены для импорта на этот же или строго идентичный по конфигурации сервер. Попытки восстановить конфигурацию одной системы Sandbox настройками параметров, сохраненными на другой системе Sandbox, могут нарушить работу системы.

3. Нажмите на кнопку **Восстановить**.

   Откроется окно выбора файлов.

4. Выберите файл формата tar.gz с параметрами Sandbox, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

   Если импорт параметров Sandbox прошел успешно, сервер Sandbox перезагрузится. Через несколько минут вам нужно обновить окно браузера и повторить вход.

Архивы с резервной копией конфигурации системы могут содержать такие конфиденциальные данные, как, например, пароли, закрытые ключи. Администратору Kaspersky Anti Targeted Attack Platform необходимо обеспечить безопасность хранения этих данных самостоятельно.

Перезагрузка сервера Sandbox

► *Чтобы перезагрузить сервер Sandbox:*

1. В окне веб-интерфейса Sandbox выберите раздел **Администрирование**.
2. В группе параметров **Питание** нажмите на кнопку **Перезагрузить**.

   Откроется окно подтверждения перезагрузки сервера Sandbox.
3. Нажмите на кнопку **Да**.

Сервер Sandbox перезагрузится. Через несколько минут вы сможете войти в систему.

Выключение сервера Sandbox

► *Чтобы выключить сервер Sandbox:*

1. В окне веб-интерфейса Sandbox выберите раздел **Администрирование**.
2. В группе параметров **Питание** нажмите на кнопку **Выключить**.

   Откроется окно подтверждения выключения сервера Sandbox.
3. Нажмите на кнопку **Да**.

Изменение пароля учетной записи администратора Sandbox

► *Чтобы изменить пароль учетной записи администратора Sandbox:*

1. В окне веб-интерфейса Sandbox выберите раздел **Администрирование**.
2. В блоке параметров **Изменить пароль** отобразится имя учетной записи администратора Sandbox, которое вы задали при установке Sandbox и поля для изменения пароля.
3. В поле **Текущий пароль** введите текущий пароль учетной записи администратора Sandbox.
4. В поле **Новый пароль** введите новый пароль учетной записи администратора Sandbox.
5. В поле **Подтвердить пароль** введите новый пароль учетной записи администратора Sandbox повторно.
6. Нажмите на кнопку **Изменить пароль**.

   Пароль учетной записи администратора Sandbox будет изменен.

kaspersky

Администратору: работа в веб-интерфейсе приложения

Этот раздел адресован специалистам, которые осуществляют установку и администрирование Kaspersky Anti Targeted Attack Platform, а также управление серверами PCN и SCN и тенантами в режиме распределенного решения и мультитенантности.

В этом разделе

Интерфейс Kaspersky Anti Targeted Attack Platform 243

Мониторинг работы приложения 244

Управление серверами Central Node, PCN или SCN с помощью веб-интерфейса приложения 253

Управление компонентом Sensor 260

Управление кластером 277

Уведомления о максимальной загрузке центрального процессора и оперативной памяти серверов Central Node и Sensor 280

Настройка соединения с протоколом SNMP 282

Работа с информацией о хостах с компонентом Endpoint Agent 284

Настройка интеграции с компонентом Sandbox 297

Настройка интеграции с внешними системами 300

Настройка интеграции с Kaspersky Managed Detection and Response 302

Настройка интеграции с SIEM-системой 304

Управление журналом активности 312

Обновление баз приложения 317

Создание списка паролей для архивов 319

Интерфейс Kaspersky Anti Targeted Attack Platform

Работа с приложением осуществляется через веб-интерфейс. Разделы веб-интерфейса приложения различаются в зависимости от роли пользователя – **Администратор** или **Старший сотрудник службы безопасности** / **Сотрудник службы безопасности/Аудитор** (см. раздел "**Сотруднику службы безопасности: работа в веб-интерфейсе приложения**" на стр. 320).

Окно веб-интерфейса приложения содержит следующие элементы:

- разделы в левой части и в нижней части окна веб-интерфейса приложения;
- закладки в верхней части окна веб-интерфейса приложения для некоторых разделов приложения;
- рабочую область в нижней части окна веб-интерфейса приложения.

Разделы окна веб-интерфейса приложения

Веб-интерфейс приложения для роли **Администратор** содержит следующие разделы:

- **Мониторинг**. Содержит данные мониторинга Kaspersky Anti Targeted Attack Platform.
- **Режим работы**. Содержит информацию о серверах PCN и SCN и о тенантах в режиме распределенного решения и мультитенантности.
- **Endpoint Agents**. Содержит информацию о подключенных компьютерах с компонентом Endpoint Agent и их параметрах.
- **Отчеты**: **Журнал активности**. Содержит информацию о параметрах записи информации о действиях пользователей в веб-интерфейсе приложения.
- **Параметры**. Содержит параметры сервера с компонентом Central Node.
- **Серверы Sensor**. Содержит информацию о подключенных компонентах Sensor и их параметры.
- **Серверы Sandbox**. Содержит информацию о подключении компонента Central Node к компонентам Sandbox.
- **Внешние системы**. Содержит информацию об интеграции приложения с почтовыми сенсорами.

Рабочая область окна веб-интерфейса приложения

В рабочей области отображается информация, просмотр которой вы выбираете в разделах и на закладках окна веб-интерфейса приложения, а также элементы управления, с помощью которых вы можете настроить отображение информации.

Пользователи с ролью **Аудитор** также могут просматривать эти разделы веб-интерфейса приложения.

Мониторинг работы приложения

Вы можете осуществлять мониторинг работы приложения с помощью виджетов в разделе **Мониторинг** окна веб-интерфейса приложения. Вы можете добавлять, удалять, перемещать виджеты, настраивать масштаб отображения виджетов и выбирать период отображения данных.

kaspersky

В этом разделе

О виджетах и схемах расположения виджетов 245

Выбор тенанта и сервера для работы в разделе Мониторинг 246

Добавление виджета на текущую схему расположения виджетов 246

Перемещение виджета на текущей схеме расположения виджетов 246

Удаление виджета с текущей схемы расположения виджетов 247

Сохранение схемы расположения виджетов в PDF 247

Настройка периода отображения данных на виджетах 247

Мониторинг приема и обработки входящих данных 248

Мониторинг очередей обработки данных модулями и компонентами приложения 250

Мониторинг обработки данных компонентом Sandbox 251

Просмотр состояния работоспособности модулей и компонентов приложения 251

О виджетах и схемах расположения виджетов

С помощью виджетов вы можете осуществлять мониторинг работы приложения.

Схема расположения виджетов – вид рабочей области окна веб-интерфейса приложения в разделе **Мониторинг**. Вы можете добавлять, удалять и перемещать виджеты на схеме расположения виджетов.

В приложении доступны следующие виджеты:

- **Обработано** (см. раздел "**Мониторинг приема и обработки входящих данных**" на стр. 248). Отображение состояния обработки трафика, поступающего от компонента Sensor и компонента Endpoint Agent на сервер с компонентом Central Node.
- **Очереди** (см. раздел "**Мониторинг очередей обработки данных модулями и компонентами приложения**" на стр. 250). Отображение сведений о количестве и объеме объектов, ожидающих проверки модулями и компонентами приложения.
- **Время обработки в Sandbox** (см. раздел "**Мониторинг обработки данных компонентом Sandbox**" на стр. 251). Отображение среднего времени, за которое были получены результаты проверки объектов компонентом Sandbox.

Если вы используете режим распределенного решения и мультитенантности, в разделе отображаются данные по выбранному вами тенанту и серверу (см. раздел "Выбор тенанта и сервера для работы в разделе Мониторинг" на стр. 246).

Выбор тенанта и сервера для работы в разделе Мониторинг

Если вы используете режим распределенного решения и мультитенантности, перед началом работы в разделе **Мониторинг** вам нужно выбрать тенант и сервер, данные по которым вы хотите просмотреть.

► *Чтобы выбрать тенант и сервер для отображения данных в разделе **Мониторинг**:*

1. В правой верхней части окна веб-интерфейса приложения нажмите на стрелку рядом с именем сервера.
2. В раскрывшемся меню выберите тенант и нужный вам сервер из списка.

Отобразятся данные по выбранному вами серверу. Если вы хотите изменить тенант и сервер, вам нужно повторить действия по выбору тенанта и сервера.

Добавление виджета на текущую схему расположения виджетов

► *Чтобы добавить виджет на текущую схему расположения виджетов:*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку ≡.
3. В раскрывающемся списке выберите **Изменить**.
4. Нажмите на кнопку **Виджеты**.
5. В появившемся окне **Настроить виджеты** выполните следующие действия:
   - Если вы хотите добавить виджет **Очереди**, включите переключатель рядом с названием этого виджета.
   - Если вы хотите добавить виджет **Время обработки в Sandbox**, включите переключатель рядом с названием этого виджета.
   - Если вы хотите добавить виджет **Обработано**, нажмите на кнопку + рядом с названием этого виджета.

Выбранный виджет будет добавлен на текущую схему расположения виджетов.

Перемещение виджета на текущей схеме расположения виджетов

► *Чтобы переместить виджет на текущей схеме расположения виджетов:*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку ≡.
3. В раскрывающемся списке выберите **Изменить**.
4. Выберите виджет, который вы хотите переместить на схеме расположения виджетов.

5. Нажав и удерживая левую клавишу мыши на верхней части виджета, перетащите виджет на другое место схемы расположения виджетов.
6. Нажмите на кнопку **Сохранить**.

Текущая схема расположения виджетов будет сохранена.

Удаление виджета с текущей схемы расположения виджетов

► *Чтобы удалить виджет с текущей схемы расположения виджетов:*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку .
3. В раскрывающемся списке выберите **Изменить**.
4. Нажмите на значок в правом верхнем углу виджета, который вы хотите удалить со схемы расположения виджетов.

   Виджет будет удален из рабочей области окна веб-интерфейса приложения.
5. Нажмите на кнопку **Сохранить**.

Виджет будет удален с текущей схемы расположения виджетов.

Сохранение схемы расположения виджетов в PDF

► *Чтобы сохранить схему расположения виджетов в PDF:*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку .
3. В раскрывающемся списке выберите **Сохранить как PDF**.

   Откроется окно **Сохранение в PDF**.
4. В нижней части окна в раскрывающемся списке **Ориентация** выберите ориентацию страницы.
5. Нажмите на кнопку **Скачать**.

   Схема расположения виджетов в формате PDF будет сохранена на жесткий диск вашего компьютера в папку загрузки браузера.
6. Нажмите на кнопку **Закрыть**.

Настройка периода отображения данных на виджетах

Вы можете настроить отображение данных на виджетах за следующие периоды:

- **День**.
- **Неделя**.

- **Месяц**.

► *Чтобы настроить отображение данных на виджетах за сутки (с 00:00 до 23:59):*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса приложения в раскрывающемся списке периодов отображения данных выберите **День**.
3. В календаре справа от названия периода **День** выберите дату, за которую вы хотите получить данные на виджете.

На всех виджетах страницы **Мониторинг** отобразятся данные за выбранный вами период.

► *Чтобы настроить отображение данных на виджетах за неделю (с понедельника по воскресенье):*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса приложения в раскрывающемся списке периодов отображения данных выберите **Неделя**.
3. В календаре справа от названия периода **Неделя** выберите неделю, за которую вы хотите получить данные на виджете.

На всех виджетах страницы **Мониторинг** отобразятся данные за выбранный вами период.

► *Чтобы настроить отображение данных на виджетах за месяц (календарный месяц):*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса приложения в раскрывающемся списке периодов отображения данных выберите **Месяц**.
3. В календаре справа от названия периода **Месяц** выберите месяц, за который вы хотите получить данные на виджете.

На всех виджетах страницы **Мониторинг** отобразятся данные за выбранный вами период.

Мониторинг приема и обработки входящих данных

На виджете **Обработано** вы можете оценить статус обработки данных, поступающих от компонента Sensor и компонента Endpoint Agent на сервер с компонентом Central Node, и отследить ошибки обработки данных.

Вы можете выбрать компонент (Sensor или Endpoint Agent), поступление данных с которого вы хотите оценить, в раскрывающемся списке справа от названия виджета **Обработано**.

Вы можете выбрать тип отображения данных в раскрывающемся списке справа от названия компонента (Sensor или Endpoint Agent):

- **Текущая загрузка** – 5 минут до текущего момента.
- **Выбранный период**. В этом случае вы также можете настроить период отображения данных на виджетах (см. раздел "Настройка периода отображения данных на виджетах" на стр. 247).

В левой части каждого виджета отображается легенда виджета по цветам, которые используются на самих виджетах.

Если выбран тип отображения данных **Текущая загрузка**, справа от легенды отображается средняя скорость обработки данных за последние 5 минут.

Пример:

На виджете **Обработано**, где выбран Sensor типа **(SPAN)** или **(ICAP)** и тип отображения данных **Текущая загрузка**, отображается скорость обработки данных SPAN- и ICAP-трафика, поступающих от компонента Sensor на сервер с компонентом Central Node в определенное время.

Отображаются следующие данные:

- **Трафик** – скорость поступления трафика на сервер с компонентом Central Node зеленым цветом (Мбит/сек.).
- **Файлы** – скорость обработки файлов серым цветом (объектов/сек.).
- **URL-адреса** – скорость обработки URL-адресов синим цветом (объектов/сек.).
- **Не обработано** – количество необработанных объектов вертикальными линиями красного цвета.

При наведении курсора мыши на виджет появляется всплывающее окно, в котором отображается скорость обработки данных в определенное время.

На виджете **Обработано**, где выбран Sensor типа **(SMTP)** и тип отображения данных **Текущая загрузка**, отображается скорость обработки данных почтового трафика, поступающих от почтового сенсора на сервер с компонентом Central Node в определенное время.

Отображаются следующие данные:

- **Трафик** – скорость поступления трафика на сервер с компонентом Sensor зеленым цветом (сообщений/сек.).
- **Файлы** – скорость обработки файлов серым цветом (объектов/сек.).
- **URL-адреса** – скорость обработки URL-адресов синим цветом (объектов/сек.).
- **Не обработано** – количество необработанных объектов вертикальными линиями красного цвета.

При наведении курсора мыши на виджет появляется всплывающее окно, в котором отображается скорость обработки данных в определенное время.

На виджете **Обработано**, где выбран Sensor типа **(LOAD) Endpoint Agents** и тип отображения данных **Текущая загрузка**, отображается скорость обработки событий, поступающих от компонентов Endpoint Agent на сервер с компонентом Central Node в определенное время (Событий/сек.).

При наведении курсора мыши на виджет появляется всплывающее окно, в котором отображается скорость обработки данных в определенное время.

Если выбран тип отображения данных **Выбранный период**, справа от легенды отображается средняя скорость поступления трафика на сервер с компонентом Central Node и количество обработанных объектов за выбранный период.

Пример:

На виджете **Обработано**, где выбран Sensor типа **(SPAN)** или **(ICAP)** и тип отображения данных **Выбранный период** с настроенным периодом отображения данных **Месяц**, отображается скорость поступления SPAN- и ICAP-трафика на сервер с компонентом Central Node, а также количество файлов и URL-адресов, извлеченных из почтового трафика за выбранный месяц.

Отображаются следующие данные:

- **Средний трафик** – скорость поступления трафика на сервер с компонентом Central Node зеленым цветом (объектов/сек.).
- **Файлы** – количество извлеченных файлов серым цветом.
- **URL-адреса** – количество извлеченных URL-адресов синим цветом.
- **Не обработано** – количество необработанных объектов вертикальными линиями красного цвета.

При наведении курсора мыши на виджет появляется всплывающее окно, в котором отображается скорость поступления трафика на сервер с компонентом Central Node и количество обработанных объектов в определенное время.

На виджете **Обработано**, где выбраны Sensor типа **(SMTP)** и тип отображения данных **Выбранный период** с настроенным периодом отображения данных **Месяц**, отображается скорость обработки данных почтового трафика, поступающих от почтового сенсора на сервер с компонентом Central Node, а также количество файлов и URL-адресов, извлеченных из почтового трафика за выбранный месяц.

Отображаются следующие данные:

- **Средний трафик** – скорость поступления трафика на сервер с компонентом Central Node зеленым цветом (объектов/сек.).
- **Файлы** – количество извлеченных файлов серым цветом.
- **URL-адреса** – количество извлеченных URL-адресов синим цветом.
- **Не обработано** – количество необработанных объектов вертикальными линиями красного цвета.

При наведении курсора мыши на виджет появляется всплывающее окно, в котором отображается скорость поступления трафика на сервер с компонентом Central Node и количество обработанных объектов в определенное время.

На виджете **Обработано**, где выбран Sensor типа **(LOAD) Endpoint Agents** и тип отображения данных **Выбранный период** с настроенным периодом отображения данных **Месяц**, отображается количество событий, поступивших от хостов с компонентом Endpoint Agent на сервер с компонентом Central Node за выбранный месяц.

При наведении курсора мыши на виджет появляется всплывающее окно, в котором отображается количество событий, поступивших в определенное время.

Мониторинг очередей обработки данных модулями и компонентами приложения

На виджете **Очереди** вы можете оценить статус обработки данных модулями приложения YARA, AM Engine, компонентом Sandbox и отследить объем необработанных данных.

Передача данных в очереди измеряется сообщениями.

Вы можете выбрать тип отображения данных в раскрывающемся списке справа от названия виджета **Очереди**:

- **Текущая загрузка** – 5 минут до текущего момента.
- **Выбранный период**. В этом случае вы также можете настроить период отображения данных на виджетах.

В левой части виджета отображается легенда виджета по цветам, которые используются на виджете.

На виджете **Очереди** отображаются следующие данные:

- **Количество сообщений** и **Объем данных**, обработанных модулями и компонентами приложения:
  - **YARA** – синим цветом.
  - **Sandbox** – фиолетовым цветом.
  - **AM Engine** – зеленым цветом.
- **Не обработано** – объем необработанных данных вертикальными линиями красного цвета.

При наведении курсора мыши на виджет появляется всплывающее окно, в котором отображается статус обработки данных модулями приложения **YARA**, **AM Engine** и компонентом **Sandbox**, а также объем необработанных данных в определенное время.

Мониторинг обработки данных компонентом Sandbox

На виджете **Время обработки в Sandbox** отображается среднее время, прошедшее от момента отправки данных на один или несколько серверов с компонентом Sandbox (включая время ожидания отправки) до отображения результатов обработки данных компонентом Sandbox в веб-интерфейсе Kaspersky Anti Targeted Attack Platform в выбранный период.

Пример:

Если настроен период отображения данных на виджетах **Месяц**, на виджете **Время обработки в Sandbox** отображаются столбики оранжевого цвета на каждый день месяца.

При наведении курсора мыши на каждый столбик появляется всплывающее окно, в котором отображается среднее время, прошедшее от момента отправки данных на один или несколько серверов с компонентом Sandbox до отображения результатов обработки данных компонентом Sandbox в веб-интерфейсе Kaspersky Anti Targeted Attack Platform в выбранный день.

Вы можете увеличить скорость обработки данных компонентом Sandbox и пропускную способность компонента Sandbox, увеличив количество серверов с компонентом Sandbox (см. раздел "Расчеты для компонента Sandbox" на стр. 103) и распределив по этим серверам данные, предназначенные для обработки.

Просмотр состояния работоспособности модулей и компонентов приложения

Если в работе модулей и компонентов приложения возникли проблемы, на которые администратору рекомендуется обратить внимание, в верхней части окна раздела **Мониторинг** веб-интерфейса приложения отображается рамка желтого цвета с предупреждениями.

Пользователю с ролью **Локальный администратор**, **Администратор** или **Аудитор** доступна информация о работоспособности того сервера Central Node, PCN или SCN, на котором он сейчас работает.

Пользователю с ролью **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности** или **Аудитор** доступна следующая информация о работоспособности:

- Если вы используете отдельный сервер Central Node, пользователю доступна информация о работоспособности того сервера Central Node, на котором он сейчас работает.
- Если вы используете режим режим распределенного решения и мультитенантности и пользователь работает на сервере SCN, пользователю доступна информация о работоспособности этого сервера SCN в рамках тех тенантов, к данным которых у него есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса приложения" на стр. 200).
- Если вы используете режим режим распределенного решения и мультитенантности и пользователь работает на сервере PCN, пользователю доступна информация о работоспособности этого сервера PCN и всех серверов SCN, подключенных к этому серверу, в рамках тех тенантов, к данным которых у него есть доступ.

► *Чтобы получить более подробную информацию о работоспособности модулей и компонентов приложения,*

по ссылке **Просмотреть сведения** откройте окно **Работоспособность системы**.

В окне **Работоспособность системы** в зависимости от работоспособности модулей и компонентов приложения отображается один из следующих значков:

- Значок OK, если модули и компоненты приложения работают нормально.
- Значок с количеством проблем (например, 1), если обнаружены проблемы, на которые администратору рекомендуется обратить внимание. В этом случае в правой части окна **Работоспособность системы** отображается подробная информация о проблемах.

Окно **Работоспособность системы** содержит разделы:

- **Работоспособность компонентов** – статус работы модулей и компонентов приложения, карантина, а также обновления баз на всех серверах, на которых работает приложение.

Пример:

Если базы одного или нескольких компонентов приложения не обновлялись в течение 24 часов, рядом с именем сервера, на котором установлены модули и компоненты приложения, отображается значок !.

Для решения проблемы убедитесь, что серверы обновлений доступны. Если для соединения с серверами обновлений вы используете прокси-сервер, убедитесь, что на прокси-сервере нет ошибок, связанных с подключением к серверам Kaspersky Anti Targeted Attack Platform.

- **Обработано** – статус приема и обработки входящих данных. Статус формируется на основе следующих критериев:
  - Состояние получения данных с серверов с компонентом Sensor, с сервера или виртуальной машины с почтовым сенсором, с хостов с компонентом Endpoint Agent.
  - Информация о превышении максимально допустимого времени, которое объекты ожидают в очереди на проверку модулями и компонентами приложения.
- **Соединение с серверами** – состояние соединения между сервером PCN и подключенными серверами SCN (отображается, если вы используете режим распределенного решения и мультитенантности).

kaspersky

В случае обнаружения проблем в работоспособности модулей и компонентов приложения, которые вы не можете решить самостоятельно, рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Обращение в Службу технической поддержки" на стр. 670).

Управление серверами Central Node, PCN или SCN с помощью веб-интерфейса приложения

С помощью веб-интерфейса приложения вы можете выполнять следующие действия с сервером, на котором установлен компонент Central Node:

- настраивать дату и время сервера;
- выключать и перезагружать сервер;
- генерировать или загружать самостоятельно подготовленный сертификат сервера;
- настраивать сетевые параметры сервера;
- контролировать уровень заполнения дискового пространства сервера.

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

В этом разделе

Настройка даты и времени сервера....254
Генерация или загрузка TLS-сертификата сервера....254
Скачивание TLS-сертификата сервера на компьютер....256
Назначение DNS-имени сервера....256
Настройка параметров DNS....257
Настройка параметров сетевого интерфейса....257
Настройка сетевого маршрута для использования по умолчанию....258
Настройка параметров соединения с прокси-сервером....258
Настройка параметров соединения с почтовым сервером....258
Выбор операционных систем для проверки объектов в Sandbox....259

Настройка даты и времени сервера

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить дату и время сервера:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Дата и время**.
2. В раскрывающемся списке **Часовой пояс** выберите часовой пояс, в котором находится сервер с компонентом Central Node.

   Вы можете указать страну и часовой пояс, выбрав нужный регион на карте под раскрывающимися списками.
3. В блоке **NTP-серверы** выполните следующие действия:
   - Если вы хотите добавить новый NTP-сервер, выполните следующие действия:
     a. Нажмите на кнопку **Добавить**.
     b. В появившемся поле введите IP-адрес или доменное имя NTP-сервера.
     c. Справа от поля нажмите на кнопку ✓.
   - Если вы хотите изменить IP-адрес или доменное имя NTP-сервера, в строке с этим сервером нажмите на кнопку .
   - Если вы хотите удалить NTP-сервер, в строке с этим сервером нажмите на кнопку .
4. Нажмите на кнопку **Применить**.

Дата и время сервера будут настроены.

Генерация или загрузка TLS-сертификата сервера

Если вы уже используете TLS-сертификат сервера и сгенерируете или загрузите новый сертификат, сертификат, который используется в приложении, будет удален и заменен на новый сертификат. Вам потребуется указать данные нового сертификата везде, где использовался старый.

Если вы замените TLS-сертификат на новый, вам потребуется

- Повторно авторизовать почтовые сенсоры (KSMG, KLMS) на Central Node (см. раздел "Настройка интеграции с внешними системами" на стр. 300).
- Повторно настроить соединение Central Node, PCN и SCN с Sandbox (см. раздел "Настройка интеграции с компонентом Sandbox" на стр. 297).
- Повторно настроить перенаправление трафика от Endpoint Agent на Sensor и доверенное соединение с Endpoint Agent (см. раздел "Настройка перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor" на стр. 177).
- Загрузить новый сертификат в Active Directory (если вы используете Active Directory).

Удалите все правила изоляции хостов Endpoint Agent. Соединение с изолированными хостами будет разорвано, вы не сможете ими управлять.

Вы можете сгенерировать новый сертификат через веб-интерфейс сервера Central Node или загрузить самостоятельно созданный сертификат.

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы сгенерировать TLS-сертификат сервера Central Node:*

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform (см. раздел "Начало работы с приложением" на стр. 186) под учетной записью администратора (см. раздел "Создание учетной записи администратора веб-интерфейса приложения" на стр. 194).
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Сертификаты**.
3. В разделе **Сертификат сервера** нажмите на кнопку **Сгенерировать**.

   Откроется окно подтверждения действия.
4. Нажмите на кнопку **Да**.

Kaspersky Anti Targeted Attack Platform сгенерирует новый TLS-сертификат. Страница автоматически обновится.

► *Связь с почтовыми сенсорами, компонентом Sandbox, приложением Kaspersky Endpoint Agent будет прервана до повторной авторизации.*

Вы можете самостоятельно подготовить TLS-сертификат и загрузить его через веб-интерфейс Kaspersky Anti Targeted Attack Platform.

Файл TLS-сертификата, предназначенный для загрузки, должен удовлетворять следующим требованиям:

- Файл должен содержать сам сертификат и закрытый ключ шифрования соединения.
- Файл должен иметь формат PEM.

  Приложение не работает с сертификатами другого формата.

  Если вы подготовили сертификат в другом формате, вам нужно конвертировать его в формат PEM.
- Длина закрытого ключа должна быть 2048 бит или более.

Подробнее о подготовке TLS-сертификатов к импорту см. в документации Open SSL.

Выполняйте действия по загрузке TLS-сертификат в веб-интерфейсе того сервера, на который вы хотите загрузить сертификат.

► *Чтобы загрузить самостоятельно подготовленный TLS-сертификат через веб-интерфейс Kaspersky Anti Targeted Attack Platform:*

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью администратора (см. раздел "Создание учетной записи администратора веб-интерфейса приложения" на стр. 194).
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Сертификаты**.
3. В разделе **Сертификат сервера** нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.
4. Выберите файл TLS-сертификата, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

TLS-сертификат будет добавлен в Kaspersky Anti Targeted Attack Platform.

Связь с почтовыми сенсорами, компонентом Sandbox, приложением Kaspersky Endpoint Agent будет прервана до повторной авторизации.

Скачивание TLS-сертификата сервера на компьютер

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы скачать TLS-сертификат сервера на компьютер:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Сертификаты**.
2. В разделе **Сертификат сервера** нажмите на кнопку **Скачать**.

Файл сертификата сервера будет сохранен в папке загрузки браузера.

Назначение DNS-имени сервера

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы назначить имя сервера для использования DNS-серверами:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сетевые параметры**.
2. В поле **Имя сервера (FQDN)** введите полное доменное имя сервера.

   Указывайте имя сервера в формате FQDN (например, `host.domain.com` или `host.domain.subdomain.com`).
3. Нажмите на кнопку **Применить**.

Имя сервера будет назначено.

Настройка параметров DNS

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить параметры DNS:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сетевые параметры**.
2. В блоке параметров **Параметры DNS** в поле **Главный и дополнительный DNS-серверы** введите IP-адреса DNS-серверов.
3. Нажмите на кнопку **Применить**.

Параметры DNS будут настроены.

Настройка параметров сетевого интерфейса

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить параметры сетевого интерфейса:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сетевые параметры**.
2. Выберите сетевой интерфейс, параметры которого вы хотите настроить.

   Откроется окно **Изменить сетевой интерфейс**.
3. В блоке параметров **Состояние** выберите один из следующих вариантов:
   - **Выключено**.
   - **Включено, используется DHCP-сервер**, если вы хотите, чтобы для сетевого интерфейса использовались параметры, полученные от DHCP-сервера.
   - **Включено, настройка вручную**, если вы хотите, чтобы для сетевого интерфейса использовались параметры, заданные вручную.
4. Если вы выбрали **Включено, настройка вручную**, укажите значения для следующих параметров:
   a. В поле **IP** укажите IP-адрес сетевого интерфейса.
   b. В поле **Маска подсети** укажите маску подсети сетевого интерфейса.
   c. В поле **Шлюз** введите IP-адрес шлюза.
5. Нажмите на кнопку **Сохранить**.

Параметры сетевого интерфейса будут настроены.

Настройка сетевого маршрута для использования по умолчанию

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить сетевой маршрут для использования по умолчанию:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сетевые параметры**.
2. В блоке параметров **Сетевой маршрут** в раскрывающемся списке **Сетевой интерфейс** выберите сетевой интерфейс, для которого вы хотите настроить сетевой маршрут.
3. В поле **Шлюз** введите IP-адрес шлюза.
4. Нажмите на кнопку **Применить**.

Сетевой маршрут для использования по умолчанию будет настроен.

Настройка параметров соединения с прокси-сервером

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить параметры соединения с прокси-сервером:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке параметров **Прокси-сервер** переведите переключатель в положение **Включено**.
3. В поле **Хост** укажите URL-адрес прокси-сервера.
4. В поле **Порт** укажите порт подключения к прокси-серверу.
5. В поле **Имя пользователя** укажите имя пользователя для аутентификации на прокси-сервере.
6. В поле **Пароль** укажите пароль для аутентификации на прокси-сервере.
7. Если вы не хотите использовать прокси-сервер при подключении к локальным адресам, установите флажок **Не использовать прокси-сервер для локальных адресов**.
8. Нажмите на кнопку **Применить**.

Параметры соединения с прокси-сервером будут настроены.

Настройка параметров соединения с почтовым сервером

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Приложение может отправлять уведомления об обнаружениях и работе системы. Для этого необходимо настроить параметры сервера для отправки уведомлений.

► *Чтобы настроить параметры сервера для отправки уведомлений:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на вкладку **Конфигурация почтового сервера**.
3. В поле **Хост** укажите IP-адрес почтового сервера.
4. В поле **Порт** укажите порт подключения к почтовому серверу.
5. В поле **Отправлять с адреса** укажите адрес электронной почты, с которого будут отправляться уведомления.
6. Если вы хотите включить проверку подлинности на почтовом сервере, установите флажок **Использовать SMTP-проверку подлинности получателей сообщений**.
7. В поле **Имя пользователя** укажите имя пользователя для аутентификации на сервере для отправки уведомлений.
8. В поле **Пароль** укажите пароль для аутентификации на сервере для отправки уведомлений.
9. Если вы хотите использовать TLS-шифрование при отправке уведомлений, установите флажок **Использовать TLS-шифрование**.
10. Если вы хотите проверить сертификат почтового сервера, установите флажок **Подтверждать TLS-шифрование**.

    В поле **Отпечаток сертификата** отобразится отпечаток сертификата почтового сервера.

    > Если флажок **Подтверждать TLS-шифрование** не установлен, приложение будет считать любой сертификат почтового сервера доверенным.

11. Нажмите на кнопку **Применить**.

Параметры сервера для отправки уведомлений будут настроены.

Выбор операционных систем для проверки объектов в Sandbox

Вы можете выбрать набор операционных систем, на основе которого будут формироваться задачи на проверку объектов для компонента Sandbox. Вам потребуется установить виртуальные машины с операционными системами (см. раздел "Установка и настройка образов операционных систем и приложений для работы компонента Sandbox" на стр. 221), которые соответствуют выбранному набору, на сервере Sandbox.

► *Чтобы выбрать набор операционных систем:*

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sandbox**.
2. Выберите закладку **Параметры**.
3. В блоке параметров **Набор ОС** выберите один из вариантов:
   - **Windows 7, Windows 10**.
   - **CentOS 7.8, Windows 7, Windows 10**.

- **Astra Linux 1.7, Windows 7, Windows 10**.
- **Пользовательские**.

4. Если вы выбрали **Пользовательские**, в блоке параметров **Состав набора** установите флажки напротив операционных систем, которые вы хотите использовать в наборе.

   Пользовательские операционные системы отображаются в списке, если виртуальные машины с этими операционными системами были установлены на сервере Sandbox. Преднастроенные операционные системы всегда отображаются в списке, но если виртуальные машины с этими операционными системами не развернуты, рядом с названием операционной системы отображается статус **Неизвестно**.

Kaspersky Anti Targeted Attack Platform будет создавать задачи на проверку объектов в Sandbox в соответствии с выбранным набором.

Если набор операционных систем, установленных на сервере Sandbox, не совпадает с набором, выбранным на сервере Central Node, объекты не отправляются на проверку этому серверу Sandbox. При подключении к серверу Central Node нескольких серверов Sandbox приложение отправляет объекты на проверку тем серверам Sandbox, на которых установлены операционные системы, соответствующие выбранному на Central Node набору.

Вы можете изменить набор операционных систем в ходе эксплуатации приложения. В этом случае вам нужно убедиться, что конфигурация сервера Sandbox соответствует аппаратным требованиям (см. раздел "Аппаратные и программные требования" на стр. 27).

В режиме распределенного решения и мультитенантности настройки набора операционных систем, заданные на сервере PCN, не распространяются на подключенные к нему серверы SCN. Вы можете выбрать набор операционных систем для каждого сервера PCN и SCN отдельно.

Управление компонентом Sensor

Компонент Sensor (на стр. 66) выполняет прием данных из сетевого и почтового трафика.

Вы можете установить компоненты Sensor и Central Node на одном сервере или на отдельных серверах. Установленный на отдельном сервере компонент Sensor необходимо подключить к серверу с компонентом Central Node. Запрос на подключение создается во время установки компонента (см. раздел "Установка компонента Sensor на отдельном сервере" на стр. 142).

Если компонент Sensor установлен на одном сервере с компонентом Central Node, вы можете настраивать параметры компонента Sensor в веб-интерфейсе Kaspersky Anti Targeted Attack Platform. Если компонент Sensor установлен на отдельном сервере, в веб-интерфейсе Kaspersky Anti Targeted Attack Platform вы можете только обрабатывать запросы на подключение от этого компонента (см. раздел "Обработка запроса на подключение от компонента Sensor" на стр. 262) и просматривать информацию о нем в таблице серверов с компонентом Sensor (см. раздел "Просмотр таблицы серверов с компонентом Sensor" на стр. 261). Другие параметры компонента настраиваются в меню администратора (см. раздел "Начало работы в меню администратора приложения" на стр. 188).

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия по подключению к серверам PCN или SCN.

В этом разделе

Просмотр таблицы серверов с компонентом Sensor 261

Обработка запроса на подключение от компонента Sensor 262

Настройка максимального размера проверяемого файла 262

Настройка получения зеркалированного трафика со SPAN-портов 263

Выбор сетевых протоколов для получения зеркалированного трафика со SPAN-портов 263

Настройка интеграции с почтовым сервером по протоколу SMTP 265

Настройка TLS-шифрования соединений с почтовым сервером по протоколу SMTP 266

Настройка интеграции с прокси-сервером по протоколу ICAP 267

Настройка записи сырого сетевого трафика 273

Настройка интеграции с почтовым сервером по протоколу POP3 275

Просмотр таблицы серверов с компонентом Sensor

Таблица серверов с компонентом Sensor находится в разделе **Серверы Sensor** окна веб-интерфейса приложения.

В поле **Отпечаток сертификата** отображается отпечаток TLS-сертификата сервера Central Node.

В таблице **Список серверов** содержится следующая информация:

- **IP/имя** – IP-адрес или доменное имя сервера с компонентом Sensor.
- **Тип** – тип компонента Sensor. Может принимать следующие значения:
  - **Central Node** – компонент Sensor установлен на том же сервере, что и компонент Central Node.
  - **Удаленный** – компонент Sensor установлен на другом сервере или в качестве компонента Sensor используется почтовый сенсор.
- **Отпечаток сертификата** – отпечаток TLS-сертификата, с помощью которого устанавливается шифрованное соединение между серверами с компонентами Sensor и Central Node.
- **KSN/KPSN** – состояние подключения к репутационным базам KSN/KPSN.
- **SPAN** – состояние обработки SPAN-трафика.
- **SMTP** – состояние интеграции с почтовым сервером по протоколу SMTP.
- **ICAP** – состояние интеграции с прокси-сервером по протоколу ICAP.
- **POP3** – состояние интеграции с почтовым сервером по протоколу POP3.
- **Состояние** – состояние запроса на подключение.

Обработка запроса на подключение от компонента Sensor

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Вы можете принять, отклонить или отозвать ранее принятый запрос на подключение от компонента Sensor.

► *Чтобы обработать запрос на подключение от компонента Sensor, выполните следующие действия:*

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.

   В таблице **Список серверов** отобразятся уже подключенные компоненты Sensor, а также запросы на подключение.

2. В строке с запросом на подключение компонента Sensor выполните одно из следующих действий:
   - Если вы хотите подключить компонент Sensor, нажмите на кнопку **Принять**.
   - Если вы не хотите подключать компонент Sensor, нажмите на кнопку **Отклонить**.
3. В окне подтверждения нажмите на кнопку **Да**.

Запрос на подключение от компонента Sensor будет обработан.

Настройка максимального размера проверяемого файла

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить максимальный размер проверяемого файла:*

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.

   Отобразится таблица **Список серверов**.

2. Выберите компонент Sensor, для которого вы хотите настроить максимальный размер проверяемого файла.

   Откроется страница с параметрами компонента Sensor.

3. Выберите раздел **Общие параметры**.
4. Если вы хотите, чтобы приложение проверяло файлы любых размеров, установите флажок **Без ограничений**.
5. Если вы хотите установить максимальный размер, при превышении которого приложение не будет проверять файлы, выполните следующие действия:
   a. Снимите флажок **Без ограничений**.
   b. В поле под флажком введите максимально допустимый размер файла.
   c. В раскрывающемся списке справа от поля выберите единицу измерения.

6. Нажмите на кнопку **Применить**.

Максимальный размер проверяемого файла будет настроен.

Настройка получения зеркалированного трафика со SPAN-портов

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить получение зеркалированного трафика со SPAN-портов:*

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.

   Отобразится таблица **Список серверов**.

2. Выберите компонент Sensor, для которого вы хотите настроить получение зеркалированного трафика со SPAN-портов.

   Откроется страница с параметрами компонента Sensor.

3. Выберите раздел **Обработка SPAN-трафика**.

   Отобразится таблица **Сетевые интерфейсы**.

4. В строке сетевого интерфейса, с которого вы хотите настроить получение зеркалированного трафика, переведите переключатель в столбце **Проверка SPAN-трафика** в положение **Включено**.
5. В раскрывающемся списке **Поток перехвата** выберите поток, который будет обрабатывать этот сетевой интерфейс.
6. В раскрывающемся списке **Выбор процессора** выберите процессор, который будет обрабатывать сетевой трафик.
7. Нажмите на кнопку **Применить**.

Получение зеркалированного трафика со SPAN-портов будет настроено.

Выбор сетевых протоколов для получения зеркалированного трафика со SPAN-портов

Kaspersky Anti Targeted Attack Platform может получать, обрабатывать зеркалированный трафик и извлекать объекты и метаинформацию протоколов. Вы можете настроить получение зеркалированного трафика со SPAN-портов.

► *Чтобы выбрать сетевые протоколы для получения зеркалированного трафика со SPAN-портов:*

1. Войдите в консоль управления сервера Sensor по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке приложения (см. раздел "Установка и первоначальная настройка приложения" на стр. 110).

Откроется меню параметров компонента Sensor. Если меню не открылось, введите команду `kata-admin-menu` и нажмите на клавишу **ENTER**.

3. Перейдите в раздел **Program settings** → **Configure traffic capture** → **Setup capture protocols**, используя клавиши ↑, ↓ и **ENTER**. Выбранная строка подсвечивается красным.

   Откроется окно, где вы можете включить или отключить получение зеркалированного трафика со SPAN-портов по следующим сетевым протоколам:

   - **DNS**.
   - **FTP**.
   - **HTTP**.
   - **HTTP2**.
   - **SMTP**.
   - **SMB**.
   - **NFS**.

   Для того чтобы анализировать трафик NFS, необходимо смонтировать NFS-раздел с указанием версии протокола.

Пример:

для NFS v.4:

```
mount -t nfs -o vers=4 -O uid=1000, iocharset=utf-8
<address>:/from/dir /to/dir
```

для NFS v.3:

```
mount -t nfs -o vers=3 -O uid=1000, iocharset=utf-8
<address>:/from/dir /to/dir
```

   Если получение зеркалированного трафика со SPAN-порта по сетевому протоколу включено, справа от названия сетевого протокола отображается **[x]**. Если получение трафика зеркалированного трафика со SPAN-порта по какому-либо сетевому протоколу отключено, справа от названия сетевого протокола отображается **[ ]**.

   По умолчанию получение зеркалированного трафика со SPAN-портов включено по всем сетевым протоколам, кроме **HTTP2**.

4. Если вы хотите включить или отключить получение зеркалированного трафика со SPAN-портов по какому-либо сетевому протоколу, выберите сетевой протокол, используя клавиши ↑, ↓,и нажмите на клавишу **ENTER**.
5. Выберите **Apply and Exit** и нажмите на клавишу **ENTER**.

Сетевые протоколы для получения зеркалированного трафика со SPAN-портов будут выбраны.

Настройка интеграции с почтовым сервером по протоколу SMTP

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить интеграцию с почтовым сервером по протоколу SMTP:*

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.

   Отобразится таблица **Список серверов**.

2. Выберите компонент Sensor, для которого вы хотите настроить интеграцию с почтовым сервером по протоколу SMTP.

   Откроется страница с параметрами компонента Sensor.

3. Выберите раздел **SMTP-интеграция**.
4. В поле **Состояние** переведите переключатель в положение **Включено**.
5. В поле **Домены назначения** укажите имя почтового домена или поддомена. Приложение будет проверять сообщения электронной почты, отправленные на почтовые ящики указанных доменов.

   Чтобы отключить домен или поддомен, заключите его в форму `!domain.tld`.

   Если вы оставите имя почтового домена пустым, приложение будет принимать сообщения, отправленные на любые адреса электронной почты.

6. В поле **Клиенты** укажите IP-адреса хостов и/или маски подсетей в нотации CIDR, с которыми приложении разрешено взаимодействовать по протоколу SMTP.

   Чтобы отключить хост или подсеть, заключайте адрес в форму `!host`.

   Если вы оставите это поле пустым, приложение будет принимать следующие сообщения:

   - с любых адресов электронной почты, если вы указали почтовые домены в поле **Домены назначения**;
   - от почтового сервера, находящегося в той же подсети, что и сервер с компонентом Sensor, если в поле **Домены назначения** не указан ни один домен.

7. Если вы хотите, чтобы приложение принимало сообщения любых размеров, в группе параметров **Ограничение по размеру сообщения** установите флажок **Без ограничений**.
8. Если вы хотите установить максимально допустимый размер входящих сообщений, выполните следующие действия:

   a. Снимите флажок **Без ограничений**.

   b. В поле под флажком введите максимально допустимый размер сообщения.

   c. В раскрывающемся списке справа от поля выберите единицу измерения.

9. Нажмите на кнопку **Применить**.

Интеграция с почтовым сервером по протоколу SMTP будет настроена. Приложение будет проверять сообщения электронной почты, полученные по протоколу SMTP, согласно заданным параметрам.

Если вы развернули компоненты Central Node и Sensor в виде кластера (см. раздел "Развертывание компонентов Central Node и Sensor в виде кластера" на стр. 124), вы можете настроить отказоустойчивую интеграцию с почтовым сервером.

► *Чтобы настроить отказоустойчивую интеграцию с почтовым сервером:*

1. Настройте на сервере DNS функцию Round Robin для доменного имени, соответствующего кластеру Central Node.
2. В параметрах почтового сервера укажите это доменное имя.

Интеграция с почтовым сервером будет настроена по доменному имени. Почтовый сервер обратится к случайному серверу кластера. При отказе этого сервера почтовый сервер будет обращаться к другому работоспособному серверу кластера.

Настройка TLS-шифрования соединений с почтовым сервером по протоколу SMTP

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить TLS-шифрование соединений с почтовым сервером по протоколу SMTP:*

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.

   Отобразится таблица **Список серверов**.
2. Выберите компонент Sensor, для которого вы хотите настроить TLS-шифрование соединений с почтовым сервером по протоколу SMTP.

   Откроется страница с параметрами компонента Sensor.
3. Выберите раздел **SMTP-интеграция**.
4. В поле **Состояние** переведите переключатель в положение **Включено**, если он выключен.
5. В блоке **Режим TLS-безопасности клиента** выберите один из следующих вариантов:
   - **Не использовать TLS-шифрование**.

     Приложение не будет устанавливать TLS-шифрование соединений с почтовым сервером.
   - **Проверять возможность TLS-шифрования входящих сообщений**.

     Приложение будет поддерживать TLS-шифрование соединений, но шифрование не будет являться обязательным.
   - **Требовать TLS-шифрование входящих сообщений**.

     Приложение будет принимать сообщения только по зашифрованным каналам.
6. Нажмите на кнопку **Скачать TLS-сертификат**, чтобы сохранить TLS-сертификат сервера с компонентом Sensor на компьютере в папке загрузки браузера.

   Этот сертификат необходим для проверки подлинности на почтовом сервере.
7. В блоке **Запрос клиентского TLS-сертификата** выберите один из следующих вариантов:
   - **Не запрашивать**.

     Приложение не будет проверять TLS-сертификат почтового сервера.
   - **Запрашивать**.

Приложение будет запрашивать у почтового сервера TLS-сертификат при его наличии.

- **Требовать**.

  Приложение будет принимать сообщения только от тех почтовых серверов, у которых есть TLS-сертификат.

8. Нажмите на кнопку **Применить**.

TLS-шифрование соединений с почтовым сервером по протоколу SMTP будет настроено.

Настройка интеграции с прокси-сервером по протоколу ICAP

Интеграция с прокси-сервером по протоколу ICAP с обратной связью позволяет вам предотвратить попадание вредоносных объектов в локальную сеть организации и ограничить переход на вредоносные или фишинговые веб-сайты пользователям хоста. Kaspersky Anti Targeted Attack Platform выступает в роли ICAP-сервера, а ваш прокси-сервер – в роли ICAP-клиента. В процессе работы прокси-сервер передает запросы по протоколу ICAP на ICAP-сервер. ICAP-сервер выполняет проверку и возвращает результат на прокси-сервер. В случае обнаружения угроз пользователю хоста отобразится HTML-страница оповещения.

В этом разделе

Включение и отключение интеграции с прокси-сервером по протоколу ICAP....267
Включение и отключение проверки ICAP-трафика в режиме реального времени....269
Настройка параметров проверки ICAP-трафика в режиме реального времени....271
Настройка отображения страниц уведомлений....272

Включение и отключение интеграции с прокси-сервером по протоколу ICAP

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

При использовании отдельного прокси-сервера Kaspersky Anti Targeted Attack Platform не обеспечивает шифрование ICAP-трафика и аутентификацию ICAP-клиентов по умолчанию. Администратору приложения необходимо самостоятельно обеспечить безопасное сетевое соединение между вашим прокси-сервером и Kaspersky Anti Targeted Attack Platform с помощью туннелирования трафика или средствами iptables.

► *Чтобы включить или отключить интеграцию с прокси-сервером по протоколу ICAP на сервере с установленными компонентами Central Node и Sensor:*

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.

   Отобразится таблица **Список серверов**.

2. Нажмите на компонент Sensor **localhost**.

Откроется страница с параметрами компонента Sensor.

3. Выберите раздел **ICAP-интеграция с прокси-сервером**.
4. В разделе **Параметры > <имя сервера с компонентом Sensor>** в поле **Состояние** выполните одно из следующих действий:
   - Если вы хотите включить интеграцию с прокси-сервером по протоколу ICAP, переведите переключатель в положение **Включено**.

     По умолчанию переключатель находится в положении **Выключено**.
   - Если вы хотите отключить интеграцию с прокси-сервером по протоколу ICAP, переведите переключатель в положение **Выключено**.
5. В поле **Хост** отображается URL-адрес службы Response Modification (RESPMOD), обрабатывающей входящий трафик, в формате `icap://<host>:1344/av/respmod, где <host>` – IP-адрес сервера с установленным компонентом Sensor. Для настройки интеграции с Kaspersky Anti Targeted Attack Platform скопируйте этот URL-адрес и укажите его в параметрах прокси-сервера, который используется в вашей организации.

Интеграция с прокси-сервером по протоколу ICAP будет настроена.

► *Чтобы включить или отключить интеграцию с прокси-сервером по протоколу ICAP на отдельном сервере с компонентом Sensor:*

1. Войдите в консоль управления сервера Sensor по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке приложения.

   Откроется меню параметров компонента Sensor. Если меню не открылось, введите команду `kata-admin-menu` и нажмите на клавишу **ENTER**.
3. Перейдите в раздел **Program settings** → **Configure ICAP integration.**

   Для выбора строки вы можете использовать клавиши ↑, ↓ и **ENTER**. Выбранная строка подсвечивается красным.
4. В открывшемся окне выберите строку **Enabled** нажмите на клавишу **ENTER**.

   Справа от названия параметра **Enabled** отобразится значение **[x]**.
5. Укажите в параметрах используемого в вашей организации прокси-сервера URL-адрес, который отображается в поле **RESPMOD**.

Интеграция с прокси-сервером и отдельным сервером с компонентом Sensor по протоколу ICAP будет настроена.

Если вы развернули компоненты Central Node и Sensor в виде кластера, вы можете настроить отказоустойчивую интеграцию с прокси-сервером.

► *Чтобы настроить отказоустойчивую интеграцию с прокси-сервером:*

1. Настройте на сервере DNS функцию Round Robin для доменного имени, соответствующего кластеру Central Node.
2. В параметрах прокси-сервера укажите это доменное имя.

Интеграция с прокси-сервером будет настроена по доменному имени. Прокси-сервер обратится к случайному серверу кластера. При отказе этого сервера прокси-сервер будет обращаться к другому работоспособному серверу кластера.

Включение и отключение проверки ICAP-трафика в режиме реального времени

Включение и отключение проверки ICAP-трафика в режиме реального времени доступно, если включена интеграция с прокси-сервером по протоколу ICAP (см. раздел "Включение и отключение интеграции с прокси-сервером по протоколу ICAP" на стр. 267).

Если проверка ICAP-трафика в режиме реального времени включена, Kaspersky Anti Targeted Attack Platform передает информацию о проверенных объектах ICAP-клиенту в режиме реального времени. Это позволяет предотвратить скачивание вредоносных объектов и переход по недоверенным ссылкам.

► *Чтобы включить или отключить проверку ICAP-трафика в режиме реального времени на сервере с установленными компонентами Central Node и Sensor:*

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.

   Отобразится таблица **Список серверов**.
2. Нажмите на компонент Sensor **localhost**.
3. Выберите раздел **ICAP-интеграция с прокси-сервером**.

   При включении интеграции (см. раздел "Включение и отключение интеграции с прокси-сервером по протоколу ICAP" на стр. 267) в окне **Параметры** > **<имя сервера Sensor>** отобразится раздел **Проверка в режиме реального времени**.
4. В блоке параметров **Проверка в режиме реального времени** выберите один из следующих вариантов:
   - **Отключено**.

     При выборе этого варианта проверка ICAP-трафика в режиме реального времени будет отключена. По умолчанию выбран этот вариант.
   - **Включено, стандартная проверка трафика ICAP**.

     При включении этого типа проверки репутация файлов и URL-адресов проверяется в базе знаний Kaspersky Security Network, файлы проверяются модулями Anti-Malware Engine и YARA.
   - **Включено, усиленная проверка трафика ICAP**.

     При включении этого типа проверки репутация файлов и URL-адресов проверяется в базе знаний Kaspersky Security Network, файлы проверяются компонентом Sandbox и модулями Anti-Malware Engine и YARA.
5. Нажмите на кнопку **Применить**.
6. Если вы включили проверку ICAP-трафика в режиме реального времени и установили режим усиленной проверки или режим стандартной проверки, в поле **Хост** отобразится URL-адрес службы Request Modification (REQMOD), обрабатывающей исходящий трафик, в формате icap://<host>:1344/av/reqmod, где <host> – IP-адрес сервера с установленным компонентом Sensor. Для настройки интеграции с Kaspersky Anti Targeted Attack Platform скопируйте URL-адрес и укажите его в параметрах прокси-сервера, который используется в вашей организации.

Проверка ICAP-трафика в режиме реального времени будет включена или отключена.

► *Чтобы включить или отключить проверку ICAP-трафика в режиме реального времени на отдельном сервере с компонентом Sensor:*

1. Войдите в консоль управления сервера Sensor по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке приложения.

   Откроется меню параметров компонента Sensor. Если меню не открылось, введите команду `kata-admin-menu` и нажмите на клавишу **ENTER**.
3. Перейдите в раздел **Program settings** → **Configure ICAP integration**.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и **ENTER**. Выбранная строка подсвечивается красным.
4. В открывшемся окне убедитесь, что справа от параметра **Enabled** установлено значение **[x]**.
5. Выберите один из следующих вариантов:
   - **Disable real-time scanning**.

     При выборе этого варианта проверка ICAP-трафика в режиме реального времени будет отключена. По умолчанию выбран этот вариант.
   - **Standard ICAP scanning**.

     При включении этого типа проверки репутация файлов и URL-адресов проверяется в базе знаний Kaspersky Security Network, файлы проверяются модулями Anti-Malware Engine и YARA.
   - **Advanced ICAP scanning**.

     При включении этого типа проверки репутация файлов и URL-адресов проверяется в базе знаний Kaspersky Security Network, файлы проверяются компонентом Sandbox и модулями Anti-Malware Engine и YARA.
6. Выберите необходимый вариант и нажмите на клавишу **ENTER**. Справа от выбранного значения отобразится **(O)**.

   Для выбора строки вы можете использовать клавиши ↑ и ↓. Выбранная строка подсвечивается красным.
7. Если вы включили проверку ICAP-трафика в режиме реального времени и установили режим усиленной проверки или режим стандартной проверки, укажите в параметрах используемого в вашей организации прокси-сервера URL-адрес, который отображается в поле **REQMOD**.

Проверка ICAP-трафика в режиме реального времени на отдельном сервере с компонентом Sensor будет включена или отключена.

Если вы включили проверку ICAP-трафика в режиме реального времени, при отключении интеграции с прокси-сервером проверка не будет работать. Все параметры проверки ICAP-трафика сохраняются. При следующем включении интеграции с прокси-сервером проверка ICAP-трафика также будет включена.

Настройка параметров проверки ICAP-трафика в режиме реального времени

Настройку параметров проверки ICAP-трафика в режиме реального времени на отдельных серверах с установленным компонентом Sensor возможно выполнить только в режиме Technical Support Mode (см. раздел "Начало работы с приложением в режиме Technical Support Mode" на стр. 189). Для выполнения действий в режиме Technical Support Mode вам рекомендуется обратиться в Службу технической поддержки (см. раздел "Обращение в Службу технической поддержки" на стр. 670).

Вы можете настроить параметры проверки ICAP-трафика на сервере с установленными компонентами Central Node и Sensor в режиме реального времени для антивирусной проверки данных. Результаты проверки будут отображаться пользователю хоста на HTML-странице уведомления.

► *Чтобы настроить параметры проверки ICAP-трафика в режиме реального времени:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Проверка трафика ICAP**.

   Отобразится страница с параметрами проверки ICAP-трафика.

   По умолчанию в блоке параметров **Уведомления** загружены страницы соответствующие следующим событиям:

   - В поле **Блокировка ссылки** загружена страница, которая будет отображаться в случае обнаружения угрозы по запрашиваемому пользователем адресу.
   - В поле **Блокировка файла** загружена страница, которая будет отображаться в случае обнаружения угрозы в проверяемом файле.
   - В поле **Проверка файла** загружена страница, которая будет отображаться в случае запуска проверки файла. Если файл безопасен, пользователю будет доступна ссылка на скачивание файла.
   - В поле **Истек срок хранения файла** файла загружена страница, которая будет отображаться в случае, если файл был проверен и приложение Kaspersky Anti Targeted Attack Platform не обнаружило угроз, но время хранения этого файла в хранилище приложения истекло.

   По умолчанию в Kaspersky Anti Targeted Attack Platform загружены HTML-страницы из комплекта поставки. Вы можете загрузить свои страницы уведомлений и настроить их отображение (см. раздел "Настройка отображения страниц уведомлений" на стр. 272). Максимальный размер страницы уведомления не должен превышать 1,5 МБ. В случае загрузки страницы уведомления размером более 1,5 МБ отобразится ошибка.

2. В блоке параметров **Порог блокировки файлов** в поле **Важность обнаружения Sandbox** выберите значение из раскрывающегося списка. Значения соответствуют возможному влиянию обнаружения на безопасность компьютера или локальной сети вашей организации по опыту "Лаборатории Касперского".

   Параметр может принимать одно из следующих значений:

   - **Высокая** – обнаружение высокой степени важности. По умолчанию выбран этот вариант.
   - **Средняя** – обнаружение средней степени важности.
   - **Низкая** – обнаружение низкой степени важности.

3. В блоке параметров **Время ожидания проверки** в поле **Время ожидания** укажите значение, по истечении которого ссылка на проверяемый файл будет разблокирована и будет доступна возможность скачать проверяемый файл.

   Значение по умолчанию: 10 минут. Вы можете установить любое значение, которое больше 1 минуты.

4. Нажмите на кнопку **Применить.**

Проверка будет выполняться в соответствии с настроенными параметрами.

Настройка отображения страниц уведомлений

Во время проверки ICAP-трафика в режиме реального времени Kaspersky Anti Targeted Attack Platform может выполнять различные операции с проверяемыми объектами: блокировать переход по URL-адресу, блокировать скачивание файла, ограничивать скачивание файла, пока он находится на проверке, и предлагать повторно загрузить файл, если срок его хранения после проверки истек. Во время выполнения этих операций для пользователя хоста, с которого был отправлен запрос на переход по URL-адресу или скачивание файла, отображается HTML-страница с уведомлением. Если вы хотите, чтобы при операциях с объектами вместо страниц по умолчанию отображались ваши страницы, вы можете загрузить HTML-страницы, настроенные вами.

► *Чтобы загрузить страницу уведомления:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Проверка трафика ICAP**.
2. В разделе **Уведомления** нажмите на кнопку **Обзор** напротив одного из нужных полей.
3. В открывшемся окне выберите свою HTML-страницу.
4. Нажмите на кнопку **Открыть.**

   Ваша страница будет загружена.

Страница уведомления события **Проверка файла** отличается от других страниц уведомления наличием ссылки для скачивания файла. В случае загрузки вашей страницы уведомления **Проверка файла** необходимо в исходном коде загружаемой страницы добавить ссылку на скачивание проверенного файла.

Пример:

```
<html>
  <body>
    <p>Файл находится на проверке. Когда проверка будет завершена, вы сможете скачать его или получите отчет об обнаруженных угрозах.</p>
    <a href="{{ download_url }}">Ссылка на скачивание...</a>
  </body>
</html>
```

Настройка записи сырого сетевого трафика

Kaspersky Anti Targeted Attack Platform позволяет сохранять сырой сетевой трафик для проведения расследования и расширяет возможности по выявлению злонамеренной активности внутри периметра локальной сети организации. Благодаря записи сырого сетевого трафика вы можете проводить ретроспективный анализ сетевых событий и расследовать действия злоумышленников. Сырой сетевой трафик сохраняется в виде дампов в формате PCAP.

Для того чтобы сохранять сырой сетевой трафик, вам необходимо включить сохранение сырого сетевого трафика и настроить параметры записи.

В этом разделе

Включение и настройка параметров записи сырого сетевого трафика на сервере с установленными компонентами Sensor и Central Node 273

Включение и настройка параметров записи сырого сетевого трафика на отдельном сервере с компонентом Sensor 274

Включение и настройка параметров записи сырого сетевого трафика на сервере с установленными компонентами Sensor и Central Node

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия на том сервере PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы включить и настроить запись сырого сетевого трафика на сервере с установленными компонентами Central Node и Sensor:*

1. Подключите и настройте внешнее хранилище (см. раздел "Подключение и настройка внешнего хранилища для компонента Sensor" на стр. 147).
2. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.

   Отобразится таблица **Список серверов**.
3. Выберите компонент Sensor с именем **localhost**.

   Откроется страница с параметрами компонента Sensor.
4. Выберите раздел **Обработка SPAN-трафика**.

   Отобразится таблица **Сетевые интерфейсы**.
5. Откройте вкладку **Запись трафика**.
6. В поле **Записывать трафик** переведите переключатель в положение **Включено**.

   По умолчанию переключатель находится в положении **Выключено**.

   Запись сырого сетевого трафика на сервере с установленными компонентами Central Node и Sensor будет включена. Отобразятся параметры настройки записи сырого трафика.

   По умолчанию сырой сетевой трафик записывается в директорию `//mnt/kaspersky/nta/dumps`. Вы не можете изменить директорию для записи сырого сетевого трафика.

7. При необходимости настройте параметры записи сырого сетевого трафика:

   a. В блоке параметров **Размер хранилища дампов** в поле **Максимальный размер хранилища** укажите максимальный размер дампов сырого трафика, который будет храниться в хранилище.

   По умолчанию значение не задано. Минимальное возможное значение – 1 МБ, максимальное – 1000000 ТБ. Если вы укажете в поле число, которое больше свободного места на жестком диске, отобразится ошибка.

   Если размер дампов, которые хранятся в хранилище, превысит значение, указанное в поле **Максимальный размер хранилища**, то будут удалены ранние дампы, суммарный размер которых равен размеру новых дампов.

   > Если вы уменьшите максимальный размер хранилища, то будут удалены ранние дампы, суммарный размер которых равен изменению параметра **Максимальный размер хранилища**.

   b. Если вы хотите ограничить захват данных в сыром сетевом трафике, в блоке параметров **Фильтрация трафика при сохранении** в поле **Состояние** переведите переключатель в положение **Включено**. Фильтрация трафика может уменьшить размер дампов, сохраняющихся в хранилище и упростить процесс анализ трафика.

   Если вы перевели переключатель в поле **Состояние** в положение **Включено**, то введите в поле **Правило фильтрации BPF** правило фильтрации**.** Для написания правила фильтрации BPF используется формат libpcap**.** Подробнее об описании синтаксиса см. в Руководстве pcap-filter https://www.tcpdump.org/manpages/pcap-filter.7.html.

   Пример выражения для фильтрации:

   ```
   tcp port 102 or tcp port 502
   ```

   c. Если вы хотите назначить срок хранения дампов сырого сетевого трафика, в блоке параметров **Срок хранения дампов** в поле **Состояние** переведите переключатель в положение **Включено**. В поле **Хранить** введите количество дней хранения дампов сырого сетевого трафика. Если дампы сырого сетевого трафика хранятся больше заданного значения хранения, они будут удалены из хранилища.

   d. Нажмите на **Применить**.

   Запись сырого сетевого трафика на сервере с установленными компонентами Sensor и Central Node будет выполняться в соответствии с настроенными параметрами.

В поле **Первый сохраняемый дамп** отображается дата и время первого сохраненного дампа сырого сетевого трафика, а в поле **Последний сохраняемый дамп** отображается дата и время последнего сохраненного дампа сырого сетевого трафика.

Включение и настройка параметров записи сырого сетевого трафика на отдельном сервере с компонентом Sensor

► *Чтобы включить запись сырого сетевого трафика на отдельном сервере с компонентом Sensor:*

1. Подключите и настройте внешнее хранилище (см. раздел "Подключение и настройка внешнего хранилища для компонента Sensor" на стр. 147).
2. Войдите в консоль управления сервера Sensor по протоколу SSH или через терминал.

3. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке приложения.

   Откроется меню параметров компонента Sensor. Если меню не открылось, введите команду `kata-admin-menu` и нажмите на клавишу **ENTER**.

4. Перейдите в раздел **Program settings** → **Configure traffic capture**.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и **ENTER**. Выбранная строка подсвечивается красным.

5. В открывшемся окне выберите строку **Enable traffic storage** нажмите на клавишу **ENTER**.

   Справа от названия строки отобразится значение **[x]**.

   Запись сырого сетевого трафика на отдельном сервере с компонентом Sensor будет включена.

6. При необходимости настройте параметры записи сырого сетевого трафика:

   a. Выберите строку **Traffic storage size** и нажмите **ENTER**. В открывшемся окне укажите максимальный размер дампов сырого трафика в терабайтах, который будет храниться в хранилище.

      По умолчанию значение не задано. Минимальное возможное значение – 1 МБ, максимальное – 1000000 ТБ.

   b. Выберите кнопку **OK** и нажмите **ENTER**.

   c. Выберите строку **Traffic capture BPF-filter** и нажмите **ENTER**. В открывшемся окне введите правило фильтрации. Для написания правила фильтрации BPF используется формат libpcap. Подробнее об описании синтаксиса см. в Руководстве pcap-filter https://www.tcpdump.org/manpages/pcap-filter.7.html.

      Пример выражения для фильтрации:

      `tcp port 102 or tcp port 502.`

   d. Выберите кнопку **OK** и нажмите **ENTER**.

   e. Выберите строку **Traffic storage duration (in days)** и нажмите **ENTER**. В открывшемся окне введите количество дней хранения дампов сырого сетевого трафика в хранилище.

   f. Выберите кнопку **OK** и нажмите **ENTER**.

Запись сырого сетевого трафика на отдельном сервере с установленным компонентом Sensor будет выполняться в соответствии с настроенными параметрами.

Настройка интеграции с почтовым сервером по протоколу POP3

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить интеграцию с почтовым сервером по протоколу POP3:*

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.

   Отобразится таблица **Список серверов**.

2. Выберите компонент Sensor, для которого вы хотите настроить интеграцию с почтовым сервером по протоколу POP3.

   Откроется страница с параметрами компонента Sensor.

3. Выберите раздел **POP3-интеграция**.
4. Переведите переключатель рядом с параметром **Состояние** в положение **Включено**.
5. В поле **Почтовый сервер** укажите IP-адрес почтового сервера, с которым вы хотите настроить интеграцию.
6. В поле **Порт** укажите порт подключения к почтовому серверу.
7. В поле **Принимать каждые** укажите частоту соединения с почтовым сервером в секундах.
8. Если вы хотите использовать TLS-шифрование соединений с почтовым сервером по протоколу POP3, установите флажок **Использовать TLS-шифрование**.
9. В поле **Имя пользователя** укажите имя учетной записи для доступа к почтовому серверу.
10. В поле **Пароль** укажите пароль доступа к почтовому серверу.
11. В раскрывающемся списке **TLS-сертификат** выберите один из следующих вариантов:
    - **Принимать любой**.
    - **Принимать недоверенный самоподписанный**.
    - **Принимать только доверенный**.

    При установке соединения с внешним почтовым сервером рекомендуется настроить прием только доверенных TLS-сертификатов. Прием недоверенных TLS-сертификатов не гарантирует защиту соединения от MITM-атак. Прием доверенных TLS-сертификатов также не полностью гарантирует защиту соединения от MITM-атак, но является самым безопасным из поддерживаемых способов интеграции с почтовым сервером по протоколу POP3.

12. При необходимости в поле **Набор шифров** измените параметры OpenSSL, используемые при установке соединения с почтовым сервером по протоколу POP3.

    Вы можете ознакомиться со справочной информацией OpenSSL по ссылке **Справка**.

13. Нажмите на кнопку **Применить**.

Интеграция с почтовым сервером по протоколу POP3 будет настроена.

Если вы развернули компоненты Central Node и Sensor в виде кластера (см. раздел "Развертывание компонентов Central Node и Sensor в виде кластера" на стр. 124), вы можете настроить отказоустойчивую интеграцию с почтовым сервером.

► *Чтобы настроить отказоустойчивую интеграцию с почтовым сервером:*

1. Настройте на сервере DNS функцию Round Robin для доменного имени, соответствующего кластеру Central Node.
2. В параметрах почтового сервера укажите это доменное имя.

Интеграция с почтовым сервером будет настроена по доменному имени. Почтовый сервер обратится к случайному серверу кластера. При отказе этого сервера почтовый сервер будет обращаться к другому работоспособному серверу кластера.

Управление кластером

Этот раздел содержит информацию об управлении серверами кластера.

В этом разделе

Просмотр таблицы серверов кластера 277

Добавление сервера в кластер 278

Увеличение дискового пространства сервера хранения 278

Вывод серверов из эксплуатации 278

Включение и выключение кластера 279

Просмотр таблицы серверов кластера

► *Чтобы просмотреть таблицу серверов кластера:*

1. Выполните вход в веб-интерфейс для управления масштабированием (см. раздел "Начало работы в веб-интерфейсе для управления масштабированием" на стр. 187).
2. Перейдите в раздел **Кластер**.

Откроется окно с таблицей.

В таблице содержится следующая информация:

- **Тип сервера** – тип сервера в зависимости от его роли в кластере.

  Могут отображаться следующие значения:

  - **Хранение**.
  - **Обработка**.
- **Состояние** – состояние сервера.

  Могут отображаться следующие значения:

  - **Подключен**.
  - **Не подключен**.
- **Имя хоста** – имя сервера.
- **IP** – IP-адрес сервера.
- **ОЗУ** – уровень загрузки оперативной памяти сервера.
- **ЦП** – уровень загрузки процессора сервера.
- **Действие** – действия, которые вы можете выполнить с сервером.

  Доступно следующее действие: **Удалить**.

Добавление сервера в кластер

Для добавления сервера в кластер вам нужно запустить установку Kaspersky Anti Targeted Attack Platform (см. раздел "Развертывание компонентов Central Node и Sensor в виде кластера" на стр. 124) на этом сервере и выполнить шаги по установке компонентов. Добавленный сервер отобразится в списке серверов кластера (см. раздел "Просмотр таблицы серверов кластера" на стр. 277).

Увеличение дискового пространства сервера хранения

Вы можете увеличить дисковое пространство функционирующего сервера хранения, установив дополнительный диск.

Для увеличения дискового пространства сервера хранения с помощью дополнительного диска вам требуется обратиться в Службу технической поддержки (см. раздел "Обращение в Службу технической поддержки" на стр. 670).

Настройка сервера производится в режиме Technical Support Mode.

Вывод серверов из эксплуатации

Для вывода из эксплуатации функционирующего сервера вам требуется обратиться в Службу технической поддержки (см. раздел "Обращение в Службу технической поддержки" на стр. 670).

При отказе сервера вы можете вывести его из эксплуатации самостоятельно.

► *Чтобы вывести из эксплуатации неработоспособный обрабатывающий сервер:*

1. Добавьте новый обрабатывающий сервер в кластер (см. раздел "Добавление сервера в кластер" на стр. 278).
2. Удалите сервер из кластера (см. раздел "Удаление сервера из кластера" на стр. 279).
3. Настройте параметры масштабирования приложения для новой конфигурации.

Обрабатывающий сервер будет выведен из эксплуатации.

► *Чтобы вывести из эксплуатации неработоспособный сервер хранения:*

1. Добавьте новый сервер хранения в кластер (см. раздел "Добавление сервера в кластер" на стр. 278).
2. Удалите неработоспособный сервер хранения из кластера (см. раздел "Удаление сервера из кластера" на стр. 279).

Для удаления неработоспособного сервера хранения из кластера вам потребуется обратиться в Службу технической поддержки (см. раздел "Обращение в Службу технической поддержки" на стр. 670).

Сервер хранения будет выведен из эксплуатации.

Удаление сервера из кластера

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.
Удаленный сервер нельзя восстановить. Убедитесь, что выбранный сервер не функционирует.

► *Чтобы удалить сервер из кластера:*

1. Выполните вход в веб-интерфейс для управления масштабированием (см. раздел "Начало работы в веб-интерфейсе для управления масштабированием" на стр. 187).
2. Перейдите в раздел **Кластер**.
3. В столбце **Действие** нажмите на ссылку **Удалить** напротив того сервера, который вы хотите удалить.
4. Нажмите на кнопку **Продолжить**.

Процесс удаления будет запущен. Удаление может занять около суток. Информация об удаленном сервере не будет отображаться в таблице серверов.

После удаления сервера вы можете изменить конфигурацию серверов кластера или добавить сервер с аналогичной ролью, чтобы сохранить производительность приложения на прежнем уровне.

Включение и выключение кластера

Если вы хотите отключить питание работоспособных серверов кластера, вам нужно предварительно выключить кластер, чтобы избежать потери данных.

► *Чтобы выключить кластер:*

1. Выполните вход в веб-интерфейс для управления масштабированием (см. раздел "Начало работы в веб-интерфейсе для управления масштабированием" на стр. 187).
2. Перейдите в раздел **Кластер**.
3. Нажмите на кнопку **Выключить**.

Работа основных компонентов приложения будет остановлена. Вы можете отключить питание серверов кластера.

► *Чтобы запустить серверы кластера:*

1. Отключите питание серверов, если оно не было отключено ранее.

2. Включите питание сервера хранения.
3. Включите питание остальных серверов.

Серверы кластера будут запущены.

Веб-интерфейс для управления масштабированием (см. раздел "Начало работы в веб-интерфейсе для управления масштабированием" на стр. 187) становится доступным, когда запускается больше половины серверов кластера. Например, если в кластере 7 серверов, веб-интерфейс будет доступен при включении 4 серверов кластера.

Уведомления о максимальной загрузке центрального процессора и оперативной памяти серверов Central Node и Sensor

Высокая загрузка центрального процессора и оперативной памяти серверов Central Node и Sensor может привести к неработоспособности компонентов приложения.

Вы можете настроить максимальные допустимые значения загрузки центрального процессора и оперативной памяти серверов Central Node и Sensor, при превышении которых в верхней части окна раздела **Мониторинг** веб-интерфейса приложения для пользователей с ролью **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности**, **Администратор** и **Локальный администратор** отобразится рамка желтого цвета с предупреждением. Также вы можете настроить отправку уведомлений на адрес или адреса электронной почты и соединение с протоколом SNMP для отправки данных об уровне загрузки центрального процессора и оперативной памяти во внешние системы, поддерживающие этот протокол.

Если вы развернули компоненты Central Node и Sensor в виде кластера, предупреждения отображаются отдельно для каждого сервера кластера.

Пользователи с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** также могут создавать правила для отправки уведомлений. В этом случае для корректной отправки уведомлений вам требуется предварительно настроить максимальные допустимые значения загрузки центрального процессора и оперативной памяти серверов, а также параметры сервера для отправки уведомлений.
В существующих правилах для отправки уведомлений о работе компонентов приложения функция уведомления о загрузке центрального процессора и оперативной памяти серверов будет включена автоматически, если при создании правила в блоке параметров **Компоненты** был установлен флажок **Все**.

kaspersky

В этом разделе

Настройка максимального допустимого значения загрузки центрального процессора и оперативной памяти серверов Central Node и Sensor 281

Настройка максимального допустимого значения загрузки центрального процессора и оперативной памяти серверов Central Node и Sensor

В режиме распределенного решения и мультитенантности вам нужно задать максимальные допустимые значения загрузки центрального процессора и оперативной памяти на каждом сервере Central Node, с которого вы хотите получать уведомления. Если вы используете кластер Central Node, вы можете настроить эти параметры на любом сервере кластера.

► *Чтобы настроить максимальное допустимое значение загрузки центрального процессора и оперативной памяти серверов Central Node и Sensor:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке параметров **Мониторинг** выполните следующие действия:
   - В поле **Уведомление о загрузке ЦП более чем на N % в течение M минут** укажите максимальное допустимое значение загрузки центрального процессора и время, в течение которого указанная загрузка считается допустимой.

     По умолчанию максимальное допустимое значение загрузки центрального процессора составляет 95% в течение 5 минут.
   - В поле **Уведомление о загрузке ОЗУ более чем на N % в течение M минут** укажите максимальное допустимое значение загрузки оперативной памяти и время, в течение которого указанная загрузка считается допустимой.

     По умолчанию максимальное допустимое значение загрузки оперативной памяти составляет 95% в течение 5 минут.
3. Нажмите на кнопку **Применить**.

Максимальное значение загрузки центрального процессора и оперативной памяти серверов будет настроено. При превышении одного из заданных показателей на сервере Central Node и/или Sensor, в верхней части окна раздела **Мониторинг** веб-интерфейса приложения для пользователей с ролью **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности**, **Администратор** и **Локальный администратор** отобразится рамка желтого цвета с предупреждением (см. раздел "Мониторинг работы приложения" на стр. 244).

Настройка соединения с протоколом SNMP

Вы можете отправлять данные о загрузке центрального процессора и оперативной памяти серверов Central Node и Sensor во внешние системы, поддерживающие протокол SNMP. Для этого вам требуется настроить параметры соединения с протоколом.

Если компонент Central Node развернут в виде кластера, во внешние системы отправляются данные о загрузке центрального процессора и оперативной памяти каждого сервера кластера.

► *Чтобы настроить параметры соединения с протоколом SNMP на сервере Central Node:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке параметров **SNMP** установите флажок **Использовать SNMP**.
3. В поле **Версия протокола** выберите одну из следующих версий протокола:
   - **v2c**.
   - **v3**.
4. Если вы выбрали версию протокола **v2c**, в поле **Строка сообщества** укажите пароль, который будет использоваться для подключения к Kaspersky Anti Targeted Attack Platform.
5. Если вы выбрали **v3**, выполните следующие действия:
   a. В поле **Протокол аутентификации** выберите один из следующих вариантов проверки достоверности и целостности данных, переданных во внешнюю систему:
      - **MD5**.
      - **SHA256**.
   b. В поле **Имя пользователя** укажите имя пользователя.
   c. В поле **Пароль** укажите пароль для аутентификации.

      Имя пользователя и пароль, заданные в полях **Имя пользователя** и **Пароль** должны совпадать с именем пользователя и паролем, заданными при создании учетной записи во внешней системе. Если данные не совпадают, соединение не будет установлено.

   d. В поле **Протокол шифрования** выберите один из следующих типов шифрования:
      - **DES**.
      - **AES**.
   e. В поле **Пароль** укажите пароль для шифрования.

      Пароль, заданный в этом поле, должен совпадать с паролем, заданным во внешней системе.

Параметры соединения с протоколом на сервере Central Node будут настроены. При успешной обработке запроса на получение данных на сервере внешней системы отобразится информация о загрузке центрального процессора и оперативной памяти сервера Central Node.

► *Чтобы настроить параметры соединения с протоколом SNMP на сервере Sensor:*

1. Войдите в консоль управления сервера Sensor по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке приложения (см. раздел "Установка и первоначальная настройка приложения" на стр. 110).

   Отобразится меню администратора компонента приложения.
3. Выполните шаги 2 – 5 инструкции, приведенной выше.

Параметры соединения с протоколом на сервере Sensor будут настроены. При успешной обработке запроса на сервере внешней системы отобразится информация о загрузке центрального процессора и оперативной памяти сервера Sensor.

В режим распределенного решения и мультитенантности параметры соединения с протоколом SNMP для каждого сервера PCN, SCN и Sensor настраиваются отдельно.

В этом разделе

Описание объектов MIB Kaspersky Anti Targeted Attack Platform 283

Описание объектов MIB Kaspersky Anti Targeted Attack Platform

В таблице ниже приведена информация об объектах MIB Kaspersky Anti Targeted Attack Platform.

Таблица 33. Данные о загрузке жесткого диска, центрального процессора и оперативной памяти серверов Central Node и Sensor

Символьное имя	Описание	Идентификатор (OID)
dskTotal	Размер диска или тома, КБ.	1.3.6.1.4.1.2021.9.1.6
dskAvail	Свободное пространство на диске, КБ.	1.3.6.1.4.1.2021.9.1.7
dskUsed	Используемое пространство на диске, КБ.	1.3.6.1.4.1.2021.9.1.8
dskPercent	Процент используемого пространства на диске, %.	1.3.6.1.4.1.2021.9.1.9
laLoad	Среднее значение загрузки системы (load average) в течение 1, 5 и 15 минут.	1.3.6.1.4.1.2021.10.1.3
memTotalReal	Размер оперативной памяти, КБ.	1.3.6.1.4.1.2021.4.5
memAvailReal	Количество используемой оперативной памяти, КБ.	1.3.6.1.4.1.2021.4.6
memTotalFree	Количество свободной оперативной памяти, КБ.	1.3.6.1.4.1.2021.4.11

Работа с информацией о хостах с компонентом Endpoint Agent

Приложение, выступающее в роли компонента Endpoint Agent (см. раздел "Компонент Endpoint Agent" на стр. 68), устанавливается на отдельные компьютеры (далее также "хосты"), входящие в IT-инфраструктуру организации. Приложение осуществляет постоянное наблюдение за процессами, запущенными на этих хостах, открытыми сетевыми соединениями и изменяемыми файлами.

Пользователи с ролью **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности**, **Аудитор**, **Локальный администратор** и **Администратор** могут оценить регулярность получения данных с хостов с компонентом Endpoint Agent, на закладке **Endpoint Agents** окна веб-интерфейса сервера Central Node в рамках тех тенантов, к данным которых у них есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса приложения" на стр. 200). Если вы используете режим распределенного решения и мультитенантности, то в веб-интерфейсе сервера PCN отображается список хостов с компонентом Endpoint Agent для PCN и всех подключенных SCN.

Пользователи с ролью **Локальный администратор** и **Администратор** могут настроить отображение регулярности получения данных с хостов с компонентом Endpoint Agent в рамках тех тенантов, к данным которых у них есть доступ.

В случае возникновения подозрительной сетевой активности пользователь с ролью **Старший сотрудник службы безопасности** может изолировать от сети (см. раздел "Сетевая изоляция хостов с компонентом Endpoint Agent" на стр. 448) любой из хостов с компонентом Endpoint Agent в рамках тех тенантов, к данным которых у него есть доступ. При этом соединение между сервером с компонентом Central Node и хостом с компонентом Endpoint Agent не будет прервано.

Для оказания поддержки при неполадках в работе компонента Endpoint Agent специалисты Службы технической поддержки (см. раздел «Обращение в Службу технической поддержки» на стр. 670) могут попросить вас в отладочных целях выполнить следующие действия (в том числе в режиме Technical Support Mode (см. раздел «Начало работы с приложением в режиме Technical Support Mode» на стр. 189)):

- Активировать функциональность получения расширенной диагностической информации.
- Изменить параметры отдельных компонентов приложения.
- Изменить параметры хранения и отправки получаемой диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

Специалисты Службы технической поддержки сообщат вам необходимую для выполнения перечисленных действий информацию (описание последовательности шагов, изменяемые параметры, конфигурационные файлы, скрипты, дополнительные возможности командной строки, отладочные модули, специализированные утилиты и так далее), а также состав получаемых в отладочных целях данных. Полученная расширенная диагностическая информация сохраняется на компьютере пользователя. Автоматическая пересылка полученных данных в "Лабораторию Касперского" не выполняется.

Перечисленные выше действия должны выполняться только под руководством специалистов Службы технической поддержки по полученным от них инструкциям. Самостоятельное изменение параметров работы приложения способами, не описанными в настоящем руководстве, может привести к замедлению и сбоям в работе операционной системы, снижению уровня защиты компьютера, а также к нарушению доступности и целостности обрабатываемой информации.

kaspersky

В этом разделе

Выбор тенанта для работы в разделе Endpoint Agents 286

Просмотр таблицы хостов с компонентом Endpoint Agent на отдельном сервере Central Node 286

Просмотр информации о хосте 287

Фильтрация и поиск хостов с компонентом Endpoint Agent по имени хоста 287

Фильтрация и поиск хостов с компонентом Endpoint Agent, изолированных от сети 288

Фильтрация и поиск хостов с компонентом Endpoint Agent по именам серверов PCN и SCN 289

Фильтрация и поиск хостов с компонентом Endpoint Agent по IP-адресу компьютера 289

Фильтрация и поиск хостов с компонентом Endpoint Agent по версии операционной системы на компьютере 290

Фильтрация и поиск хостов с компонентом Endpoint Agent по версии компонента 290

Фильтрация и поиск хостов с компонентом Endpoint Agent по их активности 291

Быстрое создание фильтра хостов с компонентом Endpoint Agent 292

Сброс фильтра хостов с компонентом Endpoint Agent 292

Настройка показателей активности компонента Endpoint Agent 293

Удаление хостов с компонентом Endpoint Agent 293

Автоматическое удаление неактивных хостов 294

Поддерживаемые интерпретаторы и процессы 295

Выбор тенанта для работы в разделе Endpoint Agents

Если вы используете режим распределенного решения и мультитенантности, перед началом работы в разделе **Endpoint Agents** вам нужно выбрать тенанты, данные по которым вас интересуют.

► *Чтобы выбрать тенант для работы в разделе **Endpoint Agents**:*

1. В верхней части меню веб-интерфейса приложения нажмите на стрелку рядом с названием тенанта.
2. В раскрывшемся списке выберите тенант.

Отобразятся данные по выбранному вами тенанту. Если вы хотите изменить тенант, вам нужно повторить действия по выбору тенанта.

Просмотр таблицы хостов с компонентом Endpoint Agent на отдельном сервере Central Node

Таблица хостов с компонентом Endpoint Agent находится в разделе **Endpoint Agents** окна веб-интерфейса приложения.

В таблице могут отображаться следующие данные:

- Количество хостов и показатели активности компонента Endpoint Agent (см. раздел "Настройка показателей активности компонента Endpoint Agent" на стр. 293):
  - **Критическое бездействие** – количество хостов, от которых последние данные были получены очень давно.
  - **Предупреждение** – количество хостов, от которых последние данные были получены давно.
  - **Нормальная активность** – количество хостов, от которых последние данные были получены недавно.
- **Хост** – имя хоста с компонентом Endpoint Agent.
- **Серверы** – имена серверов, к которым подключен хост с компонентом Endpoint Agent.

  Поле отображается, если вы используете режим распределенного решения и мультитенантности.
- **IP** – IP-адрес компьютера, на который установлен компонент Endpoint Agent.
- **ОС** – версия операционной системы, установленной на компьютере с компонентом Endpoint Agent.
- **Версия** – версия приложения, которое используется в роли компонента Endpoint Agent.
- **Активность** – показатель активности компонента Endpoint Agent. Может принимать следующие значения:
  - **Нормальная активность** – хосты, от которых последние данные были получены недавно.
  - **Предупреждение** – хосты, от которых последние данные были получены давно.
  - **Критическое бездействие** – хосты, от которых последние данные были получены очень давно.
- **Последнее подключение** – дата и время последнего подключения компонента Endpoint Agent к серверу Central Node.

По ссылке в столбцах таблицы раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скопировать значение в буфер**.

Просмотр информации о хосте

► *Чтобы просмотреть информацию о хосте с компонентом Endpoint Agent:*

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.
2. Выберите хост, информацию о котором вы хотите просмотреть.

Откроется окно с информацией о хосте.

Окно содержит следующую информацию:

- В разделе **Хост**:
  - **Имя** – имя хоста с компонентом Endpoint Agent.
  - **IP** – IP-адрес хоста, на который установлен компонент Endpoint Agent.
  - **ОС** – версия операционной системы на хосте, на который установлен компонент Endpoint Agent.
  - **Сервер** – имя сервера SCN или PCN. Отображается только в режиме распределенного решения и мультитенантности.
  - **Имя сервера** – имя сервера Central Node.
- В разделе **Endpoint Agent**:
  - **Версия** – версия приложения, которое используется в роли компонента Endpoint Agent.
  - **Активность** – показатель активности компонента Endpoint Agent (см. раздел "Настройка показателей активности компонента Endpoint Agent" на стр. 293). Может иметь следующие значения:
    - **Нормальная активность** – хосты, от которых последние данные были получены недавно.
    - **Предупреждение** – хосты, от которых последние данные были получены давно.
    - **Критическое бездействие** – хосты, от которых последние данные были получены очень давно.
  - **Подключен к серверу** – имя сервера, Central Node, SCN или PCN, к которому подключен хост.
  - **Последнее подключение** – время последнего соединения с сервером Central Node, SCN или PCN.
  - **Лицензия** – состояние лицензионного ключа приложение, которое используется в роли компонента Endpoint Agent.

Фильтрация и поиск хостов с компонентом Endpoint Agent по имени хоста

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по имени хоста:*

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.

Откроется таблица хостов.

2. По ссылке **Хост** откройте окно настройки фильтрации.
3. Если вы хотите, чтобы отобразились только изолированные хосты, установите флажок **Показывать только изолированные Endpoint Agents**.
4. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
5. В поле ввода укажите один или несколько символов имени хоста.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
7. Если вы хотите удалить условие фильтрации, нажмите на кнопку справа от поля.
8. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с компонентом Endpoint Agent, изолированных от сети

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent, изолированные от сети:*

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **Хост** откройте окно настройки фильтрации.
3. Установите флажок **Показывать только изолированные Endpoint Agents**.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с компонентом Endpoint Agent по именам серверов PCN и SCN

Если вы используете режим распределенного решения и мультитенантности, вы можете отфильтровать или найти хосты с компонентом Endpoint Agent по именам серверов PCN и SCN, к которым подключены эти хосты.

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по именам серверов PCN и SCN:*

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **Серверы** откройте окно настройки фильтрации.
3. Установите флажки рядом с теми именами серверов, по которым вы хотите отфильтровать или найти хосты с компонентом Endpoint Agent.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с компонентом Endpoint Agent по IP-адресу компьютера

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по IP-адресу компьютера, на котором установлено приложение:*

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **IP** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов IP-адреса компьютера. Вы можете ввести IP-адрес компьютера или маску подсети в формате IPv4 (например, `192.0.0.1` или `192.0.0.0/16`).
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
6. Если вы хотите удалить условие фильтрации, нажмите на кнопку справа от поля.

7. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с компонентом Endpoint Agent по версии операционной системы на компьютере

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по версии операционной системы, установленной на компьютере:*

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **ОС** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов версии операционной системы.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
6. Если вы хотите удалить условие фильтрации, нажмите на кнопку справа от поля.
7. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с компонентом Endpoint Agent по версии компонента

Вы можете отфильтровать хосты по версии приложения, которое используется в роли компонента Endpoint Agent.

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по версии компонента:*

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **Версия** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов версии приложение, которое используется в роли компонента Endpoint Agent.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
6. Если вы хотите удалить условие фильтрации, нажмите на кнопку справа от поля.
7. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с компонентом Endpoint Agent по их активности

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по их активности:*

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **Активность** откройте окно настройки фильтрации.

   Установите флажки рядом с одним или несколькими показателями активности:
   - **Нормальная активность**, если вы хотите найти хосты, от которых последние данные были получены недавно.
   - **Предупреждение**, если вы хотите найти хосты, от которых последние данные были получены давно.
   - **Критическое бездействие**, если вы хотите найти хосты, от которых последние данные были получены очень давно.
3. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Быстрое создание фильтра хостов с компонентом Endpoint Agent

► *Чтобы быстро создать фильтр хостов с компонентом Endpoint Agent:*

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. Выполните следующие действия по быстрому добавлению условий фильтрации в создаваемый фильтр:

   a. Наведите курсор мыши на ссылку с тем значением столбца таблицы, которое вы хотите добавить в качестве условия фильтрации.

   b. Нажмите на левую клавишу мыши.

      Откроется список действий над значением.

   c. В открывшемся списке выберите одно из следующих действий:

      - **Добавить в фильтр**, если вы хотите включить это значение в условие фильтрации.
      - **Исключить из фильтра**, если вы хотите исключить это значение из условия фильтрации.

3. Если вы хотите добавить несколько условий фильтрации в создаваемый фильтр, выполните действия по быстрому добавлению каждого из условий фильтрации в создаваемый фильтр.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Сброс фильтра хостов с компонентом Endpoint Agent

► *Чтобы сбросить фильтр хостов с компонентом Endpoint Agent по одному или нескольким условиям фильтрации:*

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.
2. Нажмите на кнопку ☒ справа от того заголовка столбца таблицы, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Настройка показателей активности компонента Endpoint Agent

Пользователи с ролью **Локальный администратор** и **Администратор** могут определить, какой период бездействия приложения, которое используется в роли компонента Endpoint Agent, считать нормальной, низкой и очень низкой активностью, а также настроить показатели активности приложения. Пользователям с ролью **Аудитор** доступен только просмотр параметров показателей активности приложения. Пользователи с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** могут просмотреть показатели активности приложения в столбце **Активность** таблицы хостов с компонентом Endpoint Agent в разделе **Endpoint Agents** окна веб-интерфейса приложения.

► *Чтобы настроить показатели активности компонента Endpoint Agent, выполните следующие действия:*

1. Войдите в веб-интерфейс приложения под учетной записью **Локальный администратор**, **Администратор** или **Старший сотрудник службы безопасности**.
2. В окне веб интерфейса приложения выберите раздел **Параметры**, подраздел **Endpoint Agents**.
3. В полях под названием раздела введите количество дней бездействия хостов с компонентом Endpoint Agent, которое вы хотите отображать как **Предупреждение** и **Критическое бездействие**.
4. Нажмите на кнопку **Применить**.

Показатели активности компонента Endpoint Agent будут настроены.

Удаление хостов с компонентом Endpoint Agent

Чтобы удалить один или несколько хостов из таблицы **Endpoint Agents**:

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.
2. Установите флажки рядом с одним или несколькими хостами, которые вы хотите удалить. Вы можете выбрать все хосты, установив флажок в строке с заголовками столбцов.

   В нижней части окна отобразится панель управления.
3. Нажмите на кнопку **Удалить**.
4. В открывшемся окне подтверждения действия нажмите на кнопку **Да**.

Выбранные хосты будут удалены из таблицы **Endpoint Agents**.

При удалении хостов в веб-интерфейсе Kaspersky Anti Targeted Attack Platform происходят следующие изменения:

- Для удаленного хоста нельзя создать задачу (см. раздел "Работа с задачами" на стр. 456), правило запрета (см. раздел "Работа с политиками (правилами запрета)" на стр. 486) и правило сетевой изоляции (см. раздел "Сетевая изоляция хостов с компонентом Endpoint Agent" на стр. 448).
- Если для хоста ранее было создано правило запрета, при удалении этого хоста его имя в окне просмотра правила (см. раздел "Просмотр правила запрета" на стр. 490) (поле **Запрет для**) будет скрыто. Правило продолжит действовать.

  При повторном подключении этого хоста к серверу Central Node имя хоста будет восстановлено в поле **Запрет для** и правило запрета снова будет на него распространяться.
- Если для хоста ранее было создано правило сетевой изоляции, оно продолжит действовать до истечения времени, указанного в правиле.

При повторном подключении этого хоста к серверу Central Node правило снова будет распространяться на этот хост.

- Метаданные объектов, помещенных на карантин на удаленном хосте, удаляются из карантина Kaspersky Anti Targeted Attack Platform (см. раздел "Просмотр таблицы объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent" на стр. 545).

  При повторном подключении этого хоста к серверу Central Node метаданные объектов в карантине Kaspersky Anti Targeted Attack Platform **не** восстанавливаются. Вы можете избежать переполнения карантина на хосте, очистив его с помощью командной строки или через Kaspersky Security Center. Подробнее см. в справке приложения, которое используется в роли компонента Endpoint Agent.

- Если объект был помещен на карантин по задаче **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478) только на одном хосте и этот хост был удален, в окне просмотра задачи (см. раздел "Просмотр информации о задаче" на стр. 459) кнопка **Восстановить все** будет неактивна, так как восстановить файл на удаленном хосте нельзя.

Поиск событий (см. раздел "Поиск угроз по базе событий" на стр. 366) по имени удаленного хоста остается доступным.

Автоматическое удаление неактивных хостов

Вы можете включать и отключать автоматическое удаление неактивных хостов из таблицы **Endpoint Agents**. Неактивными считаются хосты, которые не подключались к серверу Central Node в течение указанного вами времени.

Пользователи с ролью **Аудитор** могут просматривать параметры автоматического удаления неактивных хостов (см. раздел "Просмотр параметров сервера" на стр. 590). Для пользователей с ролями **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** просмотр параметров недоступен.

► *Чтобы включить или отключить автоматическое удаление хостов из таблицы **Endpoint Agents**:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Endpoint Agents**.
2. В блоке параметров **Автоматическое удаление неактивных хостов** выполните следующие действия:
   - Если вы хотите включить функцию, переведите переключатель **Удалять хосты** в положение **Включено**.
   - Если вы хотите отключить функцию, переведите переключатель **Удалять хосты** в положение **Выключено**.
3. Если вы включили функцию, в поле **Удалять после** укажите количество дней, по истечении которых хосты, не подключавшиеся за это время к компоненту Central Node, будут считаться неактивными.

   Значение не может быть меньше 1 и больше 365.

Автоматическое удаление неактивных хостов будет включено или отключено.

Если значение, указанное в поле **Удалять после**, меньше значений, указанных в полях **Предупреждение** и / или **Критическое бездействие** блока параметров **Индикаторы активности** (см. раздел "**Настройка показателей активности компонента Endpoint Agent**" на стр. 293), хосты будут удалены раньше, чем в разделе **Мониторинг** отобразится предупреждение об их неактивности.

При удалении хостов в веб-интерфейсе Kaspersky Anti Targeted Attack Platform происходят следующие изменения:

- Для удаленного хоста нельзя создать задачу (см. раздел "Работа с задачами" на стр. 456), правило запрета (см. раздел "Работа с политиками (правилами запрета)" на стр. 486) и правило сетевой изоляции (см. раздел "Сетевая изоляция хостов с компонентом Endpoint Agent" на стр. 448).
- Если для хоста ранее было создано правило запрета, при удалении этого хоста его имя в окне просмотра правила (см. раздел "Просмотр правила запрета" на стр. 490) (поле **Запрет для**) будет скрыто. Правило продолжит действовать.

  При повторном подключении этого хоста к серверу Central Node имя хоста будет восстановлено в поле **Запрет для** и правило запрета снова будет на него распространяться.
- Если для хоста ранее было создано правило сетевой изоляции, оно продолжит действовать до истечения времени, указанного в правиле.

  При повторном подключении этого хоста к серверу Central Node правило снова будет распространяться на этот хост.
- Метаданные объектов, помещенных на карантин на удаленном хосте, удаляются из карантина Kaspersky Anti Targeted Attack Platform (см. раздел "Просмотр таблицы объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent" на стр. 545).

  При повторном подключении этого хоста к серверу Central Node метаданные объектов в карантине Kaspersky Anti Targeted Attack Platform **не** восстанавливаются. Вы можете избежать переполнения карантина на хосте, очистив его с помощью командной строки или через Kaspersky Security Center. Подробнее см. в справке приложения, которое используется в роли компонента Endpoint Agent.
- Если объект был помещен на карантин по задаче **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478) только на одном хосте и этот хост был удален, в окне просмотра задачи (см. раздел "Просмотр информации о задаче" на стр. 459) кнопка **Восстановить все** будет неактивна, так как восстановить файл на удаленном хосте нельзя.

Поиск событий (см. раздел "Поиск угроз по базе событий" на стр. 366) по имени удаленного хоста остается доступным.

Поддерживаемые интерпретаторы и процессы

Приложение Kaspersky Endpoint Agent контролирует запуск скриптов следующими интерпретаторами:

- cmd.exe;
- reg.exe;
- regedit.exe;
- regedt32.exe;
- cscript.exe;

- wscript.exe;
- mmc.exe;
- msiexec.exe;
- mshta.exe;
- rundll32.exe;
- runlegacycplelevated.exe;
- control.exe;
- explorer.exe;
- regsvr32.exe;
- wwahost.exe;
- powershell.exe;
- java.exe и javaw.exe (только при запуске с опцией –jar);
- InstallUtil.exe;
- msdt.exe;
- python.exe;
- ruby.exe;
- rubyw.exe.

Информация о процессах, контролируемых приложением Kaspersky Endpoint Agent, представлена в таблице ниже.

Таблица 34. Процессы и расширения файлов, которые они открывают

Процесс	Расширения файлов
winword.exe	rtf doc dot docm docx dotx dotm docb

Процесс	Расширения файлов
excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
acrord32.exe	pdf
wordpad.exe	docx pdf
chrome.exe	pdf
MicrosoftEdge.exe	pdf

Настройка интеграции с компонентом Sandbox

Вы можете подключить один компонент Sandbox к нескольким компонентам Central Node.

Предусмотрен следующий порядок настройки соединения компонента Sandbox с компонентом Central Node:

a. **Создание запроса на подключение к компоненту Sandbox (см. раздел "Создание запроса на подключение к серверу с компонентом Sandbox" на стр. 299)**

Вы можете создать запрос в веб-интерфейсе приложения под учетной записью администратора. Если у вас есть несколько компонентов Central Node, установленных на сервере, вам нужно создать запрос для каждого сервера с компонентом Central Node, который вы хотите подключить к компоненту Sandbox. Если компонент Central Node развернут в виде кластера, вы можете создать запрос на подключение с любого сервера кластера.

b. **Обработка запроса на подключение в веб-интерфейсе Sandbox (см. раздел "Обработка запросов на подключение от серверов Central Node в веб-интерфейсе Sandbox" на стр. 217)**

Вы можете принять или отклонить каждый запрос.

После настройки соединения серверу Sandbox требуется 5–10 минут для подготовки к работе. В течение этого времени в окне **Работоспособность системы** (см. раздел "**Просмотр состояния работоспособности модулей и компонентов приложения**" на стр. 251) веб-интерфейса приложения отображается предупреждение *Возникла проблема со стандартной конфигурацией. Переустановите компонент Central Node*. Когда сервер будет готов к работе, предупреждение исчезнет.

В этом разделе

Просмотр таблицы серверов с компонентом Sandbox 298
Создание запроса на подключение к серверу с компонентом Sandbox 299
Включение и отключение соединения с компонентом Sandbox 299
Удаление соединения с компонентом Sandbox 300

Просмотр таблицы серверов с компонентом Sandbox

Пользователи с ролью **Аудитор** могут просматривать таблицу серверов с компонентом Sandbox (см. раздел "Расчеты для компонента Sandbox" на стр. 103).

Таблица серверов с компонентом Sandbox находится в разделе **Серверы Sandbox**, на закладке **Серверы** окна веб-интерфейса приложения.

В поле **Отпечаток сертификата** отображается отпечаток TLS-сертификата сервера Central Node.

Таблица **Список серверов** содержит следующую информацию:

- **IP и имя** – IP-адрес или полное доменное имя сервера с компонентом Sandbox.
- **Отпечаток сертификата** – отпечаток сертификата сервера с компонентом Sandbox.
- **Авторизация** – статус запроса на подключение к компоненту Sandbox.
- **Состояние** – состояние подключения к компоненту Sandbox.

Для пользователей с ролью **Сотрудник службы безопасности** просмотр таблицы серверов с компонентом Sandbox недоступен.

Создание запроса на подключение к серверу с компонентом Sandbox

► *Чтобы создать запрос на подключение к серверу с компонентом Sandbox через веб-интерфейс приложения:*

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sandbox**.
2. В правом верхнем углу окна нажмите на кнопку **Добавить**.

   Откроется окно **Подключение сервера Sandbox**.
3. В поле **IP** укажите IP-адрес сервера с компонентом Sandbox, к которому вы хотите подключиться.
4. Нажмите на кнопку **Получить отпечаток сертификата**.

   В рабочей области отобразится отпечаток сертификата сервера с компонентом Sandbox.
5. Сравните полученный отпечаток сертификата с отпечатком, указанным в веб-интерфейсе Sandbox в разделе **Авторизация KATA** в поле **Отпечаток сертификата**.

   Если отпечатки сертификата совпадают, выполните дальнейшие шаги инструкции.

   > Не рекомендуется подтверждать подключение при несовпадении отпечатков сертификата. Убедитесь в правильности введенных данных.
6. В поле **Имя** укажите имя компонента Sandbox, которое будет отображаться в веб-интерфейсе компонента Central Node.

   Это имя не связано с именем хоста, на котором установлен Sandbox.
7. Если вы хотите сделать соединение с Sandbox активным сразу после подключения, установите флажок **Включить**.
8. Нажмите на кнопку **Добавить**.

Запрос на подключение отобразится в веб-интерфейсе компонента Sandbox.

Включение и отключение соединения с компонентом Sandbox

► *Чтобы сделать соединение с компонентом Sandbox активным или отключить его:*

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sandbox**.

   Отобразится таблица серверов с компонентами Sandbox.
2. В строке с нужным сервером в столбце **Состояние** выполните одно из следующих действий:
   - Если вы хотите сделать соединение с компонентом Sandbox активным, переведите переключатель в положение **Включено**.
   - Если вы хотите отключить соединение с компонентом Sandbox, переведите переключатель в положение **Выключено**.
3. Нажмите на кнопку **Применить**.

Соединение с компонентом Sandbox станет активным или будет отключено.

Удаление соединения с компонентом Sandbox

► *Чтобы удалить соединение с компонентом Sandbox:*

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sandbox**.

   Отобразится таблица компьютеров, на которых установлен компонент Sandbox.
2. Установите флажок в строке с компонентом Sandbox, соединение с которым вы хотите удалить.
3. В правом верхнем углу окна нажмите на кнопку **Удалить**.
4. В окне подтверждения нажмите на кнопку **Да**.

Соединение с компонентом Sandbox будет удалено.

Настройка интеграции с внешними системами

Вы можете настроить интеграцию Kaspersky Anti Targeted Attack Platform с внешними системами для проверки хранящихся в них файлов. Результаты их проверки будут отображаться в таблице обнаружений (см. раздел "Просмотр таблицы обнаружений" на стр. 331).

В роли внешней системы может выступать почтовый сенсор – приложение "Лаборатории Касперского" Kaspersky Secure Mail Gateway или Kaspersky Security для Linux Mail Server. Почтовый сенсор отправляет сообщения электронной почты на обработку в Kaspersky Anti Targeted Attack Platform. По результатам обработки сообщений электронной почты в Kaspersky Anti Targeted Attack Platform почтовый сенсор может блокировать пересылку сообщений.

Предусмотрен следующий порядок интеграции Kaspersky Anti Targeted Attack Platform с внешними системами:

a. **Ввод параметров интеграции и создание запроса на интеграцию на стороне внешней системы**

   Подробнее о вводе параметров интеграции на стороне почтового сенсора см. Справку Kaspersky Secure Mail Gateway https://support.kaspersky.com/KSMG/2.0.1/ru-RU/201622.htm или Справку Kaspersky Security для Linux Mail Server https://support.kaspersky.com/KLMS/10/ru-RU/100512.htm.

   Для интеграции других внешних систем необходимо использовать REST API.

b. **Подтверждение интеграции на стороне Kaspersky Anti Targeted Attack Platform (см. раздел "Обработка запроса от внешней системы" на стр. 301)**

   Внешние системы должны использовать уникальные сертификаты для авторизации на сервере с компонентом Central Node. В этом случае в интерфейсе Kaspersky Anti Targeted Attack Platform будет отображаться один запрос на интеграцию. Для подключения нескольких внешних систем, имеющих один IP-адрес, вам необходимо использовать уникальный сертификат для каждой внешней системы.

   > При использовании одного сертификата вы сможете настроить интеграцию только с одной внешней системой.

c. **Проверка соединения внешней системы с Kaspersky Anti Targeted Attack Platform**

kaspersky

В этом разделе

Просмотр таблицы внешних систем 301

Обработка запроса от внешней системы 301

Удаление внешней системы из списка разрешенных к интеграции 302

Настройка приоритета обработки трафика от почтовых сенсоров 302

Просмотр таблицы внешних систем

Таблица внешних систем находится в разделе **Внешние системы** окна веб-интерфейса приложения. В таблице содержится следующая информация:

- **Sensor** – IP-адрес или доменное имя сервера внешней системы.
- **Тип** – тип внешней системы (почтовый сенсор или другая система).
- **Имя** – название интегрированной внешней системы, не являющейся почтовым сенсором.

  Для почтового сенсора в этом столбце отображается прочерк.
- **ID** – идентификатор внешней системы.
- **Отпечаток сертификата** – отпечаток TLS-сертификата сервера с внешней системой, с помощью которого устанавливается шифрованное соединение с сервером с компонентом Central Node.

  > Отпечаток сертификата сервера с компонентом Central Node отображается в верхней части окна в поле **Отпечаток сертификата**.

- **Состояние** – состояние запроса на интеграцию.

Обработка запроса от внешней системы

► *Чтобы обработать запрос на интеграцию от внешней системы:*

1. В окне веб-интерфейса приложения выберите раздел **Внешние системы**.

   В таблице **Список серверов** отобразятся уже подключенные внешние системы, а также запросы на интеграцию с Kaspersky Anti Targeted Attack Platform от внешних систем.
2. В строке с запросом на интеграцию выполните одно из следующих действий:
   - Если вы хотите настроить интеграцию с внешней системой, нажмите на кнопу **Принять**.
   - Если вы не хотите настраивать интеграцию с внешней системой, нажмите на кнопку **Отклонить**.
3. В окне подтверждения нажмите на кнопку **Да**.

Запрос на интеграцию от внешней системы будет обработан.

Удаление внешней системы из списка разрешенных к интеграции

После того как вы приняли запрос на интеграцию от внешней системы, вы можете удалить ее из списка разрешенных к интеграции. В этом случае соединение между Kaspersky Anti Targeted Attack Platform и внешней системой будет прервано.

► *Чтобы удалить внешнюю систему из списка разрешенных к интеграции:*

1. В окне веб-интерфейса приложения выберите раздел **Внешние системы**.

   В списке **Список серверов** отобразятся уже добавленные внешние системы, а также запросы на интеграцию с Kaspersky Anti Targeted Attack Platform от внешних систем.

2. Нажмите на кнопку **Удалить** в строке с запросом на интеграцию от той внешней системы, которую вы хотите удалить.
3. В окне подтверждения нажмите на кнопку **Да**.

Внешняя система будет удалена из списка разрешенных к интеграции.

Настройка приоритета обработки трафика от почтовых сенсоров

Вы можете включить или отключить максимальный приоритет обработки трафика от почтовых сенсоров.

► *Чтобы включить или отключить максимальный приоритет обработки трафика от почтовых сенсоров:*

1. В окне веб-интерфейса приложения выберите раздел **Внешние системы**.
2. Выполните одно из следующих действий:
   - Включите переключатель рядом с названием параметра **Максимальный приоритет проверки**, если вы хотите включить максимальный приоритет обработки трафика от почтовых сенсоров.
   - Выключите переключатель рядом с названием параметра **Максимальный приоритет проверки**, если вы хотите отключить максимальный приоритет обработки трафика от почтовых сенсоров.

Приоритет обработки трафика от почтовых сенсоров будет настроен.

Настройка интеграции с Kaspersky Managed Detection and Response

Приложение Kaspersky Managed Detection and Response (далее также "MDR") предназначено для обнаружения и предотвращения мошеннических действий в инфраструктуре клиента. MDR обеспечивает непрерывную управляемую защиту и позволяет организациям автоматически выявлять труднообнаружимые угрозы и освобождать сотрудников группы IT-безопасности для решения задач, требующих их участия.

Kaspersky Anti Targeted Attack Platform получает данные и отправляет их в Kaspersky Managed Detection and Response с помощью потока Kaspersky Security Network. Поэтому для настройки интеграции с MDR обязательно участие в KSN.

Интеграция с MDR доступна только при наличии хотя бы одной действующей лицензий KATA или EDR (см. раздел "О ключе" на стр. 158). Если в приложении добавлен один лицензионный ключ (только KATA или только EDR), то статистика отправляется в рамках функциональности, предусмотренной этой лицензией. Если в приложении добавлено оба лицензионных ключа, то статистика отправляется в полном объеме.

Перед настройкой интеграции Kaspersky Anti Targeted Attack Platform с приложением MDR требуется получить архив с конфигурационным файлом на портале MDR.

Настройка интеграции с MDR доступна только Локальному администратору и Администратору веб-интерфейса Kaspersky Anti Targeted Attack Platform.

В этом разделе

Включение интеграции с MDR 303

Отключение интеграции с MDR 304

Замена конфигурационного файла MDR 304

Включение интеграции с MDR

Убедитесь, что в приложении добавлен активный лицензионный ключ (см. раздел "Просмотр текста Лицензионного соглашения в веб-интерфейсе Central Node" на стр. 159) и настроено участие в KSN (см. раздел "Просмотр Положения о KSN и настройка участия в KSN" на стр. 210). В противном случае интеграция с MDR будет недоступна.

► *Чтобы включить интеграцию с MDR:*

1. Войдите в веб-интерфейс приложения под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **KSN/KPSN и MDR**.
3. В блоке параметров **Интеграция MDR** нажмите на кнопку **Загрузить**, чтобы загрузить конфигурационный файл.

   Откроется окно выбора файлов.
4. Выберите архив, полученный при регистрации на портале MDR, и нажмите кнопку **Open**.

   В окне отобразится следующая информация о лицензии MDR:

   - **Серийный номер**.
   - **Дата окончания срока действия**.
   - **Осталось дней**.

Интеграция с MDR будет включена. Параметры интеграции, указанные в конфигурационном файле, будут распространены на все подключенные компоненты Sensor. Приложение MDR начнет использовать статистику о выявленных обнаружениях, отправляемую через поток KSN.

Отключение интеграции с MDR

► *Чтобы отключить интеграцию с MDR:*

1. Войдите в веб-интерфейс приложения под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **KSN/KPSN и MDR**.
3. В блоке переметров **Интеграция MDR** нажмите на кнопку **Удалить файл**.
4. В окне подстверждения нажмите на кнопку **Да**.

Конфигурационный файл будет удален, а интеграция с MDR будет отключена. Приложение продолжит отправлять статистику на серверы KSN, однако эта информация не будет использоваться приложением MDR.

Замена конфигурационного файла MDR

► *Чтобы заменить конфигурационный файл MDR:*

1. Войдите в веб-интерфейс приложения под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **KSN/KPSN и MDR**.
3. В блоке переметров **Интеграция MDR** нажмите на кнопку **Заменить файл**.

   Откроется окно выбора файла.
4. Выберите новый архив с конфигурационным файлом и нажмите на кнопку **Open**.

   В веб-интерфейсе приложения обновится информация о лицензии MDR.

Конфигурационный файл будет заменен. Новые параметры интеграции будут распространены на все подключенные компоненты Sensor.

Настройка интеграции с SIEM-системой

Kaspersky Anti Targeted Attack Platform может публиковать информацию о действиях пользователей в веб-интерфейсе приложения и обнаружениях в *SIEM-систему*, которая уже используется в вашей организации, по протоколу Syslog.

Для передачи данных вы можете использовать TLS-шифрование.

Если вы развернули компоненты Central Node и Sensor в виде кластера (см. раздел "Развертывание компонентов Central Node и Sensor в виде кластера" на стр. 124), вы можете настроить отказоустойчивую интеграцию с внешней системой одним из следующих способов:

- Использовать функцию Round Robin.
- Настроить параметры внешней системы, чтобы при возникновении сетевой ошибки внешняя система переключалась между IP-адресами серверов кластера.

► *Чтобы настроить отказоустойчивую интеграцию с внешней системой с помощью функции Round Robin:*

1. Настройте на сервере DNS функцию Round Robin для доменного имени, соответствующего кластеру Central Node.
2. В параметрах почтового сервера укажите это доменное имя.

Интеграция с почтовым сервером будет настроена по доменному имени. Почтовый сервер обратится к случайному серверу кластера. При отказе этого сервера почтовый сервер будет обращаться к другому работоспособному серверу кластера.

В этом разделе

Включение и отключение записи информации в удаленный журнал 305
Настройка основных параметров интеграции с SIEM-системой 306
Загрузка TLS-сертификата 306
Включение и отключение TLS-шифрования соединения с SIEM-системой 307
Содержание и свойства syslog-сообщений об обнаружениях 307

Включение и отключение записи информации в удаленный журнал

Вы можете настроить запись информации о действиях пользователей в веб-интерфейсе и обнаружениях в удаленный журнал. Файл журнала хранится на сервере, на котором установлена SIEM-система. Для записи в удаленный журнал необходимо настроить параметры интеграции с SIEM-системой (см. раздел "Настройка основных параметров интеграции с SIEM-системой" на стр. 306).

► *Чтобы включить или отключить запись информации о действиях пользователей в веб-интерфейсе и обнаружениях в удаленный журнал:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **SIEM-система**.
2. Если вы хотите включить / отключить запись информации о действиях пользователей в веб-интерфейсе в удаленный журнал, выполните одно из следующих действий:
   - Если вы хотите включить запись информации о действиях пользователей в веб-интерфейсе, установите флажок **Журнал активности**.
   - Если вы хотите отключить запись информации о действиях пользователей в веб-интерфейсе, снимите флажок **Журнал активности**.
3. Если вы хотите включить / отключить запись информации об обнаружениях в удаленный журнал, выполните одно из следующих действий:
   - Если вы хотите включить запись информации об обнаружениях, установите флажок **Обнаружения**.
   - Если вы хотите отключить запись информации об обнаружениях, снимите флажок **Обнаружения**.

   Вы можете установить оба флажка одновременно.

4. Нажмите на кнопку **Применить** в нижней части окна.

Запись информации в удаленный журнал будет включена или отключена.

Пользователи с ролью **Аудитор** могут только просматривать информацию о настройках записи в удаленный журнал.

Настройка основных параметров интеграции с SIEM-системой

► *Чтобы настроить основные параметры интеграции с SIEM-системой:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **SIEM-система**.
2. Установите флажки **Журнал активности** и / или **Обнаружения**.

   Вы можете установить один из флажков или оба флажка одновременно.
3. В поле **Хост/IP** введите IP-адрес или имя хоста сервера вашей SIEM-системы.
4. В поле **Порт** введите номер порта подключения к вашей SIEM-системе.
5. В поле **Протокол** выберите **TCP** или **UDP**.
6. В поле **ID хоста** укажите идентификатор хоста. Хост с этим идентификатором в журнале SIEM-системы будет указан как источник обнаружения.
7. В поле **Периодичность сигнала** введите интервал отправки сообщений в SIEM-систему.
8. Нажмите на кнопку **Применить** в нижней части окна.

Основные параметры интеграции с SIEM-системой будут настроены.

Пользователи с ролью **Аудитор** могут только просматривать информацию о настройках интеграции с SIEM-системой.

Загрузка TLS-сертификата

► *Чтобы загрузить TLS-сертификат для шифрования соединения с SIEM-системой:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **SIEM-система**.
2. В разделе **TLS-шифрование** нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.
3. Выберите файл TLS-сертификата, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

   TLS-сертификат будет добавлен в приложение.
4. Нажмите на кнопку **Применить** в нижней части окна.

Загруженный TLS-сертификат будет использоваться для шифрования соединения с SIEM-системой.

Включение и отключение TLS-шифрования соединения с SIEM-системой

► *Чтобы включить или отключить TLS-шифрование соединения с SIEM-системой:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **SIEM-система**.
2. Установите флажки **Журнал активности** и / или **Обнаружения**.

   Вы можете установить один из флажков или оба флажка одновременно.
3. В разделе **TLS-шифрование** выполните одно из следующих действий:
   - Включите переключатель рядом с названием параметра **TLS-шифрование**, если вы хотите включить TLS-шифрование соединения с SIEM-системой.
   - Выключите переключатель рядом с названием параметра **TLS-шифрование**, если вы хотите отключить TLS-шифрование соединения с SIEM-системой.

   > Переключатель рядом с названием параметра **TLS-шифрование** доступен, только если загружен TLS-сертификат (см. раздел "Загрузка TLS-сертификата" на стр. 306).
4. Нажмите на кнопку **Применить** в нижней части окна.

TLS-шифрование соединения с SIEM-системой будет включено или отключено.

Содержание и свойства syslog-сообщений об обнаружениях

Информация о каждом обнаружении передается в отдельной syslog-категории (syslog facility), не использующейся системой для передачи сообщений от других источников. Информация о каждом обнаружении передается как отдельное syslog-сообщение формата CEF. Если обнаружение выполнено модулем Targeted Attack Analyzer, то информация о нем передается как несколько отдельных syslog-сообщений формата CEF.

Максимальный размер syslog-сообщения об обнаружении по умолчанию составляет 32 Кб. Сообщения, превышающие максимальный размер, обрываются в конце.

В заголовке каждого syslog-сообщения об обнаружении содержится следующая информация:

- Версия формата.

  Номер текущей версии: `0`. Текущее значение поля: `CEF:0`.
- Производитель.

  Текущее значение поля: `AO Kaspersky Lab`.
- Название приложения.

  Текущее значение поля: `Kaspersky Anti Targeted Attack Platform`.
- Версия приложения.

  Текущее значение поля: `6.0.2-11`.
- Тип обнаружения.

См. таблицу ниже.

- Наименование события.

  См. таблицу ниже.

- Важность обнаружения.

  Допустимые значения поля: `Low`, `Medium`, `High` или `0` (для сообщений типа `heartbeat`).

- Дополнительная информация.

Пример:

```
CEF:0|AO Kaspersky Lab| Kaspersky Anti Targeted Attack Platform |6.0.2-
11|url_web| URL from web detected|Low|
```

Тело syslog-сообщения об обнаружении соответствует информации об этом обнаружении, отображающейся в веб-интерфейсе приложения (см. раздел "Начало работы в веб-интерфейсе приложения под учетной записью локального администратора" на стр. 186). Все поля представлены в формате `"<ключ>=<значение>"`. В зависимости от того, в сетевом или почтовом трафике произошло обнаружение, а также от технологии, которая выполнила обнаружение, в теле syslog-сообщения могут передаваться разные ключи. Если значение пустое, то ключ не передается.

Ключи, а также их значения, содержащиеся в сообщении, приведены в таблице ниже.

Таблица 35. Информация об обнаружении в syslog-сообщениях

Тип обнаружения	Наименование и описание обнаружения	Ключ и описание его значения
`file_web`	`File from web detected` В сетевом трафике обнаружен файл.	`dvchost` = <имя сервера с компонентом Central Node>. `eventId` = <ID обнаружения>. `rt` = <дата и время обнаружения>. `dst` = <IP-адрес назначения>. `dpt` = <порт назначения>. `src` = <IP-адрес источника>. `spt` = <порт источника>. `shost` = <имя хоста, на котором обнаружен файл>. `suser` = <имя пользователя>. `fName` = <имя файла внутри составного объекта>. `fsize` = <размер файла внутри составного объекта (в байтах)>. `fileType` = <формат файла внутри составного объекта>. `fileHash` = <MD5-хеш файла внутри составного объекта>. `KasperskyLabKATAcompositeFilePath` = <имя составного объекта>. `KasperskyLabKATAcompositeFileSize` = <общий размер составного объекта (в байтах)>. `KasperskyLabKATAcompositeFileHash` = <MD5-хеш составного объекта>. `KasperskyLabKATAfileSHA256` = <SHA256-хеш составного объекта>. `cs2` = <технология, с помощью которой обнаружен файл>. `cs3Label` = <имя виртуальной машины, на которой обнаружен файл> (только для компонента Sandbox). `cs1` = <список типов обнаруженных объектов по классификации "Лаборатории Касперского">. `cs3` = <версия баз, с помощью которых проверен файл>. `app` = <название протокола прикладного уровня> (HTTP(S) или FTP). `requestMethod` = <метод HTTP-запроса> (только для протокола HTTP(S)).

		requestClientApplication = <User Agent клиентского компьютера> (только для протокола HTTP(S)). request = <URL обнаруженного объекта> (только для протокола HTTP(S)). requestContext = <HTTP-заголовок Referer> (только для протокола HTTP(S)).
file_mail	File from mail detected В почтовом трафике обнаружен файл.	dvchost = <имя сервера с компонентом Central Node>. eventId = <ID обнаружения>. rt = <дата и время обнаружения>. fName = <имя файла внутри составного объекта>. fsize = <размер файла внутри составного объекта (в байтах)>. fileType = <формат файла внутри составного объекта >. fileHash = <MD5-хеш файла внутри составного объекта >. KasperskyLabKATAcompositeFilePath = <имя составного объекта>. KasperskyLabKATAcompositeFileSize = <общий размер составного объекта (в байтах)>. KasperskyLabKATAcompositeFileHash = <MD5-хеш составного объекта>. KasperskyLabKATAfileSHA256 = <SHA256-хеш составного объекта>. KasperskyLabKATAmailEnvelopeFrom = <адрес электронной почты отправителя> (из заголовка Received). KasperskyLabKATAmailFor = <адрес электронной почты получателя> (из заголовка Received). KasperskyLabKATAmailRecievedFromIp = <IP-адрес первого в цепочке отправки сообщения сервера> (из заголовка Received). cs2 = <технология, с помощью которой обнаружен файл>. cs3Label = <имя виртуальной машины, на которой обнаружен файл> (только для компонента Sandbox). cs1 = <список типов обнаруженных объектов по классификации "Лаборатории Касперского">. cs3 = <версия баз, с помощью которых проверен файл>. externalId = <ID сообщения электронной почты>. suser = <адрес электронной почты отправителя>. duser = <адреса электронной почты получателей>. msg = <тема сообщения>.

ids	IDS event detected Обнаружение выполнено модулем Intrusion Detection System.	dvchost = <имя сервера с компонентом Central Node>. eventId = <ID обнаружения>. requestMethod = <метод HTTP-запроса> (только для протокола HTTP(S)). requestClientApplication = <User Agent клиентского компьютера> (только для протокола HTTP(S)). rt = <дата и время обнаружения>. dst = <IP-адрес назначения>. dpt = <порт назначения>. src = <IP-адрес источника>. spt = <порт источника>. proto = <название протокола сетевого уровня> (TCP или UDP). cs1 = <тип обнаруженного объекта по классификации "Лаборатории Касперского">. cs2Label = <название правила IDS>. cs2 = <номер правила IDS>. cs3 = <версия баз модуля Intrusion Detection System>. requestMethod = <метод HTTP-запроса> (только для протокола HTTP). requestClientApplication = <User Agent клиентского компьютера> (только для протокола HTTP). request = <URL обнаруженного объекта>.
url_web	URL from web detected Обнаружение выполнено технологией URL Reputation или Sandbox в сетевом трафике.	dvchost = <имя сервера с компонентом Central Node>. eventId = <ID обнаружения>. rt = <дата и время обнаружения>. dst = <IP-адрес назначения>. dpt = <порт назначения>. src = <IP-адрес источника>. spt = <порт источника>. shost = <имя хоста, на котором обнаружен файл>. suser = <имя пользователя>. cs1 = <список категорий, к которым принадлежит URL-адрес обнаруженного объекта>. requestMethod = <метод HTTP-запроса>. requestClientApplication = <User Agent клиентского компьютера>. request = <URL-адрес обнаруженного объекта>. requestContext = <HTTP-заголовок Referer>. reason = <код HTTP-ответа>.
url_mail	URL from mail detected Обнаружение выполнено технологией URL Reputation или Sandbox в почтовом трафике.	dvchost = <имя сервера с компонентом Central Node>. eventId = <ID обнаружения>. rt = <дата и время обнаружения>. externalId = <ID сообщения электронной почты>. suser = <адрес электронной почты отправителя>. duser = <адреса электронной почты получателей>. KasperskyLabKATAmailEnvelopeFrom = <адрес электронной почты отправителя> (из заголовка Received). KasperskyLabKATAmailFor = <адрес получателя> (из заголовка Received). KasperskyLabKATAmailRecievedFromIp = <IP-адрес первого в цепочке отправки сообщения сервера> (из заголовка Received).

		msg = <тема сообщения>. request = <URL-адрес обнаруженного объекта>. cs2 = <технология, с помощью которой выполнено обнаружение> (Sandbox или URL Reputation). cs3Label = <имя виртуальной машины, на которой обнаружен файл> (только для Sandbox). cs1 = <список типов обнаруженных объектов по классификации "Лаборатории Касперского"> (для Sandbox) или <список категорий> (для URL Reputation). cs3 = <версия баз, с помощью которых проверен файл> (только для Sandbox).
dns	DNS request detected Обнаружение выполнено технологией URL Reputation в DNS-трафике.	dvchost = <имя сервера с компонентом Central Node>. eventId = <ID обнаружения>. rt = <дата и время обнаружения>. dst = <IP-адрес назначения>. dpt = <порт назначения>. src = <IP-адрес источника>. spt = <порт источника>. shost = <имя хоста, на котором обнаружен файл>. suser = <имя пользователя>. cs2 = <список URL-категорий, к которым принадлежат доменные имена>. requestMethod = <тип DNS-сообщения> (request или response). flexString1 = <тип записи из DNS-запроса>. dhost = <имя хоста из DNS-запроса>. cs1 = <список доменных имен из DNS-ответа>.
file_endpoint	File from endpoint detected Обнаружение выполнено компонентом Endpoint Agent на хосте пользователя и содержит файл.	dvchost = <имя сервера с компонентом Central Node>. eventId = <ID обнаружения>. rt = <дата и время обнаружения>. src = <IP-адрес источника>. shost = <имя хоста, на котором обнаружен файл>. fName = <имя файла внутри составного объекта>. fsize = <размер файла внутри составного объекта (в байтах)>. fileType = <формат файла внутри составного объекта >. fileHash = <MD5-хеш файла внутри составного объекта >. KasperskyLabKATAcompositeFilePath = <имя составного объекта>. KasperskyLabKATAcompositeFileSize = <общий размер составного объекта (в байтах)>. KasperskyLabKATAcompositeFileHash = <MD5-хеш составного объекта>. KasperskyLabKATAfileSHA256 = <SHA256-хеш составного объекта>. cs2 = <технология, с помощью которой обнаружен файл>. cs3Label = <имя виртуальной машины, на которой обнаружен файл> (только для компонента Sandbox). cs1 = <список типов обнаруженных объектов по классификации "Лаборатории Касперского">. cs3 = <версия баз, с помощью которых проверен файл>. app = <название протокола прикладного уровня> (HTTP(S) или FTP). FilePath = <путь к файлу на компьютере с компонентом Endpoint Sensors>.

iocScanning	IOC has tripped on endpoint Обнаружение выполнено в результате IOC-проверки хостов с компонентом Endpoint Agent для Windows. Этот тип обнаружений доступен, если вы используете функциональность KEDR.	dvchost = <имя сервера с компонентом Central Node>. eventId = <ID обнаружения>. rt = <дата и время обнаружения>. src = <IP-адрес источника>. shost = <имя хоста, на котором обнаружен файл>. cs1 = <имя IOC-файла, по которому выполнено обнаружение>.
taaScanning	TAA has tripped on events database Обнаружение выполнено в результате IOA-анализа событий. Этот тип обнаружений доступен, если вы используете функциональность KEDR.	dvchost = <имя сервера с компонентом Central Node>. eventId = <ID обнаружения>. rt = <дата и время обнаружения>. shost = <имя хоста, на котором выполнено обнаружение>. cs1 = <имя IOA-правила, по которому выполнено обнаружение>.
yaraScanningEP	YARA has tripped on endpoint Обнаружение выполнено в результате YARA-проверки хостов с компонентом Endpoint Agent для Windows. Этот тип обнаружений доступен, если вы используете функциональность KEDR.	dvchost = <имя сервера с компонентом Central Node>. eventId = <ID обнаружения>. rt = <дата и время обнаружения>. src = <IP-адрес источника>. shost = <имя хоста, на котором выполнено обнаружение>. cs1 = <имя YARA-правила, по которому выполнено обнаружение>.
heartbeat	Периодическое сообщение, содержащее статус компонентов.	dvchost = <имя сервера с компонентом Central Node>. rt = <дата и время события>. KasperskyLabKATAcomponentName = <название компонента>. KasperskyLabKATAcomponentState = <статус компонента> (0 – OK, >0 – Ошибка).

Управление журналом активности

Некоторые действия пользователей в веб-интерфейсе приложения могут привести к ошибкам в работе Kaspersky Anti Targeted Attack Platform. Вы можете включить запись информации о действиях пользователей в веб-интерфейсе приложения в журнал и при необходимости просмотреть эту информацию, скачав файлы журнала.

В этом разделе

Включение и отключение записи информации в журнал активности 313

Скачивание файлов журнала активности 313

Содержание и свойства CEF-сообщений о действиях пользователей в веб-интерфейсе 314

Включение и отключение записи информации в журнал активности

► *Чтобы включить или отключить запись информации о действиях пользователей в веб-интерфейсе Kaspersky Anti Targeted Attack Platform в журнал активности:*

1. В окне веб-интерфейса приложения перейдите в раздел **Отчеты**, подраздел **Журнал активности**.
2. Выполните одно из следующих действий:
   - Установите переключатель **Журнал активности** в положение **Включено**, если хотите включить запись информации о действиях пользователей в веб-интерфейсе приложения в журнал активности.
   - Установите переключатель **Журнал активности** в положение **Выключено**, если хотите отключить запись информации о действиях пользователей в веб-интерфейсе приложения в журнал активности.

     По умолчанию функция включена.

Запись информации производится в течение 30 дней в файл журнала user_actions.log. По истечении 30 дней файл user_actions.log будет сохранен на сервере с компонентом Central Node в директории /var/log/kaspersky/apt-base/ с названием user_actions.log<month>. Для записи информации за текущий месяц будет создан новый файл с названием user_actions.log. Каждый файл хранится 90 дней, после чего удаляется.

Для того, чтобы просмотреть файлы журнала активности, вам нужно предварительно скачать (см. раздел "Скачивание файлов журнала активности" на стр. 313) их.

Вы можете настроить запись информации о действиях пользователей в веб-интерфейсе приложения в удаленный журнал (см. раздел "Включение и отключение записи информации в удаленный журнал" на стр. 305). Удаленный журнал хранится на сервере, на котором установлена SIEM-система. Для записи в удаленный журнал должны быть настроены параметры интеграции с SIEM-системой (см. раздел "Настройка основных параметров интеграции с SIEM-системой" на стр. 306).

В режиме распределенного решения (см. раздел "Распределенное решение и мультитенантность" на стр. 75) информация о действиях пользователей в веб-интерфейсе записывается в журнал того сервера, в веб-интерфейсе которого работают пользователи. Информация о действиях пользователей сервера PCN, влияющих на параметры серверов SCN, записывается в журнал сервера PCN. Пользователи с ролью **Аудитор** могут только просматривать настройки записи информации в журнал активности.

Скачивание файлов журнала активности

► *Чтобы скачать файл журнала активности:*

1. В окне веб-интерфейса приложения перейдите в раздел **Отчеты**, подраздел **Журнал активности**.
2. Нажмите на кнопку **Скачать**.

Файлы журнала будут сохранены на ваш локальный компьютер в папку загрузки браузера. Файлы загружаются в формате ZIP-архива.

В режиме распределенного решения вы можете скачать файлы журнала активности только для того сервера, в веб-интерфейсе которого работаете.

Содержание и свойства CEF-сообщений о действиях пользователей в веб-интерфейсе

В заголовке каждого сообщения содержится следующая информация:

- Версия формата.

  Номер текущей версии: `0`. Текущее значение поля: `CEF:0`.

- Производитель.

  Текущее значение поля: `AO Kaspersky Lab`.

- Название приложения.

  Текущее значение поля: `Kaspersky Anti Targeted Attack Platform`.

- Версия приложения.

  Текущее значение поля: `3.7.0-2067`.

- Тип события.

  См. таблицу ниже.

- Наименование события.

  См. таблицу ниже.

- Важность события.

  Текущее значение поля: `Low`.

Пример:

```
CEF:0|AO Kaspersky Lab|Kaspersky Anti Targeted Attack Platform|3.7.0-
2067|tasks|Managing tasks|Low|
```

Все поля тела CEF-сообщения представлены в формате `"<ключ>=<значение>"`. Ключи, а также их значения, содержащиеся в сообщении, приведены в таблице ниже.

Таблица 36. Информация о событии в CEF-сообщениях

Тип события	Наименование и описание события	Ключ и описание его значения
sensors	Managing the Sensor component Подключение компонента Sensor к серверу Central Node, изменение настроек компонента.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>.
sb	Configuring integration with the Sandbox component Подключение компонента Sandbox к серверу Central Node.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>.
ex_integration	Configuring integration with external systems Настройки интеграции с внешними системами.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>.
ksn_kpsn_mdr	Participation in KSN, KPSN and MDR Настройка участия в Kaspersky Security Network, включение / отключение использования Kaspersky Private Security Network и настройка интеграции с Kaspersky Managed Detection and Response.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>.
yara	Managing YARA rules Операции с правилами YARA.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>. • device external ID = <идентификатор хоста в режиме распределенного решения>. • cs1label = <имя загружаемого файла>
ioc	Managing indicator of compromise Операции с правилами IOC.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>. • deviceExternalID = <идентификатор хоста в режиме распределенного решения>.
ids	Managing IDS rules Операции с правилами IDS.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>.

		• deviceExternalID = <идентификатор хоста в режиме распределенного решения>.
taa	Managing TAA rules Операции с правилами TAA (IOA).	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>.
sb rules	Managing Sandbox rules Операции с правилами Sandbox.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>.
prevention	Managing prevention rules Операции с правилами запрета.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>.
exclusions	Managing scan exclusions Операции с правилами исключений из проверки.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>.
endpoint_agents	Managing Endpoint Agent hosts Операции с хостами, на которых установлен компонент Endpoint Agent.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>.
tasks	Managing tasks Операции с задачами.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>.
network_isolation	Network isolation of Endpoint Agent hosts Сетевая изоляция хостов Endpoint Agent.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>.
settings	Settings Изменение параметров сервера Central Node.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>.

		• cs1 = <тип события>.
settings	Settings Набор ОС виртуальных машин изменен на <версия набора ОС>.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>. • cs1label = <имя сервера, на котором обновились настройки>.
mt	Managing CN, PCN and SCN servers Изменение параметров сервера Primary Central Node и Secondary Central Node в режиме распределенного решения и мультитенантности.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>.
user_account	Managing user accounts Действия с учетными записями пользователей.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>.
notifications	Sending notifications Настройка отправки уведомлений на электронный адрес почты.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>.
license	License Управление лицензионным ключом.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>.

Если одна операция проводится с более чем 30 объектами одновременно, в журнал записывается одно сообщение об этой операции. В сообщении указывается информация об операции и количество объектов, с которыми она была проведена.

Обновление баз приложения

Базы приложения (далее также "базы") представляют собой файлы с записями, на основании которых компоненты и модули приложения обнаруживают события, происходящие в IT-инфраструктуре вашей организации.

Вирусные аналитики "Лаборатории Касперского" ежедневно обнаруживают множество новых угроз, в том числе угроз "нулевого дня", создают для них идентифицирующие записи и включают их в пакеты обновлений баз (далее также "пакеты обновлений"). *Пакет обновлений* представляет собой один или несколько файлов с записями, идентифицирующими угрозы, которые были выявлены за время, истекшее с момента выпуска предыдущего пакета обновлений. Рекомендуется регулярно получать пакеты обновлений. При установке приложения дата выпуска баз соответствует дате выпуска приложения, поэтому базы нужно обновить сразу после установки приложения.

Приложение автоматически проверяет наличие новых пакетов обновлений на серверах обновлений "Лаборатории Касперского" один раз в 30 минут. По умолчанию, если базы компонентов приложения по каким-либо причинам не обновляются в течение 24 часов, Kaspersky Anti Targeted Attack Platform отображает эту информацию в разделе **Мониторинг** окна веб-интерфейса приложения.

Если версия Kaspersky Anti Targeted Attack Platform не поддерживается, базы не обновляются. Вы можете посмотреть, какие версии приложения находятся на поддержке, на странице жизненного цикла приложений (https://support.kaspersky.com/corporate/lifecycle).

В этом разделе

Выбор источника обновления баз 318

Запуск обновления баз вручную 319

Выбор источника обновления баз

Вы можете выбрать источник, из которого приложение будет загружать обновления баз. Источником обновлений может быть сервер "Лаборатории Касперского", а также сетевая или локальная папка одного из компьютеров вашей организации.

► *Чтобы выбрать источник обновления баз приложения:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке **Обновление баз** в раскрывающемся списке **Источник обновлений** выберите одно из следующих значений:
   - **Сервер обновлений "Лаборатории Касперского"**.

     Приложение будет подключаться к серверу обновлений "Лаборатории Касперского" по протоколу HTTP и загружать актуальные базы.
   - **Сервер обновлений "Лаборатории Касперского" (безопасное подключение)**.

     Приложение будет подключаться к серверу обновлений "Лаборатории Касперского" по протоколу HTTPS и загружать актуальные базы. Рекомендуется выполнять обновления баз по протоколу HTTPS.
   - **Другой сервер**.

     Приложение будет подключаться к вашему FTP- или HTTP-серверу или к папке с базами программы на вашем компьютере и загружать актуальные базы.

3. Если вы выбрали **Другой сервер**, в поле под названием этого параметра укажите URL-адрес пакета обновлений на вашем HTTP-сервере или полный путь к папке с пакетом обновлений баз приложения на вашем компьютере.
4. Нажмите на кнопку **Применить**.

Источник обновления баз приложения будет выбран.

Запуск обновления баз вручную

► *Чтобы запустить обновление баз приложения вручную:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке **Обновление баз** нажмите на кнопку **Запустить**.
3. Нажмите на кнопку **Применить**.

Обновление баз приложения будет запущено. Справа от кнопки отобразится сообщение о результате выполнения обновления.

Создание списка паролей для архивов

Приложение не проверяет архивы, защищенные паролем. Вы можете создать список наиболее часто встречающихся паролей для архивов, которые используются при обмене файлами в вашей организации. В этом случае при проверке архива приложение будет проверять пароли из списка. Если какой-либо из паролей подойдет, архив будет разблокирован и проверен.

Список паролей, заданный в параметрах приложения, также передается на сервер с компонентом Sandbox.

► *Чтобы создать список паролей для архивов:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Пароли к архивам**.
2. В поле **Пароли к архивам** введите пароли, которые приложение будет использовать для архивов, защищенных паролем.

   Вводите каждый пароль с новой строки. Вы можете ввести до 50 паролей.
3. Нажмите на кнопку **Применить**.

Список паролей для архивов будет создан. При проверке файлов формата PDF, а также файлов приложений Microsoft Word, Excel®, PowerPoint®, защищенных паролем, приложение будет подбирать пароли из заданного списка.

Пользователи с ролью **Аудитор** могут просматривать список паролей для архивов без возможности редактирования.

Сотруднику службы безопасности: работа в веб-интерфейсе приложения

Этот раздел адресован специалистам, в обязанности которых входит обеспечение безопасности данных организации. Он содержит информацию и инструкции по настройке средств для защиты IT-инфраструктуры организации и своевременного обнаружения угроз.

Приложение допускает совместную работу нескольких специалистов по информационной безопасности.

kaspersky

В этом разделе

Интерфейс Kaspersky Anti Targeted Attack Platform 322
Выбор тенанта для работы в веб-интерфейсе приложения 323
Мониторинг работы приложения 323
Просмотр таблицы обнаружений 331
Настройка отображения таблицы обнаружений 334
Фильтрация, сортировка и поиск обнаружений 334
Рекомендации по обработке обнаружений 343
Просмотр обнаружений 350
Действия пользователей над обнаружениями 362
Поиск угроз по базе событий 366
Информация о событиях 378
Работа с информацией о хостах с компонентом Endpoint Agent 433
Сетевая изоляция хостов с компонентом Endpoint Agent 448
Автоматическая отправка файлов с хостов с компонентом Endpoint Agent на проверку в Sandbox по правилам TAA (IOA) "Лаборатории Касперского" 451
Выбор операционных систем для проверки объектов в Sandbox 454
Работа с задачами 456
Работа с политиками (правилами запрета) 486
Работа с пользовательскими правилами 497
Работа с объектами в Хранилище и на карантине 531
Работа с отчетами 552
Работа с правилами присвоения обнаружениям статуса VIP 563
Работа со списком исключений из проверки 568
Работа с IDS-исключениями 573
Работа с TAA-исключениями 577
Работа с ICAP-исключениями 584
Создание списка паролей для архивов 589
Просмотр параметров сервера 590
Просмотр таблицы серверов с компонентом Sandbox 591
Просмотр параметров набора операционных систем для проверки объектов в Sandbox 592
Просмотр таблицы серверов с компонентом Sensor 592
Работа с сырым сетевым трафиком 593
Просмотр таблицы внешних систем 595

Интерфейс Kaspersky Anti Targeted Attack Platform

Работа с приложением осуществляется через веб-интерфейс. Разделы веб-интерфейса приложения различаются в зависимости от роли пользователя – **Администратор** (см. раздел "**Администратору: работа в веб-интерфейсе приложения**" на стр. 243) или **Старший сотрудник службы безопасности** / **Сотрудник службы безопасности** / **Аудитор**.

Окно веб-интерфейса приложения содержит следующие элементы:

- разделы в левой части и в нижней части окна веб-интерфейса приложения;
- закладки в верхней части окна веб-интерфейса приложения для некоторых разделов приложения;
- рабочую область в нижней части окна веб-интерфейса приложения.

Разделы окна веб-интерфейса приложения

Веб-интерфейс приложения для пользователей с ролями **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности** и **Аудитор** содержит следующие разделы:

- **Мониторинг**. Содержит данные мониторинга Kaspersky Anti Targeted Attack Platform.
- **Обнаружения**. Содержит информацию об обнаружениях в сети тенанта, к которому у вас есть доступ.
- **Поиск угроз**. Содержит информацию о событиях, найденных на хостах тенанта, к которому у вас есть доступ.
- **Задачи**. Содержит информацию о задачах, с помощью которых вы можете работать с файлами и приложениями на хостах.
- **Политики**. Содержит информацию о политиках, с помощью которых вы можете управлять запретами запуска файлов на выбранных хостах.
- **Пользовательские правила**: **TAA**, **IDS**, **IOC** и **YARA**. Содержит информацию для работы с пользовательскими правилами.
- **Хранилище**: **Файлы** и **Карантин**. Содержит информацию для работы с объектами на карантине и в Хранилище.
- **Endpoint Agents**. Содержит информацию о компьютерах с компонентом Endpoint Agent и их параметрах.
- **Отчеты**: **Созданные отчеты** и **Шаблоны**. Содержит конструктор отчетов и список созданных отчетов об обнаружениях.
- **Параметры**: **Расписание IOC-проверки**, **Endpoint Agents**, **Репутационная база KPSN**, **Правила уведомлений**, **Статус VIP**, **Исключения**, **Пароли к архивам** и **Лицензия**. Содержит информацию о расписании IOC-проверки, параметрах публикации объектов в KPSN, присвоении обнаружениям статуса VIP на основе информации, содержащейся в обнаружениях, списке разрешенных объектов и исключениях из проверки правил IDS и TAA (IOA), паролях к архивам и добавленных ключах.

Рабочая область окна веб-интерфейса приложения

В рабочей области отображается информация, просмотр которой вы выбираете в разделах и на закладках окна веб-интерфейса приложения, а также элементы управления, с помощью которых вы можете настроить отображение информации.

kaspersky

Выбор тенанта для работы в веб-интерфейсе приложения

Если вы используете режим распределенного решения и мультитенантности под учетной записью **Старший сотрудник службы безопасности** или **Сотрудник службы безопасности**, перед началом работы с веб-интерфейсом вам нужно выбрать тенант, в рамках которого вы хотите работать с веб-интерфейсом приложения.

► *Чтобы выбрать тенант для работы в веб-интерфейсе приложения:*

1. В верхней части меню веб-интерфейса приложения нажмите на стрелку рядом с названием тенанта.
2. В раскрывающемся меню **Выберите тенант** выберите тенант из списка.

   Вы также можете ввести несколько символов названия тенанта в строку поиска и выбрать его из списка результатов поиска.

Все действия в веб-интерфейсе приложения будут связаны с выбранным тенантом. Если вы хотите изменить тенант, вам нужно повторить действия по выбору тенанта.

Выбор тенанта для работы в веб-интерфейсе недоступен для пользователей с ролью **Аудитор**.

Мониторинг работы приложения

Вы можете осуществлять мониторинг работы приложения с помощью виджетов в разделе **Мониторинг** окна веб-интерфейса приложения. Вы можете добавлять, удалять, перемещать виджеты, настраивать масштаб отображения виджетов и выбирать период отображения данных.

В этом разделе

О виджетах и схемах расположения виджетов 324

Добавление виджета на текущую схему расположения виджетов 325

Перемещение виджета на текущей схеме расположения виджетов 325

Удаление виджета с текущей схемы расположения виджетов 326

Сохранение схемы расположения виджетов в PDF 326

Настройка периода отображения данных на виджетах 326

Настройка масштаба отображения виджетов 327

Основные принципы работы с виджетами типа "Обнаружения" 328

Просмотр состояния работоспособности модулей и компонентов приложения 329

О виджетах и схемах расположения виджетов

С помощью виджетов вы можете осуществлять мониторинг работы приложения.

Схема расположения виджетов – вид рабочей области окна веб-интерфейса приложения в разделе **Мониторинг**. Вы можете добавлять, удалять и перемещать виджеты на схеме расположения виджетов, а также настраивать масштаб виджетов.

Если вы используете режим распределенного решения и мультитенантности, в разделе отображаются данные по выбранному вами тенанту.

По умолчанию в разделе отображается информация только об обнаружениях, не обработанных пользователями. Если вы хотите, чтобы информация об обработанных обнаружениях тоже отображалась, включите переключатель **Обработано** в правом верхнем углу окна.

В разделе **Мониторинг** отображаются следующие виджеты:

- Обнаружения:
  - **Обнаружения по состоянию**. Отображение состояния обнаружения в зависимости от того, какой пользователь Kaspersky Anti Targeted Attack Platform его обрабатывает и от того, обработано это обнаружение или нет.
  - **Обнаружения по технологии**. Отображение названий модулей или компонентов приложения, сделавших обнаружение.
  - **Обнаружения по вектору атаки**. Отображение обнаруженных объектов по направлению атаки.
  - **VIP-обнаружения по степени важности**. Отображение важности обнаружений со статусом VIP в соответствии с тем, какое влияние они могут оказать на безопасность компьютера или локальной сети организации, по опыту "Лаборатории Касперского".
  - **Обнаружения по степени важности**. Отображение важности обнаружений для пользователя Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние они могут оказать на безопасность компьютеров или локальной сети организации, по опыту "Лаборатории Касперского".

  В левой части каждого виджета перечислены векторы атаки, степени важности обнаружений, состояния обнаружений и технологии, выполнившие обнаружения. В правой части каждого виджета отображается количество раз, которое приложение обнаружило их за выбранный период отображения данных на виджетах (см. раздел "Настройка периода отображения данных на виджетах" на стр. 247).

  По ссылке с названием вектора атаки, степенью важности обнаружений, состоянием обнаружений и технологией, выполнившей обнаружения, можно перейти в раздел **Обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331) веб-интерфейса приложения и просмотреть связанные обнаружения. При этом обнаружения будут отфильтрованы (см. раздел "Фильтрация, сортировка и поиск обнаружений" на стр. 334) по выбранному элементу.
- Топ 10:
  - **Домены**. 10 доменов, наиболее часто встречающихся в обнаружениях.
  - **IP-адреса**. 10 IP-адресов, наиболее часто встречающихся в обнаружениях.
  - **Адреса отправителей**. 10 отправителей сообщений электронной почты, наиболее часто встречающихся в обнаружениях.
  - **Адреса получателей**. 10 получателей сообщений электронной почты, наиболее часто встречающихся в обнаружениях.

- **Хосты ТАА**. 10 хостов, наиболее часто встречающихся в событиях и обнаружениях, выполненных технологией Targeted Attack Analyzer (TAA).
- **Правила ТАА**. 10 правил TAA (IOA), наиболее часто встречающихся в событиях и обнаружениях, выполненных технологией Targeted Attack Analyzer (TAA).
- **Отправлено в Sandbox по правилам ТАА**. 10 правил TAA (IOA), по которым Kaspersky Anti Targeted Attack Platform наиболее часто отправляет файлы на проверку компоненту Sandbox.

В левой части каждого виджета перечислены домены, адреса получателей, IP-адреса и адреса отправителей сообщений, имена хостов и названия правил TAA (IOA). В правой части каждого виджета отображается количество раз, которое приложение обнаружило их за выбранный период отображения данных на виджетах.

По ссылке с именем каждого домена, адреса получателя, IP-адреса и адреса отправителя сообщений , именем хоста и названию правила TAA (IOA) можно перейти в раздел **Обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331) веб-интерфейса приложения и просмотреть связанные обнаружения. При этом обнаружения будут отфильтрованы (см. раздел "Фильтрация, сортировка и поиск обнаружений" на стр. 334) по выбранному элементу.

Добавление виджета на текущую схему расположения виджетов

► *Чтобы добавить виджет на текущую схему расположения виджетов:*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку ☰.
3. В раскрывающемся списке выберите **Изменить**.
4. Нажмите на кнопку **Виджеты**.
5. В появившемся окне **Настроить виджеты** включите переключатель рядом с виджетом, который вы хотите добавить.

Виджет будет добавлен на текущую схему расположения виджетов.

Перемещение виджета на текущей схеме расположения виджетов

► *Чтобы переместить виджет на текущей схеме расположения виджетов:*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку ☰.
3. В раскрывающемся списке выберите **Изменить**.
4. Выберите виджет, который вы хотите переместить на схеме расположения виджетов.
5. Нажав и удерживая левую клавишу мыши на верхней части виджета, перетащите виджет на другое место схемы расположения виджетов.
6. Нажмите на кнопку **Сохранить**.

Текущая схема расположения виджетов будет сохранена.

Удаление виджета с текущей схемы расположения виджетов

► *Чтобы удалить виджет с текущей схемы расположения виджетов:*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку ☰.
3. В раскрывающемся списке выберите **Изменить**.
4. Нажмите на значок ✕ в правом верхнем углу виджета, который вы хотите удалить со схемы расположения виджетов.

   Виджет будет удален из рабочей области окна веб-интерфейса приложения.
5. Нажмите на кнопку **Сохранить**.

Виджет будет удален с текущей схемы расположения виджетов.

Сохранение схемы расположения виджетов в PDF

► *Чтобы сохранить схему расположения виджетов в PDF:*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку ☰.
3. В раскрывающемся списке выберите **Сохранить как PDF**.

   Откроется окно **Сохранение в PDF**.
4. В нижней части окна в раскрывающемся списке **Ориентация** выберите ориентацию страницы.
5. Нажмите на кнопку **Скачать**.

   Схема расположения виджетов в формате PDF будет сохранена на жесткий диск вашего компьютера в папку загрузки браузера.
6. Нажмите на кнопку **Закрыть**.

Настройка периода отображения данных на виджетах

Вы можете настроить отображение данных на виджетах за следующие периоды:

- **День**.
- **Неделя**.
- **Месяц**.

► *Чтобы настроить отображение данных на виджетах за сутки (с 00:00 до 23:59):*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса приложения в раскрывающемся списке периодов отображения данных выберите **День**.

3. В календаре справа от названия периода **День** выберите дату, за которую вы хотите получить данные на виджете.

На всех виджетах страницы **Мониторинг** отобразятся данные за выбранный вами период.

► *Чтобы настроить отображение данных на виджетах за неделю (с понедельника по воскресенье):*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса приложения в раскрывающемся списке периодов отображения данных выберите **Неделя**.
3. В календаре справа от названия периода **Неделя** выберите неделю, за которую вы хотите получить данные на виджете.

На всех виджетах страницы **Мониторинг** отобразятся данные за выбранный вами период.

► *Чтобы настроить отображение данных на виджетах за месяц (календарный месяц):*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса приложения в раскрывающемся списке периодов отображения данных выберите **Месяц**.
3. В календаре справа от названия периода **Месяц** выберите месяц, за который вы хотите получить данные на виджете.

На всех виджетах страницы **Мониторинг** отобразятся данные за выбранный вами период.

Настройка масштаба отображения виджетов

Вы можете настроить масштаб отображения виджетов типа "Обнаружения". В правом верхнем углу виджетов, масштаб отображения которых можно настроить, есть значок .

► *Чтобы настроить масштаб отображения виджетов:*

1. В окне веб-интерфейса приложения выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку .
3. В раскрывающемся списке выберите **Изменить**.
4. Нажмите на значок в правом верхнем углу виджета.
5. В раскрывшемся списке выберите один из следующих размеров отображения виджета:
   - **1x1 размер**.
   - **2x1 размер**.
   - **3x1 размер**.

   Масштаб отображения выбранного виджета изменится.
6. Повторите действия для всех виджетов, масштаб отображения которых вы хотите изменить.
7. Нажмите на кнопку **Сохранить**.

Масштаб отображения виджетов будет настроен.

Основные принципы работы с виджетами типа "Обнаружения"

Для всех виджетов типа "Обнаружения" можно настроить масштаб отображения (см. раздел "Настройка масштаба отображения виджетов" на стр. 327).

В левой части каждого виджета отображается легенда виджета по цветам, которые используются на виджетах.

Пример:

На виджете **Обнаружения по степени важности** отображается количество обнаружений различной степени важности.

Важность – важность обнаружения для пользователя Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние это обнаружение может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".

На виджете **Обнаружения по степени важности** важность обнаружений отмечена следующими цветами:

- красным – обнаружения высокой степени важности;
- оранжевым – обнаружения средней степени важности;
- зеленым – обнаружения низкой степени важности.

Справа от легенды отображается количество обнаружений каждого типа за выбранный период отображения данных на виджетах (см. раздел "Настройка периода отображения данных на виджетах" на стр. 247).

По ссылке с типом каждого обнаружения можно перейти в раздел **Обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331) веб-интерфейса приложения и просмотреть все обнаружения этого типа. При этом обнаружения будут отфильтрованы (см. раздел "Фильтрация, сортировка и поиск обнаружений" на стр. 334) по данному типу.

Пример:

На виджете **Обнаружения по вектору атаки** отображаются обнаружения **Файлы из почты** – количество файлов, которые Kaspersky Anti Targeted Attack Platform обнаружила в почтовом трафике за выбранный период отображения данных на виджетах.

По ссылке **Файлы из почты** откроется раздел **Обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331) и отобразятся все обнаружения, связанные с обнаружением файлов в почтовом трафике за выбранный период отображения данных на виджетах. Данные будут отфильтрованы по следующим параметрам: **Время**, **Тип объекта**=FILE и **Источник объекта**=MAIL.

В правой части каждого виджета отображаются столбцы данных. На вертикальной оси отображается количество событий, на горизонтальной оси отображаются дата и время обнаружения. Вы можете изменить период отображения данных на виджетах (см. раздел "Настройка периода отображения данных на виджетах" на стр. 247) и выбрать тенант (см. раздел "Выбор тенанта для работы в веб-интерфейсе приложения" на стр. 323), информация о которых должна быть представлена на виджете.

При наведении курсора мыши на каждый столбец данных отображается количество обнаружений, подсчитанных за период, представленный этим столбцом. По умолчанию отображается количество

необработанных обнаружений. Вы можете включить отображение обработанных обнаружений, установив флажок **Обработано** в правом верхнем углу окна. В этом случае будет отображаться количество всех обнаружений.

Просмотр состояния работоспособности модулей и компонентов приложения

Если в работе модулей и компонентов приложения возникли проблемы, на которые администратору рекомендуется обратить внимание, в верхней части окна раздела **Мониторинг** веб-интерфейса приложения отображается рамка желтого цвета с предупреждениями.

Пользователю с ролью **Локальный администратор**, **Администратор** или **Аудитор** доступна информация о работоспособности того сервера Central Node, PCN или SCN, на котором он сейчас работает.

Пользователю с ролью **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности** или **Аудитор** доступна следующая информация о работоспособности:

- Если вы используете отдельный сервер Central Node, пользователю доступна информация о работоспособности того сервера Central Node, на котором он сейчас работает.
- Если вы используете режим режим распределенного решения и мультитенантности и пользователь работает на сервере SCN, пользователю доступна информация о работоспособности этого сервера SCN в рамках тех тенантов, к данным которых у него есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса приложения" на стр. 200).
- Если вы используете режим режим распределенного решения и мультитенантности и пользователь работает на сервере PCN, пользователю доступна информация о работоспособности этого сервера PCN и всех серверов SCN, подключенных к этому серверу, в рамках тех тенантов, к данным которых у него есть доступ.

► *Чтобы получить более подробную информацию о работоспособности модулей и компонентов приложения,*

по ссылке **Просмотреть сведения** откройте окно **Работоспособность системы**.

В окне **Работоспособность системы** в зависимости от работоспособности модулей и компонентов приложения отображается один из следующих значков:

- Значок OK, если модули и компоненты приложения работают нормально.
- Значок с количеством проблем (например, 1), если обнаружены проблемы, на которые администратору рекомендуется обратить внимание. В этом случае в правой части окна **Работоспособность системы** отображается подробная информация о проблемах.

Окно **Работоспособность системы** содержит разделы:

- **Работоспособность компонентов** – статус работы модулей и компонентов приложения, карантина, а также обновления баз на всех серверах, на которых работает приложение.

Пример:

Если базы одного или нескольких компонентов приложения не обновлялись в течение 24 часов, рядом с именем сервера, на котором установлены модули и компоненты приложения, отображается значок ⚠.

Для решения проблемы убедитесь, что серверы обновлений доступны. Если для соединения с серверами обновлений вы используете прокси-сервер, убедитесь, что на прокси-сервере нет ошибок, связанных с подключением к серверам Kaspersky Anti Targeted Attack Platform.

- **Обработано** – статус приема и обработки входящих данных. Статус формируется на основе следующих критериев:
  - Состояние получения данных с серверов с компонентом Sensor, с сервера или виртуальной машины с почтовым сенсором, с хостов с компонентом Endpoint Agent.
  - Информация о превышении максимально допустимого времени, которое объекты ожидают в очереди на проверку модулями и компонентами приложения.
- **Соединение с серверами** – состояние соединения между сервером PCN и подключенными серверами SCN (отображается, если вы используете режим распределенного решения и мультитенантности).

В случае обнаружения проблем в работоспособности модулей и компонентов приложения, которые вы не можете решить самостоятельно, рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Обращение в Службу технической поддержки" на стр. 670).

Просмотр таблицы обнаружений

Kaspersky Anti Targeted Attack Platform обрабатывает данные из следующих источников:

- Зеркалированного трафика локальной сети организации (HTTP-, FTP- и DNS-протоколов).
- HTTP- и FTP-трафика, а также HTTPS-трафика, если администратор настроил подмену SSL-сертификата на прокси-сервере.
- Копий сообщений электронной почты, полученных по протоколу POP3, SMTP, а также копий сообщений электронной почты, полученных от приложений Kaspersky Secure Mail Gateway или Kaspersky Security для Linux Mail Server, если они используется в вашей организации.
- Данных о запущенных процессах, открытых сетевых соединениях и изменяемых файлах, полученных от отдельных компьютеров, которые входят в IT-инфраструктуру организации.

Kaspersky Anti Targeted Attack Platform отображает обнаруженные признаки целевых атак и вторжений в IT-инфраструктуру организации в виде таблицы обнаружений.

В таблице обнаружений не отображается информация об объектах, для которых выполняется хотя бы одно из следующих условий:

- Объект имеет репутацию *Доверенный* в базе KSN.
- Объект имеет цифровую подпись одного из доверенных производителей:
  - "Лаборатория Касперского".
  - Google.
  - Apple.
  - Microsoft.

Информация об этих обнаружениях сохраняется в базе данных приложения (на Central Node или SCN).

Информация об обнаружениях в базе данных ротируется ежедневно в ночное время при достижении максимально разрешенного количества обнаружений:

- Обнаружения, выполненные компонентами **(IDS) Intrusion Detection System**, **(URL) URL Reputation** – 100000 обнаружений для каждого из компонентов.
- Все остальные обнаружения – 20000 обнаружений для каждого из модулей или компонентов.

Если вы используете режим распределенного решения и мультитенантности, то ротация производится на всех SCN, а затем происходит синхронизация с PCN. После синхронизации все удаленные обнаружения автоматически удаляются также на PCN.

Таблица обнаружений находится в разделе **Обнаружения**.

По умолчанию в разделе отображается информация только об обнаружениях, не обработанных пользователями. Если вы хотите, чтобы информация об обработанных обнаружениях тоже отображалась, включите переключатель **Обработано** в правом верхнем углу окна.

Вы можете сортировать обнаружения в таблице (см. раздел "Фильтрация, сортировка и поиск обнаружений" на стр. 334) по столбцам **Создано** или **Обновлено**, **Важность**, **Адрес источника** и **Состояние**.

В таблице обнаружений содержится следующая информация:

1. **VIP** – наличие у обнаружения статуса с особыми правами доступа. Например, обнаружения со статусом VIP недоступны для просмотра пользователями программы **Сотрудник службы безопасности**.
2. **Создано** – время, в которое программа выполнила обнаружение и **Обновлено** – время, в которое обнаружение было обновлено.
3. – важность обнаружения для пользователя Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние это обнаружение может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".

   Обнаружения могут принимать одну из следующих степеней важности:

   - **Высокая**, отмеченную знаком , – обнаружение высокой степени важности.
   - **Средняя**, отмеченную знаком , – обнаружение средней степени важности.
   - **Низкая**, отмеченную знаком , – обнаружение низкой степени важности.
4. **Обнаружено** – одна или несколько категорий обнаруженных объектов. Например, если приложение обнаружило файл, зараженный вирусом Trojan-Downloader.JS.Cryptoload.ad, в поле **Обнаружено** будет указана категория Trojan-Downloader.JS.Cryptoload.ad для этого обнаружения.
5. **Сведения** – краткая информация об обнаружении. Например, имя обнаруженного файла или URL-адрес вредоносной ссылки.
6. **Адрес источника** – адрес источника обнаруженного объекта. Например, адрес электронной почты, с которого был отправлен вредоносный файл, или URL-адрес, с которого был загружен вредоносный файл.
7. **Адрес назначения** – адрес назначения обнаруженного объекта. Например, адрес электронной почты почтового домена вашей организации, на который был отправлен вредоносный файл, или IP-адрес компьютера локальной сети вашей организации, на который был загружен вредоносный файл.
8. **Технологии** – названия модулей или компонентов приложения, выполнивших обнаружение.

   В столбце **Технологии** могут быть указаны следующие модули и компоненты приложения:

   - **(YARA) YARA**.
   - **(SB) Sandbox**.
   - **(URL) URL Reputation**.
   - **(IDS) Intrusion Detection System**.
   - **(AM) Anti-Malware Engine**.
   - **(TAA) Targeted Attack Analyzer**.
   - **(IOC) IOC**.
9. **Состояние** – состояние обнаружения в зависимости от того, обработал пользователь Kaspersky Anti Targeted Attack Platform это обнаружение или нет.

   Обнаружения могут быть в одном из следующих состояний:

   - **Новое** – новые обнаружения.

    - **В обработке** – обнаружения, которые один из пользователей Kaspersky Anti Targeted Attack Platform уже обрабатывает.
    - **Повторная проверка** – обнаружения, выполненные в результате повторной проверки объекта.
    - **Назначено** – имя пользователя, которому назначено обнаружение.
- **Серверы** – имена серверов, на которых выполнено обнаружение. Серверы относятся к тому тенанту, с которым вы работаете в веб-интерфейсе приложения (см. раздел "Начало работы в веб-интерфейсе приложения под учетной записью локального администратора" на стр. 186). Столбец отображается, если вы используете режим распределенного решения и мультитенантности.

Если информация в столбцах таблицы отображается в виде ссылки, по ссылке раскрывается список, в котором вы можете выбрать действие над объектом. В зависимости от типа значения ячейки вы можете выполнить одно из следующих действий:

- Любой тип значения ячейки:
    - **Добавить в фильтр**.
    - **Исключить из фильтра**.
    - **Скопировать значение в буфер**.
- MD5-хеш:
    - **Добавить в фильтр**.
    - **Исключить из фильтра**.
    - **Найти события** (см. раздел "**Информация о событиях**" на стр. 378).
    - **Найти на TIP**.
    - **Создать правило запрета** (см. раздел "**Работа с политиками (правилами запрета)**" на стр. 486).
    - **Скопировать значение в буфер**.
- SHA256-хеш:
    - **Добавить в фильтр**.
    - **Исключить из фильтра**.
    - **Найти события** (см. раздел "**Информация о событиях**" на стр. 378).
    - **Найти на TIP**.
    - **Создать правило запрета** (см. раздел "**Работа с политиками (правилами запрета)**" на стр. 486).
    - **Скопировать значение в буфер**.
- IP-адрес назначения
    - **Найти события**.
- Состояние обнаружения:
    - **Назначить мне**.
    - **Закрыть обнаружение**.

Модуль **Intrusion Detection System** консолидирует информацию об обработанных сетевых событиях в одном обнаружении при одновременном соблюдении следующих условий:

- для сетевых событий совпадает название сработавшего правила, версия баз приложения и источник;
- между событиями прошло не более 24 часов.

Для всех сетевых событий, удовлетворяющих этим условиям, отображается одно обнаружение. В уведомлении об обнаружении содержится информация только о первом сетевом событии.

Настройка отображения таблицы обнаружений

Вы можете настроить отображение столбцов, а также порядок их следования в таблице обнаружений.

► *Чтобы настроить отображение таблицы обнаружений:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. В заголовочной части таблицы нажмите на кнопку .

   Отобразится окно **Настройка таблицы**.

3. Если вы хотите включить отображение столбца в таблице, установите флажок рядом с названием того параметра, который должен отображаться в таблице.

   Если вы не хотите, чтобы параметр отображался в таблице, снимите флажок.

   Должен быть установлен хотя бы один флажок.

4. Если вы хотите изменить порядок отображения столбцов в таблице, наведите курсор мыши на строку с нужным параметром, нажмите на кнопку и переместите строку с параметром в нужное место.
5. Если вы хотите восстановить параметры отображения таблицы по умолчанию, нажмите на ссылку **По умолчанию**.
6. Нажмите на кнопку **Применить**.

Отображение таблицы обнаружений будет настроено.

Фильтрация, сортировка и поиск обнаружений

Вы можете отфильтровать обнаружения для отображения в таблице обнаружений по одному или нескольким столбцам таблицы или выполнить поиск обнаружений по некоторым столбцам таблицы по указанным вами показателям.

Вы можете создавать, сохранять и удалять фильтры, а также запускать фильтрацию и поиск обнаружений по условиям, заданным в сохраненных фильтрах.

Если вы используете режим распределенного решения и мультитенантности, вы не сможете сохранять фильтры на PCN.

Фильтры сохраняются для каждого из пользователей на том сервере, на котором они созданы.

Вы также можете сортировать обнаружения в таблице по столбцам **Создано** или **Обновлено**, **Важность**, **Адрес источника** и **Состояние**.

По умолчанию в разделе отображается информация только об обнаружениях, не обработанных пользователями. Если вы хотите, чтобы информация об обработанных обнаружениях тоже отображалась, включите переключатель **Обработано** в правом верхнем углу окна.

В этом разделе

Фильтрация обнаружений по наличию статуса VIP 335
Фильтрация и поиск обнаружений по времени 336
Фильтрация обнаружений по степени важности 336
Фильтрация и поиск обнаружений по категориям обнаруженных объектов 337
Фильтрация и поиск обнаружений по полученной информации 338
Фильтрация и поиск обнаружений по адресу источника 339
Фильтрация и поиск обнаружений по адресу назначения 339
Фильтрация и поиск обнаружений по имени сервера 340
Фильтрация и поиск обнаружений по названию технологии 340
Фильтрация и поиск обнаружений по состоянию их обработки пользователем 341
Сортировка обнаружений в таблице 342
Быстрое создание фильтра обнаружений 343
Сброс фильтра обнаружений 343

Фильтрация обнаружений по наличию статуса VIP

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю ☆ – наличие у обнаружения статуса с особыми правами доступа. Например, обнаружения со статусом VIP недоступны для просмотра пользователями программы **Сотрудник службы безопасности**.

► *Чтобы отфильтровать обнаружения по наличию статуса VIP:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Нажатием на заголовок столбца **VIP** раскройте список параметров фильтрации.

3. Настройте фильтрацию обнаружений:
   - Если вы хотите, чтобы в таблице обнаружений отобразились только обнаружения со статусом VIP, выберите **VIP**.
   - Если вы хотите, чтобы в таблице обнаружений отобразились все обнаружения, выберите **Все**.

   Если ни одно из значений не выбрано, в таблице отображаются все обнаружения.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по времени

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Создано** – время, в которое произошло обнаружение, а также **Обновлено** – время, в которое обнаружение было обновлено.

► *Чтобы отфильтровать или найти обнаружения по времени:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. По ссылке **Создано** раскройте список периодов отображения обнаружений.
3. В списке **Время** выберите один из следующих периодов отображения обнаружений:
   - **Все**, если вы хотите, чтобы приложение отображало в таблице все обнаружения.
   - **Прошедший час**, если вы хотите, чтобы приложение отображало в таблице обнаружения, произошедшие за последний час.
   - **Прошедшие сутки**, если вы хотите, чтобы приложение отображало в таблице обнаружения, произошедшие за последний день.
   - **Пользовательский диапазон**, если вы хотите, чтобы приложение отображало в таблице обнаружения, произошедшие за указанный вами период.
4. Если вы выбрали период отображения событий **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения обнаружений.
   b. Нажмите на кнопку **Применить**.

   Календарь закроется.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация обнаружений по степени важности

Вы можете отфильтровать события, обнаруженные программой, а также осуществить поиск событий в таблице событий по показателю **Важность** – важность обнаружения для пользователя Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние это обнаружение может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".

► *Чтобы отфильтровать обнаружения по степени важности:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. По значку раскройте список параметров фильтрации.
3. Выберите одну или несколько из следующих степеней важности обнаружений:
   - **Низкая** – обнаружение низкой степени важности.
   - **Средняя** – обнаружение средней степени важности.
   - **Высокая** – обнаружение высокой степени важности.

   Если ни одно из значений не выбрано, в таблице отображаются обнаружения всех степеней важности.

4. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по категориям обнаруженных объектов

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Обнаружено** – одна или несколько категорий объекта, обнаруженного в событии. Например, если вы хотите, чтобы приложение отображало в таблице обнаружения файлов, зараженных определенным вирусом, вы можете задать фильтр по названию этого вируса.

► *Чтобы отфильтровать или найти обнаружения по категориям обнаруженных объектов:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. По ссылке **Обнаружено** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации обнаружений:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода введите название категории (например, Trojan) или несколько символов из названия категории.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по полученной информации

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Сведения** – краткая информация об обнаружении. Например, имя обнаруженного файла или URL-адрес вредоносной ссылки.

► *Чтобы отфильтровать или найти обнаружения по полученной информации:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. По ссылке **Сведения** откройте окно настройки фильтрации.
3. В левом раскрывающемся списке выберите один из следующих критериев поиска:
   - **Сведения**. Поиск будет осуществляться по всем сведениям об обнаруженном объекте.
   - **ID**.
   - **Файл**.
   - **Тип файла**.
   - **MD5**.
   - **SHA256**.
   - **URL**.
   - **Домен**.
   - **Агент пользователя**.
   - **Тема**.
   - **HTTP-статус**.
   - **Источник объекта**.
   - **Тип объекта**.
   - **Автоотправка в Sandbox**.
   - **Правило TAA (IOA)**.
4. В правом раскрывающемся списке выберите один из следующих операторов фильтрации обнаружений:
   - **Содержит**.
   - **Не содержит**.
   - **Равняется**.
   - **Не равняется**.
5. В поле ввода укажите один или несколько символов информации об обнаружении.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
7. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по адресу источника

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Адрес источника** – адрес источника обнаружения. Например, адрес электронной почты, с которого был отправлен вредоносный файл, или IP-адрес компьютера локальной сети вашей организации, на который был загружен вредоносный файл.

► *Чтобы отфильтровать или найти обнаружения по адресу источника:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. По ссылке **Адрес источника** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации обнаружений:
   - **Содержит**.
   - **Не содержит**.
   - **Соответствует шаблону**.
   - **Не соответствует шаблону**.
4. В поле ввода укажите один или несколько символов адреса источника обнаружения.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по адресу назначения

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Адрес назначения** – адрес назначения обнаруженного объекта. Например, адрес электронной почты почтового домена вашей организации, на который был отправлен вредоносный файл, или IP-адрес компьютера локальной сети вашей организации, на который был загружен вредоносный файл.

► *Чтобы отфильтровать или найти обнаружения по адресу назначения:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. По ссылке **Адрес назначения** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации обнаружений:
   - **Содержит**.
   - **Не содержит**.
   - **Соответствует шаблону**.
   - **Не соответствует шаблону**.

4. В поле ввода укажите один или несколько символов адреса назначения обнаруженного объекта.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по имени сервера

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Серверы** – имена серверов, на которых выполнено обнаружение.

Если вы используете режим распределенного решения и мультитенантности, серверы относятся к тому тенанту, с которым вы работаете в веб-интерфейсе приложения (см. раздел "Начало работы в веб-интерфейсе приложения под учетной записью локального администратора" на стр. 186). Фильтрация доступна только на PCN.

► *Чтобы отфильтровать или найти обнаружения по имени сервера:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. По ссылке **Серверы** раскройте список серверов, на которых выполнены обнаружения.
3. Установите флажки рядом с одним или несколькими именами серверов.
4. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по названию технологии

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Технологии** – названия модулей или компонентов программы, выполнивших обнаружение.

► *Чтобы отфильтровать обнаружения по названию технологии:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. По ссылке **Технологии** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации обнаружений:
   - **Содержит**, если вы хотите, чтобы приложение отображало обнаружения, выполненные модулем или компонентом приложения, который вы укажете.
   - **Не содержит**, если вы хотите, чтобы приложение скрывало обнаружения, выполненные модулем или компонентом приложения, который вы укажете.

- **Равняется**, если вы хотите, чтобы приложение отображало обнаружения, выполненные модулем или компонентом приложения, который вы укажете.
- **Не равняется**, если вы хотите, чтобы приложение скрывало обнаружения, выполненные модулем или компонентом приложения, который вы укажете.

4. В раскрывающемся списке справа от выбранного вами оператора фильтрации обнаружений выберите название технологии, по которой вы хотите отфильтровать обнаружения:
   - **(YARA) YARA**.
   - **(SB) Sandbox**.
   - **(URL) URL Reputation**.
   - **(IDS) Intrusion Detection System**.
   - **(AM) Anti-Malware Engine**.
   - **(TAA) Targeted Attack Analyzer**.
   - **(IOC) IOC**.

   Например, если вы хотите, чтобы приложение отобразило в списке обнаружения, выполненные компонентом Sandbox, выберите оператор фильтрации **Содержит** и название компонента **(SB) Sandbox**.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по состоянию их обработки пользователем

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Состояние** – состояние обнаружения в зависимости от того, обработал пользователь Kaspersky Anti Targeted Attack Platform это обнаружение или нет.

► *Чтобы отфильтровать или найти обнаружения по состоянию их обработки пользователем Kaspersky Anti Targeted Attack Platform:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. Если вы хотите включить в фильтр обработанные обнаружения, включите переключатель **Обработано** в правом верхнем углу окна.
3. По ссылке **Состояние** раскройте список вариантов обнаружений в зависимости от состояния их обработки пользователем Kaspersky Anti Targeted Attack Platform.
4. Выберите одно из следующих значений:
   - **Новое**, если вы хотите, чтобы приложение отображало новые обнаружения, которые ни один из пользователей еще не начал обрабатывать.

- **В обработке**, если вы хотите, чтобы приложение отображало обнаружения, которые один из пользователей Kaspersky Anti Targeted Attack Platform уже обрабатывает.
- **Повторная проверка**, если вы хотите, чтобы приложение отображало обнаружения, произошедшие в результате повторной проверки.

5. В поле **Имя пользователя** введите имя пользователя, если вы хотите найти обнаружения, назначенные определенному пользователю **Старший сотрудник службы безопасности** или **Сотрудник службы безопасности**.
6. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Сортировка обнаружений в таблице

Вы можете сортировать обнаружения в таблице по столбцам **Создано** или **Обновлено**, **Важность**, **Адрес источника** и **Состояние**.

► *Чтобы отсортировать обнаружения в таблице обнаружений:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. Если вы хотите отсортировать обнаружения по дате, справа от названия столбца **Создано** (если в таблице отображается дата создания обнаружений) или **Обновлено** (если в таблице отображается дата обновления обнаружений) нажмите на один из значков:
   - ↑ – новые обнаружения отобразятся вверху таблицы.
   - ↓ – старые обнаружения отобразятся вверху таблицы.
3. Если вы хотите отсортировать обнаружения по степени важности, справа от значка нажмите на один из значков:
   - ↑ – обнаружения высокой степени важности отобразятся вверху таблицы.
   - ↓ – обнаружения низкой степени важности отобразятся вверху таблицы.
4. Если вы хотите отсортировать обнаружения по адресу источника обнаруженного объекта, справа от названия столбца **Адрес источника** нажмите на один из значков:
   - ↑ – сортировка выполнится по алфавиту A–Z.
   - ↓ – сортировка выполнится по алфавиту Z–A.
5. Если вы хотите отсортировать обнаружения по состоянию их обработки пользователем, справа от названия столбца **Состояние** нажмите на один из значков:
   - ↑ – обнаружения будут отсортированы по порядку их обработки **Новое** - **Повторная проверка** - **В обработке** - **Закрыто**.
   - ↓ – обнаружения будут отсортированы по порядку их обработки **Закрыто** - **В обработке** - **Повторная проверка** - **Новое**.

Быстрое создание фильтра обнаружений

► *Чтобы быстро создать фильтр обнаружений:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Выполните следующие действия по быстрому добавлению условий фильтрации в создаваемый фильтр:

   a. Наведите курсор мыши на ссылку с тем значением столбца таблицы, которое вы хотите добавить в качестве условия фильтрации.

   b. Нажмите на левую клавишу мыши.

      Откроется список действий над значением.

   c. В открывшемся списке выберите одно из следующих действий:

      - **Добавить в фильтр**, если вы хотите включить это значение в условие фильтрации.
      - **Исключить из фильтра**, если вы хотите исключить это значение из условия фильтрации.

3. Если вы хотите добавить несколько условий фильтрации в создаваемый фильтр, выполните действия по быстрому добавлению каждого из условий фильтрации в создаваемый фильтр.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Сброс фильтра обнаружений

► *Чтобы сбросить фильтр обнаружений по одному или нескольким условиям фильтрации:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Нажмите на кнопку ☒ справа от того заголовка столбца таблицы обнаружений, условия фильтрации по которому вы хотите сбросить.

   > Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Рекомендации по обработке обнаружений

В составе информации об обнаружениях, выполненных технологиями AM (Anti-Malware Engine), SB (Sandbox), YARA, IOC и IDS (intrusion Detection System) в правой части окна отображаются рекомендации по

обработке этих обнаружений.

► *Чтобы просмотреть информацию об обнаружении, выполните следующие действия:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Левой клавишей мыши нажмите на строку с тем обнаружением, информацию о котором вы хотите просмотреть.

Откроется окно с информацией об обнаружении.

В этом разделе

Рекомендации по обработке AM-обнаружений 344
Рекомендации по обработке TAA-обнаружений 345
Рекомендации по обработке SB-обнаружений 346
Рекомендации по обработке IOC-обнаружений 347
Рекомендации по обработке YARA-обнаружений 348
Рекомендации по обработке IDS-обнаружений 349

Рекомендации по обработке AM-обнаружений

В правой части окна в блоке **Рекомендации** отображаются рекомендации, которые вы можете выполнить, и количество обнаружений или событий, имеющих общие признаки с обнаружением, над которым вы работаете.

► *Вы можете выполнить следующие рекомендации:*

- В разделе **Оценка** раскройте список **Найти похожие обнаружения**.

  Отобразится список признаков, по которым вы можете найти похожие обнаружения, и количество похожих обнаружений по каждому признаку.

  Выберите один из следующих признаков:

  - **По MD5**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Сведения** - MD5-хешу. MD5-хеш файла из обнаружения, над которым вы работаете, выделен желтым цветом.
  - **По SHA256**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Сведения** - SHA256-хешу. SHA256-хеш файла из обнаружения, над которым вы работаете, выделен желтым цветом.
  - **По имени хоста**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Адрес источника**. Имя хоста из обнаружения, над которым вы работаете, выделено желтым цветом.
  - **По адресу отправителя**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Адрес источника**. Адрес отправителя сообщения электронной почты из обнаружения, над которым вы работаете, выделен желтым цветом.

- **По адресу получателя**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Адрес назначения**. Адрес получателя сообщения электронной почты из обнаружения, над которым вы работаете, выделен желтым цветом.
- **По URL**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Сведения** - URL-адресу из обнаружения, над которым вы работаете.

- В разделе **Оценка** выберите **Найти похожие события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска выбран тип события **Результат обработки обнаружения** и настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства обнаружения, над которым вы работаете. Например, MD5 файла из обнаружения.

  Действие доступно только если вы используете функциональность KEDR и добавили лицензионный ключ KEDR (см. раздел "О ключе" на стр. 158).

- В разделе **Расследование** выберите **Найти похожие события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства обнаружения, над которым вы работаете. Например, MD5 файла из обнаружения.

  Действие доступно только если вы используете функциональность KEDR и добавили лицензионный ключ KEDR (см. раздел "О ключе" на стр. 158).

Рекомендации по обработке TAA-обнаружений

В правой части окна в блоке **Рекомендации** отображаются рекомендации, которые вы можете выполнить, и количество обнаружений или событий, имеющих общие признаки с обнаружением, над которым вы работаете.

► *Вы можете выполнить следующие рекомендации:*

- В разделе **Оценка** раскройте список **Найти похожие обнаружения**.

  Отобразится список признаков, по которым вы можете найти похожие обнаружения, и количество похожих обнаружений по каждому признаку.

  Выберите один из следующих признаков:

  - **По имени правила (TAA-обнаружения)**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцам **Обнаружено** и **Технологии** - имени правила TAA (IOA), в соответствии с которым было выполнено обнаружение, и названию технологии **(TAA) Targeted Attack Analyzer**.
  - **По имени правила (SB-обнаружения)**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцам **Обнаружено** и **Технологии** - имени правила TAA (IOA), в соответствии с которым было выполнено обнаружение, и названию технологии **(SB) Sandbox**.

- В разделе **Расследование** выберите **Найти похожие события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства обнаружения, над которым вы работаете. Например, MD5 файла из обнаружения.

  Действие доступно только если вы используете функциональность KEDR и добавили лицензионный ключ KEDR (см. раздел "О ключе" на стр. 158).

Рекомендации по обработке SB-обнаружений

В правой части окна в блоке **Рекомендации** отображаются рекомендации, которые вы можете выполнить, и количество обнаружений или событий, имеющих общие признаки с обнаружением, над которым вы работаете.

► *Вы можете выполнить следующие рекомендации:*

- В разделе **Оценка** раскройте список **Найти похожие обнаружения**.

  Отобразится список признаков, по которым вы можете найти похожие обнаружения, и количество похожих обнаружений по каждому признаку.

  Выберите один из следующих признаков:

  - **По MD5**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Сведения** - MD5-хешу. MD5-хеш файла из обнаружения, над которым вы работаете, выделен желтым цветом.
  - **По SHA256**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Сведения** - SHA256-хешу. SHA256-хеш файла из обнаружения, над которым вы работаете, выделен желтым цветом.
  - **По имени хоста**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Адрес источника**. Имя хоста из обнаружения, над которым вы работаете, выделено желтым цветом.
  - **По адресу отправителя**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Адрес источника**. Адрес отправителя сообщения электронной почты из обнаружения, над которым вы работаете, выделен желтым цветом.
  - **По адресу получателя**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Адрес назначения**. Адрес получателя сообщения электронной почты из обнаружения, над которым вы работаете, выделен желтым цветом.
  - **По URL**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Сведения** - URL-адресу из обнаружения, над которым вы работаете.
  - **По URL из Sandbox**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Сведения** - URL-адресу из обнаружения, над которым вы работаете, и всем URL-адресам, связь с которыми нашел компонент Sandbox (см. раздел "Результаты проверки в Sandbox" на стр. 357) в процессе обработки обнаружения.

- В разделе **Оценка** выберите **Найти похожие EPP-события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска выбран тип события **Результат обработки обнаружения** и настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В

значениях фильтрации указаны свойства обнаружения, над которым вы работаете. Например, MD5 файла из обнаружения.

Действие доступно только если вы используете функциональность KEDR и добавили лицензионный ключ KEDR (см. раздел "О ключе" на стр. 158).

- В разделе **Расследование** выберите **Найти похожие события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства обнаружения, над которым вы работаете. Например, MD5 файла из обнаружения.

  Действие доступно только если вы используете функциональность KEDR и добавили лицензионный ключ KEDR (см. раздел "О ключе" на стр. 158).

Рекомендации по обработке IOC-обнаружений

В правой части окна в блоке **Рекомендации** отображаются рекомендации, которые вы можете выполнить, и количество обнаружений, имеющих общие признаки с обнаружением, над которым вы работаете.

► *Вы можете выполнить следующие рекомендации:*

- В разделе **Оценка** выберите **Найти похожие обнаружения по имени хоста**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Адрес источника**. Имя хоста из обнаружения, над которым вы работаете, выделено желтым цветом.
- В разделе **Оценка** выберите **Найти похожие обнаружения по IOC**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Обнаружено** - имени IOC-файла из обнаружения, над которым вы работаете.
- В разделе **Сдерживание** выберите **Изолировать <имя хоста>**. Откроется окно создания правила сетевой изоляции.

► *Чтобы создать правило сетевой изоляции хоста, настройте следующие параметры:*

1. В поле **Отключить изоляцию через** введите количество часов от 1 до 9999, в течение которых будет действовать сетевая изоляция хоста.
2. В блоке параметров **Исключения для правила изоляции хоста** в списке **Направление трафика** выберите направление сетевого трафика, которое не должно быть заблокировано:
   - **Входящее/Исходящее**.
   - **Входящее**.
   - **Исходящее**.
3. В поле **IP** введите IP-адрес, сетевой трафик которого не должен быть заблокирован.

Если в роли компонента Endpoint Agent вы используете приложение Kaspersky Endpoint Agent, вы можете использовать прокси-сервер для соединения Kaspersky Endpoint Agent для Windows с Kaspersky Anti Targeted Attack Platform. При добавлении этого прокси-сервера в исключения сетевые ресурсы, к которым открыт доступ через прокси-сервер, также добавляются в исключения. Если в исключения добавлены сетевые ресурсы, соединение с которыми происходит через прокси-сервер, но при этом исключение для самого прокси-сервера не настроено, исключение не будет работать.

4. Если вы выбрали **Входящее** или **Исходящее**, в поле **Порты** введите порты подключения.
5. Если вы хотите добавить более одного исключения, нажмите на кнопку **Добавить** и повторите действия по заполнению полей **Направление трафика**, **IP** и **Порты**.
6. Нажмите на кнопку **Сохранить**.

Рекомендации по обработке YARA-обнаружений

В правой части окна в блоке **Рекомендации** отображаются рекомендации, которые вы можете выполнить, и количество обнаружений или событий, имеющих общие признаки с обнаружением, над которым вы работаете.

► *Вы можете выполнить следующие рекомендации:*

- В разделе **Оценка** раскройте список **Найти похожие обнаружения**.

  Отобразится список признаков, по которым вы можете найти похожие обнаружения, и количество похожих обнаружений по каждому признаку.

  Выберите один из следующих признаков:

  - **По MD5**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Сведения** - MD5-хешу. MD5-хеш файла из обнаружения, над которым вы работаете, выделен желтым цветом.
  - **По SHA256**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Сведения** - SHA256-хешу. SHA256-хеш файла из обнаружения, над которым вы работаете, выделен желтым цветом.
  - **По имени хоста**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Адрес источника**. Имя хоста из обнаружения, над которым вы работаете, выделено желтым цветом.
  - **По адресу отправителя**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Адрес источника**. Адрес отправителя сообщения электронной почты из обнаружения, над которым вы работаете, выделен желтым цветом.
  - **По адресу получателя**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Адрес назначения**. Адрес получателя сообщения электронной почты из обнаружения, над которым вы работаете, выделен желтым цветом.
  - **По URL**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Сведения** - URL-адресу из обнаружения, над которым вы работаете.

- В разделе **Оценка** выберите выберите **Найти похожие обнаружения по имени хоста**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска выбран тип

события **Результат обработки обнаружения** и настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства обнаружения, над которым вы работаете. Например, MD5 файла из обнаружения.

Действие доступно только если вы используете функциональность KEDR и добавили лицензионный ключ KEDR (см. раздел "О ключе" на стр. 158).

- В разделе **Расследование** выберите **Найти похожие события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства обнаружения, над которым вы работаете. Например, MD5 файла из обнаружения.

  Действие доступно только если вы используете функциональность KEDR и добавили лицензионный ключ KEDR (см. раздел "О ключе" на стр. 158).

- В разделе **Сдерживание** выберите **Изолировать <имя хоста>**. Откроется окно создания правила сетевой изоляции.

Рекомендации по обработке IDS-обнаружений

В правой части окна в блоке **Рекомендации** отображаются рекомендации, которые вы можете выполнить, и количество обнаружений или событий, имеющих общие признаки с обнаружением, над которым вы работаете.

► *Вы можете выполнить следующие рекомендации:*

- В разделе **Оценка** выберите **Найти похожие обнаружения по имени хоста**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Адрес источника**. Имя хоста или IP-адрес из обнаружения, над которым вы работаете, выделено желтым цветом.
- В разделе **Оценка** выберите **Найти похожие обнаружения по URL**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Сведения** - URL-адресу. URL-адрес из обнаружения, над которым вы работаете, выделен желтым цветом.
- В разделе **Оценка** выберите **Добавить в исключения**.

  Откроется окно **Добавить правило IDS в исключения**. Если вы хоте добавить правило IDS, по которому выполнено обнаружение, в исключения, введите комментарий в поле **Описание** и нажмите на кнопку **Добавить**.

  Правило IDS будет добавлено в исключения и отобразится в списке исключений в разделе **Параметры** веб-интерфейса приложения, подразделе **Исключения** на закладке **IDS**.
- В разделе **Расследование** выберите **Найти похожие события по URL**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска по **URI** из обнаружения, над которым вы работаете.
- В разделе **Расследование** выберите **Найти похожие события по имени хоста**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска по **RemoteIP** из обнаружения, над которым вы работаете.

- В разделе **Расследование** по ссылке **Скачать артефакт IDS** вы можете скачать файл с данными об обнаружении.
- В разделе **Расследование** по ссылке **Скачать PCAP-файл** вы можете скачать файл с данными перехваченного трафика.

Просмотр обнаружений

В веб-интерфейсе приложения отображаются следующие типы обнаружений, на которые пользователю Kaspersky Anti Targeted Attack Platform рекомендуется обратить внимание:

- На компьютер локальной сети организации был загружен файл или была предпринята попытка загрузки файла. Приложение обнаружило этот файл в зеркалированном трафике локальной сети организации или в ICAP-данных HTTP- и FTP-трафика, а также HTTPS-трафика, если администратор настроил подмену SSL-сертификата на прокси-сервере.
- На адрес электронной почты пользователя локальной сети организации был отправлен файл. Приложение обнаружило этот файл в копиях сообщений электронной почты, полученных по протоколу POP3 или SMTP, или полученных с виртуальной машины или сервера с программой Kaspersky Secure Mail Gateway, если она используется в вашей организации.
- На компьютере локальной сети организации была открыта ссылка на веб-сайт. Приложение обнаружило эту ссылку на веб-сайт в зеркалированном трафике локальной сети организации или в ICAP-данных HTTP- и FTP-трафика, а также HTTPS-трафика, если администратор настроил подмену SSL-сертификата на прокси-сервере.
- IP-адрес или доменное имя компьютера локальной сети организации были замечены в сетевой активности. Приложение обнаружило эту сетевую активность в зеркалированном трафике локальной сети организации.
- На компьютере локальной сети организации были запущены процессы. Приложение обнаружило эти процессы с помощью компонента Endpoint Agent, установленного на компьютеры, входящие в IT-инфраструктуру организации.

Если обнаружен файл, в зависимости от того, какие модули или компоненты программы выполнили обнаружение, в веб-интерфейсе программы может отображаться следующая информация:

- общая информация об обнаружении и обнаруженном файле (например, IP-адрес компьютера, на котором обнаружен файл, имя обнаруженного файла);
- результаты антивирусной проверки файла, выполненной ядром AM Engine;
- результаты проверки файла на наличие признаков вторжения в IT-инфраструктуру организации, выполненной модулем YARA;
- результаты исследования поведения файла, выполненного компонентом Sandbox;
- результаты анализа исполняемых файлов формата APK в облачной инфраструктуре на основе технологии машинного обучения.

Если обнаружена ссылка на веб-сайт, в зависимости от того, какие модули или компоненты программы выполнили обнаружение, в веб-интерфейсе программы может отображаться следующая информация:

- общая информация об обнаружении и обнаруженной ссылке на веб-сайт (например, IP-адрес компьютера, на котором обнаружена ссылка на веб-сайт, адрес ссылки на веб-сайт);

- результаты проверки ссылки на наличие признаков вредоносного, фишингового URL-адреса или URL-адреса, который ранее использовался злоумышленниками для целевых атак на IT-инфраструктуру организаций, выполненной модулем URL Reputation.

Если обнаружена сетевая активность IP-адреса или доменного имени компьютера локальной сети организации, в веб-интерфейсе программы может отображаться следующая информация:

- общая информация об обнаружении и обнаруженной сетевой активности;
- результаты проверки интернет-трафика на наличие признаков вторжения в IT-инфраструктуру организации по предустановленным правилам, выполненной модулем Intrusion Detection System (IDS);
- результаты исследования сетевой активности, выполненного по правилам TAA (IOA) "Лаборатории Касперского";
- результаты исследования сетевой активности, выполненного по пользовательским правилам TAA (IOA), IDS, IOC.

Если обнаружены процессы, запущенные на компьютере локальной сети организации, на котором установлен компонент Endpoint Agent, в веб-интерфейсе программы может отображаться следующая информация:

- общая информация об обнаружении и процессах, запущенных на этом компьютере;
- результаты исследования сетевой активности компьютера, выполненного по правилам TAA (IOA) "Лаборатории Касперского";
- результаты исследования сетевой активности компьютера, выполненного по пользовательским правилам TAA (IOA), IOC.

В этом разделе

Просмотр информации об обнаружении 351

Просмотр информации об обнаружении

► *Чтобы просмотреть информацию об обнаружении:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Левой клавишей мыши нажмите на строку с тем обнаружением, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией об обнаружении.

Общая информация об обнаружении любого типа

Независимо от того, какой технологией выполнено обнаружение - в заголовке окна с информацией об обнаружении отображается идентификатор обнаружения. Рядом с состоянием отображается значок ☆ или ★ в зависимости от наличия у обнаружения статуса VIP.

В верхней части окна с информацией об обнаружении может отображаться следующая общая информация

об обнаружении:

- **Состояние** – состояние обнаружения в зависимости от того, обработал пользователь Kaspersky Anti Targeted Attack Platform это обнаружение или нет.
- **Важность** – важность обнаружения для пользователя Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние это обнаружение может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".
- **Сервер** – имя сервера, на котором выполнено обнаружение. Серверы относятся к той организации, с которой вы работаете в веб-интерфейсе приложения (см. раздел "Начало работы в веб-интерфейсе приложения под учетной записью локального администратора" на стр. 186).
- **Хост** – доменное имя компьютера, на котором произошло обнаружение.
- **Источник данных** – источник данных. Например, SMTP Sensor или SPAN Sensor.
- **Время создания** – время, когда было выполнено обнаружение.
- **Время обновления** – время, когда была обновлена информация об обнаружении.

Информация в блоке Информация об объекте

В блоке **Информация об объекте** может отображаться следующая информация об обнаруженном объекте:

- Имя файла.

  По ссылке с именем файла раскрывается действие **Скопировать значение в буфер**.
- Тип файла. Например, ExecutableWin32.

  Кнопка **Найти на TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.

  Кнопка **Создать правило запрета** позволяет запретить запуск файла.

  Кнопка **Скачать** позволяет загрузить файл на жесткий диск вашего компьютера.

  Файл загружается в формате ZIP-архива, зашифрованного паролем infected. Имя файла внутри архива заменено на MD5-хеш файла. Расширение файла внутри архива не отображается.
- Размер файла в килобайтах.
- **MD5** – MD5-хеш файла.

  По ссылке с **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на TIP**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.
- **SHA256** – SHA256-хеш файла.

  По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на TIP**.
  - **Найти на virustotal.com**.

  - **Найти события**.
  - **Найти обнаружения**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.
- **Адрес отправителя** – адрес электронной почты, с которого было отправлено сообщение, содержащее файл.
- **Адрес получателя** – один или несколько адресов электронной почты, на которые было отправлено сообщение, содержащее файл.
- **Исходный адрес отправителя** – исходный адрес электронной почты, с которого было отправлено сообщение, содержащее файл.

  Данные для этого поля берутся из заголовка Received.
- **Исходный адрес получателя** – исходный адрес или адреса электронной почты, на которые было отправлено сообщение, содержащее файл.

  Данные для этого поля берутся из заголовка Received.
- **Тема** – тема сообщения.
- **IP сервера-отправителя** – IP-адрес первого в цепочке отправки сообщения почтового сервера.

  По ссылке **IP сервера-отправителя** раскрывается список, в котором вы можете выбрать одно из следующих действий:
  - **Найти события**.
  - **Найти обнаружения**.
  - **Скопировать значение в буфер**.
- **Заголовки** – расширенный набор заголовков сообщения электронной почты. Например, может содержать информацию об адресах электронной почты отправителя и получателей сообщения, о почтовых серверах, передавших сообщение, о типе контента сообщения электронной почты.

Информация в блоке Информация об обнаружении

В блоке **Информация об обнаружении** может отображаться следующая информация об обнаружении:

- , или – важность обнаружения для пользователя Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние это обнаружение может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".
- **Время** – время, в которое программа выполнила обнаружение.
- **Обнаружено** – одна или несколько категорий обнаруженных объектов. Например, если приложение обнаружило файл, зараженный вирусом Trojan-Downloader.JS.Cryptoload.ad, в поле **Обнаружено** будет указана категория Trojan-Downloader.JS.Cryptoload.ad для этого обнаружения.
- **Метод** – метод HTTP-запроса. Например, Get, Post или Connect.
- **URL** – обнаруженный URL-адрес. Может также содержать код ответа.

  По ссылке с **URL** раскрывается список, в котором вы можете выбрать одно из следующих действий:
  - **Найти на TIP по URL**.

- **Найти на TIP по имени домена**.
- **Найти события**.
- **Найти обнаружения**.
- **Скопировать значение в буфер**.

- **Referrer** – URL-адрес, с которого произошло перенаправление на ссылку на веб-сайт, требующую внимания. В HTTP-протоколе это один из заголовков запроса клиента, содержащий URL-адрес источника запроса.
- **IP назначения** – IP-адрес ресурса, к которому обращался пользователь или приложение.

  По ссылке с **IP назначения** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на TIP**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Скопировать значение в буфер**.
- **Имя пользователя** – имя учетной записи пользователя, действия которого привели к возникновению события.
- **Запрос/Ответ** – длина запроса и ответа.

Информация в блоке Результаты проверки

В блоке **Результаты проверки** могут отображаться следующие результаты проверки обнаружения:

- Названия модулей или компонентов приложения, выполнивших обнаружение.
- Одна или несколько категорий обнаруженного объекта. Например, может отображаться название вируса Virus.Win32.Chiton.i.
- Версии баз модулей и компонентов Kaspersky Anti Targeted Attack Platform, выполнивших обнаружение.
- Результаты проверки обнаружений модулями и компонентами приложения:
  - **YARA** – результаты потоковой проверки файлов и объектов, поступающих на Central Node, или результаты проверки хостов с компонентом Endpoint Agent. Может принимать следующие значения:
    - Категория обнаруженного файла в правилах YARA (например, может отображаться название категории susp_fake_Microsoft_signer).

      Отображается при потоковой проверке.

      Кнопка **Создать правило запрета** позволяет запретить запуск файла.

      Кнопка **Найти на TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.
    - Путь к файлу и/или имя дампа памяти.

      Отображается при проверке хостов с компонентом Endpoint Agent.

      По ссылке с путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

      - **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).

- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- **Скопировать значение в буфер**.

Кнопка **Создать задачу** позволяет создать следующие задачи (см. раздел "Работа с задачами" на стр. 456):

- **Собрать данные** → **Файл** (см. раздел "**Создание задачи получения файла**" на стр. 460), **Образ диска** (см. раздел "**Создание задачи получения образа диска**" на стр. 466), **Дамп памяти** (см. раздел "**Создание задачи получения дампа оперативной памяти**" на стр. 469).
- **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
- **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).

Кнопка **Создать правило запрета** позволяет запретить запуск файла.

Кнопка **Найти на TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.

Кнопка **Просмотреть на карантине** позволяет просмотреть информацию об объекте, помещенном на карантин (см. раздел "Просмотр информации об объекте на карантине" на стр. 546).

- **SB** (Sandbox) – результаты исследования поведения файла, выполненного компонентом Sandbox.

  Нажатием на кнопку **Sandbox-обнаружение** вы можете открыть окно с подробной информацией о результатах исследования поведения файла.

  Кнопка **Найти на TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.

  Кнопка **Создать правило запрета** позволяет запретить запуск файла.

  Вы можете загрузить подробный журнал исследования поведения файла во всех операционных системах нажав на кнопку **Скачать сведения об отладке**.

  Файл загружается в формате ZIP-архива, зашифрованного паролем infected. Имя проверенного файла внутри архива заменено на MD5-хеш файла. Расширение файла внутри архива не отображается.

  > По умолчанию максимальный объем жесткого диска для хранения журналов исследования поведения файлов во всех операционных системах составляет 300 ГБ. По достижении этого ограничения приложение удаляет журналы исследования поведения файлов, созданные раньше остальных, и заменяет их новыми журналами.

- **URL** (URL Reputation) – категория обнаруженного вредоносного, фишингового URL-адреса или URL-адреса, который ранее использовался злоумышленниками для целевых атак на IT-инфраструктуру организаций.
- **IDS** (Intrusion Detection System) – категория обнаруженного объекта по базе Intrusion Detection System или название пользовательского правила IDS, по которому было выполнено обнаружение. Например, может отображаться категория Trojan-Clicker.Win32.Cycler.a.

  По ссылке открывается информация о категории объекта в базе угроз "Лаборатории Касперского" Kaspersky Threats.
- **AM** (Anti-Malware Engine) – категория обнаруженного объекта по антивирусной базе. Например, может отображаться название вируса Virus.Win32.Chiton.i.

По ссылке открывается информация о категории объекта в базе угроз "Лаборатории Касперского" Kaspersky Threats.

Кнопка **Найти на TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.

Кнопка **Создать правило запрета** позволяет запретить запуск файла.

Кнопка **Скачать** позволяет загрузить файл на жесткий диск вашего компьютера.

- **TAA** (Targeted Attack Analyzer) – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

  По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

- **IOC** – Название IOC-файла, по которому было выполнено обнаружение.

  При выборе IOC-файла открывается окно с результатами IOC-проверки (см. раздел "Результаты IOC-проверки" на стр. 359).

  По ссылке **Все события, связанные с обнаружением** в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска, например, по **MD5**, **FileFullName**. В значениях фильтрации указаны свойства обнаружения, над которым вы работаете. Например, MD5 файла из обнаружения.

Информация в блоке Правило IDS

В блоке **Правило IDS** отображается информация об обнаружении, выполненном технологией IDS (Intrusion Detection System), в формате матрицы HEX-редактора.

HEX-редактор (англ. hex-editor), шестнадцатеричный редактор — приложение для редактирования данных, в котором данные представлены как последовательность байтов.

В верхней части матрицы отображается длина правила IDS.

В левой части матрицы отображаются данные правила в текстовом формате.

В разделе **Содержание правила** блока **Правило IDS** отображается заголовок правила IDS и данные IDS-обнаружения в формате Suricata. Например, могут отображаться данные о направлении трафика (`flow`), метод HTTP-запроса (`http_method`), HTTP-заголовок (`http_header`), идентификатор безопасности (`sid`).

Информация в блоке Сетевое событие

В блоке **Сетевое событие** может отображаться следующая информация о ссылке на веб-сайт, открытой на компьютере:

- **Дата** и **Время** – дата и время сетевого события.
- **Метод** – тип HTTP-запроса, например, GET или POST.
- **IP источника** – IP-адрес компьютера, на котором была открыта ссылка на веб-сайт.
- **IP назначения** – IP-адрес компьютера, с которого была открыта ссылка на веб-сайт.
- **URL** – тип HTTP-запроса, например, GET или POST и URL-адрес веб-сайта.

По ссылке с URL-адресом раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на TIP по URL**.
- **Найти на TIP по имени домена**.
- **Найти события**.
- **Найти обнаружения**.
- **Скопировать значение в буфер**.

- **Агент пользователя** – информация о браузере, с помощью которого был загружен файл или была предпринята попытка загрузки файла, или была открыта ссылка на веб-сайт. Текстовая строка в составе HTTP-запроса, обычно содержащая название и версию браузера, а также название и версию операционной системы, установленной на компьютере пользователя.

Результаты проверки в Sandbox

В окне результатов проверки объекта в Sandbox могут отображаться следующие сведения об обнаружении:

- **Файл** – полное имя и путь проверенного файла.
- **Размер файла** – размер файла.
- **MD5** – MD5-хеш файла.

  По ссылке с **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на TIP**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.
- **Обнаружено** – одна или несколько категорий обнаруженных объектов. Например, если приложение обнаружило файл, зараженный вирусом Trojan-Downloader.JS.Cryptoload.ad, в поле **Обнаружено** будет указана категория Trojan-Downloader.JS.Cryptoload.ad для этого обнаружения.
- **Время обработки** – время выполнения проверки файла.
- **Версии баз** – версии баз модулей и компонентов Kaspersky Anti Targeted Attack Platform, выполнивших обнаружение.

Кнопка **Новое правило запрета** в правом верхнем углу окна позволяет запретить запуск файла (см. раздел "Работа с политиками (правилами запрета)" на стр. 486).

Информация о результатах исследования поведения файла приводится для каждой операционной системы, в которой компонент Sandbox выполнил проверку. Для операционной системы Windows 7 (64-разрядная) вы можете просмотреть журналы активности файла для двух режимов проверки компонента Sandbox – **Режим быстрой проверки** и **Режим ведения полного журнала**.

Для каждого режима проверки могут быть доступны следующие журналы активности:

- **Список активностей** – действия файла внутри операционной системы.
- **Дерево активностей** – графическое представление процесса исследования файла.
- **Журнал HTTP-активности** – журнал HTTP-активности файла. Содержит следующую информацию:

- **IP назначения** – IP-адрес, на который файл пытается перейти из операционной системы.
- **Метод** – метод HTTP-запроса, например, GET или POST.
- **URL** – URL-адрес ссылки на веб-сайт, которую файл пытается открыть из операционной системы.

По ссылкам в столбце **IP назначения** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на TIP**.
- **Найти события**.
- **Найти обнаружения**.
- **Скопировать значение в буфер**.

По ссылкам в столбце **URL** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на TIP по URL**.
- **Найти на TIP по имени домена**.
- **Найти события**.
- **Найти обнаружения**.
- **Скопировать значение в буфер**.

- **Журнал действий IDS** – журнал сетевой активности файла. Содержит следующую информацию:
  - **IP источника** – IP-адрес хоста, на котором хранится файл.
  - **IP назначения** – IP-адрес, на который файл пытается перейти из операционной системы.
  - **Метод** – метод HTTP-запроса, например, GET или POST.
  - **URL** – URL-адрес ссылки на веб-сайт, которую файл пытается открыть из операционной системы.

  По ссылкам в столбце **IP назначения** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на TIP**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Скопировать значение в буфер**.

  По ссылкам в столбце **URL** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на TIP по URL**.
  - **Найти на TIP по имени домена**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Скопировать значение в буфер**.
- **Журнал DNS-активности** – журнал DNS-активности файла. Содержит следующую информацию:

- Тип запроса (Request или Response)
- **DNS-имя** – доменное имя сервера.
- **Тип** – тип DNS-запроса (например, A или CNAME).
- **Хост** – имя хоста или IP-адрес, с которым осуществлялось взаимодействие.

  По ссылкам в столбцах **DNS-имя** и **Хост** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на TIP**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Скопировать значение в буфер**.

Кнопка **Скачать полный журнал** в нижней части каждого из режимов проверки **Режим быстрой проверки** и **Режим ведения полного журнала** позволяет скачать журнал исследования поведения файла в каждой операционной системе на компьютер.

Результаты IOC-проверки

В зависимости от типа обработанного объекта, в окне результатов поиска индикаторов компрометации могут отображаться следующие данные:

- **ARP-протокол**:
  - IP-адрес из ARP-таблицы.
  - Физический адрес из ARP-таблицы.
- **DNS-запись**:
  - Тип и имя записи DNS.
  - IP-адрес защищаемого компьютера.
- **Событие в журнале Windows**:
  - Идентификатор записи в журнале событий.
  - Имя источника данных в журнале.
  - Имя журнала.
  - Учетная запись пользователя.
  - Время события.
- **Файл**:
  - MD5-хеш файла.
  - SHA256-хеш файла.
  - Полное имя файла (включая путь).
  - Размер файла.
- **Порт**:
  - Удаленный IP-адрес, с которым было установлено соединение в момент проверки.

  - Удаленный порт, с которым было установлено соединение в момент проверки.
  - IP-адрес локального адаптера.
  - Порт, открытый на локальном адаптере.
  - Протокол в виде числа (в соответствии со стандартом IANA).
- **Процесс**:
  - Имя процесса.
  - Аргументы процесса.
  - Путь к файлу процесса.
  - Windows идентификатор (PID) процесса.
  - Windows идентификатор (PID) родительского процесса.
  - Имя учетной записи пользователя, запустившего процесс.
  - Дата и время запуска процесса.
- **Служба**:
  - Имя службы.
  - Описание службы.
  - Путь и имя DLL-службы (для svchost).
  - Путь и имя исполняемого файла службы.
  - Windows идентификатор (PID) службы.
  - Тип службы (например, драйвер ядра или адаптер).
  - Статус службы.
  - Режим запуска службы.
- **Пользователь**:
  - Имя учетной записи пользователя.
- **Том**:
  - Наименование тома.
  - Буква тома.
  - Тип тома.
- **Реестр**:
  - Значение реестра Windows.
  - Значение куста реестра.
  - Путь к ключу реестра (без куста и без имени значения).
  - Параметр реестра.
- **Переменные окружения**:
  - Физический адрес (MAC) защищаемого компьютера.
  - Система (окружение).

- Имя ОС с версией.
- Сетевое имя защищаемого устройства.
- Домен или группа, к которой принадлежит защищаемый компьютер.

В разделе **IOC** отображается структура IOC-файла. При совпадении обработанного объекта с одним из условий IOC-правила, это условие подсвечивается. Если обработанный объект совпадает с несколькими условиями, выделяется текст всей ветки.

Информация в блоке Хосты

В блоке **Хосты** отображается следующая информация о хостах, на которых сработало правило TAA (IOA):

- **Имя хоста** – IP-адрес или доменное имя компьютера, на котором произошло событие. По ссылке открывается раздел **Поиск угроз** с условием поиска, содержащим ID выбранного правила и выбранный хост.
- **IP** – IP-адрес компьютера, на котором произошло событие.

  Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный компьютеру на момент создания или обновления обнаружения.

  Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес компьютера не отображается.

- **Количество событий** – количество событий, произошедших на хосте.
- **Найти события**. По ссылке открывается раздел **Поиск угроз** с условием поиска, содержащим ID выбранного правила.

Информация в блоке Журнал изменений

В блоке **Журнал изменений** может отображаться следующая информация об обнаружении:

- Дата и время изменения обнаружения.
- Автор изменений.

  Например, **Система** или имя пользователя приложения.

- Изменение, произошедшее с обнаружением.

  Например, обнаружению может быть присвоена принадлежность группе VIP, или оно может быть отмечено как обработанное.

Отправка данных об обнаружении

Вы можете предоставить в "Лабораторию Касперского" данные об обнаружении (кроме технологий URL Reputation и IOC) для дальнейшего исследования.

Для этого необходимо скопировать данные об обнаружении в буфер обмена, а затем отправить их в "Лабораторию Касперского" по электронной почте.

Данные об обнаружении могут содержать данные о вашей организации, которые вы считаете конфиденциальными. Вам необходимо самостоятельно согласовать отправку этих данных для дальнейшего исследования в "Лабораторию Касперского" со Службой безопасности вашей организации.

► *Чтобы скопировать данные об обнаружении в буфер обмена:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Левой клавишей мыши нажмите на строку с тем обнаружением, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией об обнаружении.

3. Нажмите на ссылку **Предоставить данные об обнаружении в "Лабораторию Касперского"** в нижней части окна с информацией об обнаружении.

   Откроется окно **Подробнее**.

4. Просмотрите данные об обнаружении для отправки в "Лабораторию Касперского".

5. Если вы хотите скопировать эти данные, нажмите на кнопку **Скопировать в буфер**.

   Данные об обнаружении будут скопированы в буфер обмена. Вы сможете отправить их в "Лабораторию Касперского" для дальнейшего исследования.

Действия пользователей над обнаружениями

При работе в веб-интерфейсе приложения под учетной записью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** вы можете выполнять следующие действия над обнаружениями:

- Назначать обнаружение себе или другому пользователю веб-интерфейса приложения.

  Вы можете просмотреть все обнаружения, назначенные определенному пользователю, используя фильтр обнаружений по состоянию их обработки пользователем (см. раздел "Фильтрация и поиск обнаружений по состоянию их обработки пользователем" на стр. 341).

- Отметить обнаружение как обработанное.

  Вы можете просмотреть все обнаружения, обработанные определенным пользователем, используя фильтр обнаружений по состоянию их обработки пользователем (см. раздел "Фильтрация и поиск обнаружений по состоянию их обработки пользователем" на стр. 341).

- Добавить комментарий к обнаружению.

  Вы можете найти обнаружения, содержащие комментарий, по ключевым словам комментария, используя фильтр обнаружений по полученной информации (см. раздел "Фильтрация и поиск обнаружений по полученной информации" на стр. 338).

- Присвоить обнаружению статус VIP.

  Это действие доступно только пользователям с ролью **Старший сотрудник службы безопасности**. Пользователи с этой ролью могут просмотреть все обнаружения со статусом VIP,

используя фильтр обнаружений по наличию статуса VIP (см. раздел "Фильтрация обнаружений по наличию статуса VIP" на стр. 335).

Пользователи с ролью **Аудитор** могут просматривать информацию об обнаружениях без возможности редактирования.

В этом разделе

Назначение обнаружений определенному пользователю 363
Отметка о завершении обработки одного обнаружения 364
Отметка о завершении обработки обнаружений 365
Изменение статуса VIP обнаружений 365
Добавление комментария к обнаружению 366

Назначение обнаружений определенному пользователю

Пользователи с ролями **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** могут назначить обнаружение или несколько обнаружений себе или другому пользователю веб-интерфейса приложения с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности**.

► *Чтобы назначить обнаружение себе или другому пользователю веб-интерфейса приложения:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Установите флажок напротив обнаружения или обнаружений, которые вы хотите назначить себе или другому пользователю.

   Вы можете установить флажок в заголовке таблицы, чтобы выбрать все обнаружения.

3. В появившейся панели в нижней части окна нажатием на стрелку справа от кнопки **Назначить** раскройте список пользователей.

4. Выберите пользователя, которому вы хотите назначить обнаружения.

   Откроется окно подтверждения действия. Вы также можете оставить комментарий, который отобразится в истории изменения обнаружения.

5. Нажмите на кнопку **Продолжить**.

Обнаружения будут назначены выбранному пользователю.

Вы можете просмотреть все обнаружения, назначенные определенному пользователю, используя фильтр обнаружений по состоянию их обработки пользователем (см. раздел "Фильтрация и поиск обнаружений по состоянию их обработки пользователем" на стр. 341).

Пользователи с ролью **Аудитор** не могут назначать обнаружения себе или другим пользователям веб-интерфейса приложения. Пользователи с ролями **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** также не могут назначать обнаружения пользователям с ролью **Аудитор**.

Отметка о завершении обработки одного обнаружения

► *Чтобы отметить в таблице обнаружений одно обнаружение, назначенное вам, как обработанное:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. В столбце **Состояние** того обнаружения, которое вы хотите отметить как обработанное, левой клавишей мыши нажмите на ваше имя пользователя.
3. В списке действий выберите **Закрыть обнаружение**.

Обнаружение будет отмечено как обработанное.

► *Чтобы отметить обнаружение как обработанное в процессе работы с этим обнаружением, выполните следующие действия:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Откройте обнаружение, которое вы хотите отметить как обработанное.

   Раскройте список действий. В правом верхнем углу окна нажмите на стрелку справа от кнопки со статусом обнаружения.

   Откроется список действий.

3. В списке действий выберите **Закрыть обнаружение**.

Обнаружение будет отмечено как обработанное. Если обнаружение было назначено другому пользователю, оно будет отмечено как обработанное вами.

Вы можете просмотреть все обнаружения, обработанные определенным пользователем, используя фильтр обнаружений по состоянию их обработки пользователем (см. раздел "Фильтрация и поиск обнаружений по состоянию их обработки пользователем" на стр. 341).

Если в течение суток (с 00:00 до 23:59) поступит обнаружение по технологии TAA (IOA), IDS, URL, аналогичное обработанному, приложение либо создаст новое обнаружение, либо обновит информацию в идентичном обнаружении со статусом **Новое** или **В обработке**.
Для пользователей с ролью **Аудитор** недоступны функции назначения и обработки обнаружений.

Отметка о завершении обработки обнаружений

► *Чтобы отметить одно или несколько обнаружений как обработанные:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Установите флажки напротив тех обнаружений, которые вы хотите отметить как обработанные.

   Вы можете установить флажок в заголовке таблицы, чтобы выбрать все обнаружения.

3. В появившейся панели в нижней части окна нажмите на кнопку **Закрыть обнаружение**.

   Откроется окно подтверждения действия.

   Вы также можете оставить комментарий, который отобразится в истории изменения обнаружения.

4. Нажмите на кнопку **Продолжить**.

Выбранные обнаружения будут отмечены как обработанные. Если обнаружения были назначены другим пользователям, они будут отмечены как обработанные вами.

Вы можете просмотреть все обработанные обнаружения, используя фильтр обнаружений по состоянию их обработки пользователем (см. раздел "Фильтрация и поиск обнаружений по состоянию их обработки пользователем" на стр. 341).

Если в течение суток (с 00:00 до 23:59) поступит обнаружение по технологии TAA (IOA), IDS, URL, аналогичное обработанному, приложение либо создаст новое обнаружение, либо обновит информацию в идентичном обнаружении со статусом **Новое** или **В обработке**.
Для пользователей с ролью **Аудитор** недоступны функции назначения и обработки обнаружений.

Изменение статуса VIP обнаружений

Пользователи с ролью **Старший сотрудник службы безопасности** могут присваивать обнаружениям статус VIP и лишать обнаружения статуса VIP.

► *Чтобы изменить статус VIP для обнаружений:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Установите флажки напротив обнаружений,для которых вы хотите изменить статус VIP.

   Вы можете установить флажок в заголовке таблицы, чтобы выбрать все обнаружения.

3. Выполните одно из следующих действий:

   - Если вы хотите присвоить обнаружениям статус VIP, в появившейся панели в нижней части окна нажмите на кнопку **Присвоить статус VIP**.
   - Если вы хотите лишить обнаружения статуса VIP, в появившейся панели в нижней части окна в раскрывающемся списке **Присвоить статус VIP** выберите **Лишить статуса VIP**.

   Откроется окно подтверждения действия.

   Вы также можете оставить комментарий, который отобразится в истории изменения обнаружения.

4. Нажмите на кнопку **Продолжить**

   Статус VIP для обнаружений будет изменен.

Пользователи с ролью **Старший сотрудник службы безопасности** и **Аудитор** могут просмотреть все обнаружения со статусом VIP, используя фильтр обнаружений по наличию статуса VIP (см. раздел "Фильтрация обнаружений по наличию статуса VIP" на стр. 335).

Добавление комментария к обнаружению

Пользователи с ролями **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** могут добавить комментарий к обнаружению.

► *Чтобы добавить комментарий к обнаружению:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Выберите обнаружение, к которому вы хотите добавить комментарий.

   Откроется окно с информацией об обнаружении.

3. В поле добавления комментария под блоком **Журнал изменений** введите комментарий к обнаружению.

4. Нажмите на кнопку **Добавить**.

   Комментарий к обнаружению будет добавлен и отобразится в блоке **Журнал изменений** этого обнаружения.

Вы можете найти обнаружения, содержащие комментарий, по ключевым словам комментария, используя фильтр обнаружений по полученной информации (см. раздел "Фильтрация и поиск обнаружений по полученной информации" на стр. 338).

Пользователи с ролью **Аудитор** могут просматривать комментарии к обнаружениям без возможности редактирования.

Поиск угроз по базе событий

При работе в веб-интерфейсе приложения вы можете формировать поисковые запросы и использовать IOC-файлы для поиска угроз по базе событий в рамках тех тенантов, к данным которых у вас есть доступ.

Для формирования поисковых запросов по базе событий вы можете использовать *режим конструктора* или *режим исходного кода*.

В режиме конструктора (см. раздел "Поиск событий в режиме конструктора" на стр. 367) вы можете создавать и изменять поисковые запросы с помощью раскрывающихся списков с вариантами типа значения поля и операторов.

В режиме исходного кода (см. раздел "Поиск событий в режиме исходного кода" на стр. 371) вы можете создавать и изменять поисковые запросы с помощью текстовых команд.

Вы можете загрузить IOC-файл (см. раздел "Загрузка IOC-файла и поиск событий по условиям, заданным в IOC-файле" на стр. 376) и искать события по условиям, заданным в этом IOC-файле.

Пользователи с ролью **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности** также могут создавать правила TAA (IOA) (см. раздел "Создание правила TAA (IOA) на основе условий поиска событий" на стр. 377) на основе условий поиска событий.

В этом разделе

Поиск событий в режиме конструктора 367

Поиск событий в режиме исходного кода 371

Сортировка событий в таблице 373

Изменение условий поиска событий 374

Поиск событий по результатам их обработки в приложениях EPP 374

Загрузка IOC-файла и поиск событий по условиям, заданным в IOC-файле 376

Создание правила TAA (IOA) на основе условий поиска событий 377

Поиск событий в режиме конструктора

► *Чтобы задать условия поиска событий в режиме конструктора:*

1. В окне веб-интерфейса приложения выберите раздел **Поиск угроз**, закладку **Конструктор**.

   Откроется форма поиска событий.

2. В раскрывающемся списке выберите критерий для поиска событий.

   Вы можете посмотреть описание критериев для поиска событий в разделе Критерии для поиска событий (на стр. 368).

3. В раскрывающемся списке выберите оператор.

   Вы можете посмотреть список доступных операторов в разделе Операторы (на стр. 371).

   Для каждого типа значения поля будет доступен свой релевантный набор операторов. Например, при выборе типа значения поля **EventType** будут доступны операторы **=** и **!=**.

4. В зависимости от выбранного типа значения поля выполните одно из следующих действий:

   - Укажите в поле один или несколько символов, по которым вы хотите выполнить поиск событий.
   - В раскрывающемся списке выберите вариант значения поля, по которому вы хотите выполнить поиск событий.

   Например, для поиска полного совпадения по имени пользователя введите имя пользователя.

5. Если вы хотите добавить новое условие, используйте логический оператор **AND** или **OR** и повторите действия по добавлению условия.

6. Если вы хотите добавить группу условий, нажмите на кнопку **Group** и повторите действия по добавлению условий.

7. Если вы хотите удалить группу условий, нажмите на кнопку **Remove group**.

8. Если вы хотите выполнить поиск событий за определенный период, в раскрывающемся списке **За все время** выберите один из следующих периодов поиска событий:
   - **За все время**, если вы хотите, чтобы приложение отображало в таблице события, найденные за все время.
   - **Прошедший час**, если вы хотите, чтобы приложение отображало в таблице события, найденные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы приложение отображало в таблице события, найденные за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы приложение отображало в таблице события, найденные за указанный вами период.
9. Если вы выбрали **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения событий.
   b. Нажмите на кнопку **Применить**.

   Календарь закроется.
10. Нажмите на кнопку **Найти**.

    Отобразится таблица событий, соответствующих условиям поиска.

    Если вы используете режим распределенного решения и мультитенантности, отобразятся уровни группировки найденных событий: Сервер – Названия тенантов – Имена серверов.
11. Нажмите на имя того сервера, события которого вы хотите просмотреть.

Отобразится таблица хостов выбранного сервера. Уровни группировки событий отобразятся над таблицей.

Критерии для поиска событий

Для поиска событий доступны следующие критерии:

- **Общие сведения**:
  - Host – имя хоста.
  - HostIP – IP-адрес хоста.
  - EventType – тип события.
  - UserName – имя пользователя.
  - OsFamily – семейство операционной системы.
  - OsVersion – версия операционной системы, используемой на хосте.
- **Свойства ТАА**:
  - IOAId – идентификатор правила ТАА (IOA).
  - IOATag – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила ТАА (IOA), по которому было выполнено обнаружение.
  - IOATechnique – техника MITRE.
  - IOATactics – тактика MITRE.

  - IOAImportance – степень важности, присвоенная событию, выполненному по этому правилу ТАА (IOA).
  - IOAConfidence – уровень надежности в зависимости от вероятности ложных срабатываний правила.
- **Свойства файла**:
  - CreationTime – время создания события.
  - FileName – имя файла.
  - FilePath – путь к директории, в которой располагается файл.
  - FileFullName – полный путь к файлу. Включает путь к директории и имя файла.
  - ModificationTime – время изменения файла.
  - FileSize – размер файла.
  - MD5 – MD5-хеш файла.
  - SHA256 – SHA256-хеш файла.
  - SimilarDLLPath – вредоносная DLL, помещенная в директорию по стандартному пути обхода, чтобы система загрузила ее раньше, чем исходную DLL.
- **Процессы Linux**:
  - LogonRemoteHost – IP-адрес хоста, с которого был выполнен удаленный вход.
  - RealUserName – имя пользователя, назначенное ему при регистрации в системе.
  - EffectiveUserName – имя пользователя, которое было использовано для входа в систему.
  - Environment – переменные окружения.
  - ProcessType – тип процесса.
  - OperationResult – результат операции.
- **Запущен процесс**:
  - PID – идентификатор процесса.
  - ParentFileFullName – путь к файлу родительского процесса.
  - ParentMD5 – MD5-хеш файла родительского процесса.
  - ParentSHA256 – SHA256-хеш файла родительского процесса.
  - StartupParameters – параметры запуска процесса.
  - ParentPID – идентификатор родительского процесса.
- **Удаленное соединение**:
  - HTTPMethod – метод HTTP-запроса. Например, Get, Post или Connect.
  - ConnectionDirection – направление соединения (входящее или исходящее).
  - LocalIP – IP-адрес локального компьютера, с которого была произведена попытка удаленного соединения.
  - LocalPort – порт локального компьютера, с которого была произведена попытка удаленного соединения.

- RemoteHostName – имя компьютера, на который была произведена попытка удаленного соединения.
- RemoteIP – IP-адрес компьютера, на который была произведена попытка удаленного соединения.
- RemotePort – порт компьютера, на который была произведена попытка удаленного соединения.
- URl – адрес ресурса, к которому произведен запрос HTTP.

- **Изменение в реестре**:
  - RegistryKey – путь к ключу реестра.
  - RegistryValueName – имя параметра реестра.
  - RegistryValue – значение параметра реестра.
  - RegistryOperationType – тип операции с реестром.
  - RegistryPreviousKey – предыдущий путь к ключу реестра.
  - RegistryPreviousValue – предыдущее имя параметра реестра.
- **Журнал событий ОС**:
  - WinLogEventID – идентификатор типа события безопасности в журнале Windows.
  - LinuxEventType – тип события. Данный критерий используется для операционных систем Linux и macOS.
  - WinLogName – имя журнала.
  - WinLogEventRecordID – идентификатор записи в журнале.
  - WinLogProviderName – идентификатор системы, записавшей событие в журнал.
  - WinLogTargetDomainName – доменное имя удаленного компьютера.
  - WinLogObjectName – имя объекта, инициировавшего событие.
  - WinlogPackageName – имя пакета, инициировавшего событие.
  - WinLogProcessName – имя процесса, инициировавшего событие.
- **Обнаружение и результат обработки**:
  - DetectName – имя обнаруженного объекта.
  - RecordID – идентификатор сработавшего правила.
  - ProcessingMode – режим проверки.
  - ObjectName – имя объекта.
  - ObjectType – тип объекта.
  - ThreatStatus – режим обнаружения.
  - UntreatedReason – статус обработки события.
  - ObjectContent (for AMSI events too) – содержание скрипта, переданного на проверку.
  - ObjectContentType (for AMSI events too) – тип содержимого скрипта.
- **Интерактивный ввод команд в консоли**:
  - InteractiveInputText – текст, введенный в командную строку.

- InteractiveInputType – тип ввода (консоль или канал).
- **Изменен файл**:
  - FileOperationType – тип операции с файлом.
  - FilePreviousPath – путь к директории, в которой файл располагался ранее.
  - FilePreviousFullName – полное имя файла, включающее предыдущий путь к директории, в которой файл располагался ранее, и / или предыдущее имя файла.
  - DroppedFileType – тип измененного файла.

Операторы

Доступны следующие операторы:

- **=**.
- **!=**.
- **CONTAINS**.
- **!CONTAINS**.
- **STARTS**.
- **!STARTS**.
- **ENDS**.
- **!ENDS**.
- **>**.
- **<**.

Поиск событий в режиме исходного кода

► *Чтобы задать условия поиска событий в режиме исходного кода:*

1. В окне веб-интерфейса приложения выберите раздел **Поиск угроз**, вкладку **Редактор кода**.

   Откроется форма с полем ввода условий поиска событий в режиме исходного кода.

2. Введите условия поиска событий, используя критерии (см. раздел "Критерии для поиска событий" на стр. 368), операторы (на стр. 371), логические операторы `OR` и `AND`, а также скобки для создания групп условий.

   Условие поиска должно соответствовать следующему синтаксису: `<критерий> <оператор> <значение критерия>`.

Пример:

```
EventType = "filechange"
AND (
    FileName CONTAINS "example"
    OR UserName = "example"
)
```

3. Если вы хотите скрыть специальные символы разделителей строк в окне редактирования, нажмите на кнопку **Перевести спецсимволы в переносы строк** . Если вы хотите отобразить специальные символы разделителей строк, нажмите на кнопку **Перевести переносы строк в спецсимволы** .

   При использовании сложного условия поиска, состоящего из нескольких значений критерия, каждое значение критерия должно находиться на новой строке в окне редактирования исходного кода. Для отображения переноса на новую строку в Kaspersky Anti Targeted Attack Platform используются специальные символы разделителей строк (^r ^n). Вам необходимо контролировать правильность расстановки специальных символов разделителей строк для выполнения корректного поиска событий.

4. Если вы хотите выполнить поиск событий за определенный период, нажмите на кнопку **За все время** и выберите один из следующих периодов поиска событий:
   - **За все время**, если вы хотите, чтобы приложение отображало в таблице события, найденные за все время.
   - **Прошедший час**, если вы хотите, чтобы приложение отображало в таблице события, найденные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы приложение отображало в таблице события, найденные за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы приложение отображало в таблице события, найденные за указанный вами период.
5. Если вы выбрали **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения событий.
   b. Нажмите на кнопку **Применить**.

   Календарь закроется.
6. Нажмите на кнопку **Найти**.

   Отобразится таблица событий, соответствующих условиям поиска.

   Если вы используете режим распределенного решения и мультитенантности, отобразятся уровни группировки найденных событий: **Сервер** – Названия тенантов – Имена серверов.
7. Нажмите на имя того сервера, события по которому вы хотите просмотреть.

   Отобразится таблица хостов выбранного сервера. Уровни группировки событий отобразятся над таблицей.

Сортировка событий в таблице

Вы можете сортировать события в таблице по столбцам **Время события**, **Тип события**, **Хост** и **Имя пользователя**.

► *Чтобы отсортировать события в таблице событий:*

1. В окне веб-интерфейса приложения выберите раздел **Поиск угроз**.

   Откроется окно **Поиск угроз**.

2. Задайте условия для поиска событий в режиме конструктора (см. раздел "Поиск событий в режиме конструктора" на стр. 367) или режиме исходного кода (см. раздел "Поиск событий в режиме исходного кода" на стр. 371).

   Отобразится таблица событий, соответствующих условиям поиска.

3. Если вы хотите отсортировать события по времени, справа от названия столбца **Время события** нажмите на один из значков:
   - ↑ – новые события отобразятся вверху таблицы.
   - ↓ – старые события отобразятся вверху таблицы.
4. Если вы хотите отсортировать события по названию типов событий, справа от названия столбца **Тип события** нажмите на один из значков:
   - ↑ – сортировка выполнится по алфавиту А–Я.
   - ↓ – сортировка выполнится по алфавиту Я–А.
5. Если вы хотите отсортировать события по именам хостов, на которых были выполнены обнаружения, справа от названия столбца **Хост** нажмите на один из значков:
   - ↑ – сортировка выполнится по алфавиту А–Я.
   - ↓ – сортировка выполнится по алфавиту Я–А.
6. Если вы хотите отсортировать события по именам пользователей хостов, справа от названия **Имя пользователя** нажмите на один из значков:
   - ↑ – сортировка выполнится по алфавиту А–Я.
   - ↓ – сортировка выполнится по алфавиту Я–А.
7. Если вы хотите сгруппировать события по именам хостов или по названию типов событий, выберите в раскрывающемся списке **Группировать по** одно из значений:
   - **Группировать по имени хоста**, если хотите сгруппировать события по именам хостов.
   - **Группировать по типу события**, если хотите сгруппировать события по названиям типов событий.

   Если события были отсортированы по полю **Хост** или **Тип события**, при группировке событий по аналогичному признаку результат сортировки сбрасывается. Чтобы вернуться к результатам сортировки, выберите в раскрывающемся списке **Группировать по** значение **Группировать по**.

По умолчанию события в таблице отсортированы по времени: новые события располагаются вверху таблицы.
Вы можете отсортировать события только по одному признаку.

При сортировке по типу события на русском языке события сортируются в соответствии с внутренним наименованием типа события на английском языке.

Изменение условий поиска событий

► *Чтобы изменить условия поиска событий, выполните следующие действия в разделе **Поиск угроз** окна веб-интерфейса приложения:*

1. Нажмите на форму с условиями поиска событий в верхней части окна.
2. Выберите одну из следующих закладок:
   - **Конструктор**, если вы хотите изменить условия поиска событий в режиме конструктора.
   - **Редактор кода**, если вы хотите изменить условия поиска событий в режиме исходного кода.
3. Внесите необходимые изменения.
4. Нажмите на одну из следующих кнопок:
   - **Обновить**, если вы хотите обновить текущий поиск событий новыми условиями.
   - **Новый поиск**, если вы хотите выполнить новый поиск событий.

Отобразится таблица событий, соответствующих условиям поиска.

Поиск событий по результатам их обработки в приложениях EPP

► *Чтобы выполнить поиск событий по результатам их обработки в приложениях EPP в режиме конструктора:*

1. В окне веб-интерфейса приложения выберите раздел **Поиск угроз**, закладку **Конструктор**.

   Откроется форма поиска событий.
2. Если вы хотите выполнить поиск событий по статусу обработки, выполните следующие действия:
   a. В раскрывающемся списке критериев поиска событий в группе **Обнаружение и результат обработки** выберите критерий **ThreatStatus**.
   b. В раскрывающемся списке операторов сравнения выберите один из вариантов:
      - **=** (равно);
      - **!=** (не равно).
   c. В раскрывающемся списке статусов обработки события выберите один из вариантов:
      - **Объект не заражен**.
      - **Объект вылечен**.
      - **Ложное срабатывание**.
      - **Объект добавлен пользователем**.
      - **Объект добавлен в исключения**.
      - **Объект удален**.

- **Объект помещен на карантин**.
- **Объект не найден**.
- **Выполнен откат к предыдущему состоянию**.
- **Объект не поддается обработке**.
- **Объект не обработан**.
- **Обработка прервана**.
- **Неизвестно**.

3. Если вы хотите выполнить поиск событий по причинам, по которым они не были обработаны, выполните следующие действия:
   a. В раскрывающемся списке критериев поиска событий в группе **Обнаружение и результат обработки** выберите критерий **UntreatedReason**.
   b. В раскрывающемся списке операторов сравнения выберите один из вариантов:
      - **=** (равно);
      - **!=** (не равно).
   c. В раскрывающемся списке причин, по которым события не были обработаны, выберите один из вариантов:
      - **Объект уже был обработан**.
      - **Приложение работает в режиме Только отчет**.
      - **Не удалось создать резервную копию объекта**.
      - **Не удалось создать копию объекта**.
      - **Устройство не готово**.
      - **Объект заблокирован**.
      - **Нет прав на выполнение действия**.
      - **Объект невозможно вылечить**.
      - **Объект невозможно перезаписать**.
      - **Объект не найден**.
      - **Нет места на диске**.
      - **Обработка отменена**.
      - **Действие отложено**.
      - **Задача на обработку прервана**.
      - **Ошибка чтения данных**.
      - **Нет данных**.
      - **Объект является критическим системным**.
      - **Ошибка записи данных**.
      - **Запись данных не поддерживается**.
      - **Объект защищен от записи**.

4. Если вы хотите добавить новое условие, используйте логический оператор **AND** или **OR** и повторите действия по добавлению условия.
5. Если вы хотите добавить группу условий, нажмите на кнопку **Group** и повторите действия по добавлению условий.
6. Если вы хотите удалить группу условий, нажмите на кнопку **Remove group**.
7. Если вы хотите выполнить поиск событий за определенный период, в раскрывающемся списке **За все время** выберите один из следующих периодов поиска событий:
   - **За все время**, если вы хотите, чтобы приложение отображало в таблице события, найденные за все время.
   - **Прошедший час**, если вы хотите, чтобы приложение отображало в таблице события, найденные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы приложение отображало в таблице события, найденные за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы приложение отображало в таблице события, найденные за указанный вами период.
8. Если вы выбрали период отображения найденных событий **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения событий.
   b. Нажмите на кнопку **Применить**.

   Календарь закроется.
9. Нажмите на кнопку **Найти**.

Отобразится таблица событий, соответствующих условиям поиска.

Загрузка IOC-файла и поиск событий по условиям, заданным в IOC-файле

► *Чтобы загрузить IOC-файл и искать события по условиям, заданным в этом IOC-файле:*

1. В окне веб-интерфейса приложения выберите раздел **Поиск угроз**.

   Откроется форма поиска событий.
2. Нажмите на кнопку **Импортировать**.

   Откроется окно выбора файлов.
3. Выберите IOC-файл, который хотите загрузить, и нажмите на кнопку **Открыть**.

   IOC-файл загрузится.

   На закладке **Редактор кода** в форме с условиями поиска событий отобразятся условия, заданные в загруженном IOC-файле.

   Вы можете искать события по этим условиям. Вы также можете изменить условия, заданные в загруженном IOC-файле, или добавить условия поиска событий в режиме исходного кода (см. раздел "Поиск событий в режиме исходного кода" на стр. 371).

4. Если вы хотите выполнить поиск событий за определенный период, нажмите на кнопку **За все время** и выберите один из следующих периодов поиска событий:
   - **За все время**, если вы хотите, чтобы приложение отображало в таблице события, найденные за все время.
   - **Прошедший час**, если вы хотите, чтобы приложение отображало в таблице события, найденные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы приложение отображало в таблице события, найденные за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы приложение отображало в таблице события, найденные за указанный вами период.
5. Если вы выбрали период отображения найденных событий **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения событий.
   b. Нажмите на кнопку **Применить**.

   Календарь закроется.
6. Нажмите на кнопку **Найти**.

Отобразится таблица событий, соответствующих условиям, заданным в IOC-файле.

Создание правила TAA (IOA) на основе условий поиска событий

► *Чтобы создать правило TAA (IOA) на основе условий поиска событий:*

1. В окне веб-интерфейса приложения выберите раздел **Поиск угроз**.

   Откроется форма поиска событий.
2. Выполните поиск событий в режиме конструктора или режиме исходного кода.
3. Нажмите на кнопку **Сохранить как правило TAA (IOA)**.

   Откроется окно **Новое правило TAA (IOA)**.
4. В поле **Имя** введите имя правила.
5. Нажмите на кнопку **Сохранить**.

Условие поиска событий будет сохранено. В таблице правил TAA (IOA) раздела **Пользовательские правила**, в подразделе **TAA** веб-интерфейса отобразится новое правило с заданным именем.

Не рекомендуется в условиях поиска событий, сохраняемых как пользовательское правило TAA (IOA), использовать следующие поля:

- IOAId.
- IOATag.
- IOATechnique.
- IOATactics.
- IOAImportance.
- IOAConfidence.

На момент сохранения пользовательского правила TAA (IOA) в приложении может не быть событий, содержащих данные для этих полей. Когда события с этими данными появятся, пользовательское правило TAA (IOA), созданное ранее, не сможет разметить события по этим полям.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция создания правила TAA (IOA) на основе условий поиска событий недоступна.

Информация о событиях

Если вы используете режим распределенного решения и мультитенантности, при работе в веб-интерфейсе приложения вы можете просматривать информацию о событиях в рамках тех тенантов, к данным которых у вас есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса приложения" на стр. 200).

В информации о событиях отображаются локальные метки времени того компьютера с компонентом Endpoint Agent, на котором было обнаружено событие. Администратору приложения требуется контролировать актуальность времени на компьютерах с компонентом Endpoint Agent.

► *Чтобы включить отображение событий по всем тенантам, выполните следующие действия:*

1. В окне веб-интерфейса приложения выберите раздел **Поиск угроз**.
2. Включите переключатель **Искать по всем тенантам**.

В таблице событий отобразятся события по всем тенантам.

kaspersky

В этом разделе

Рекомендации по обработке событий....379
Информация о событиях в дереве событий....384
Просмотр таблицы событий....387
Настройка отображения таблицы событий....389
Просмотр информации о событии....390
Информация о событии Запущен процесс....390
Информация о событии Завершен процесс....394
Информация о событии Загружен модуль....397
Информация о событии Удаленное соединение....400
Информация о событии Правило запрета....402
Информация о событии Заблокирован документ....405
Информация о событии Изменен файл....407
Информация о событии Журнал событий ОС....412
Информация о событии Изменение в реестре....414
Информация о событии Прослушан порт....416
Информация о событии Загружен драйвер....418
Информация о событии Обнаружение....421
Информация о событии Результат обработки обнаружения....423
Информация о событии Интерпретированный запуск файла....426
Информация о событии AMSI-проверка....428
Информация о событии Интерактивный ввод команд в консоли....431

Рекомендации по обработке событий

В окне события в рамке между деревом событий и текстовой информацией для пользователей с ролью **Старший сотрудник службы безопасности** отображаются рекомендации по обработке этого события.

Вы можете выполнить следующие рекомендации:

- **Изолировать <имя хоста>** (см. раздел "**Выполнение рекомендации по изоляции хоста**" на стр. 381) – изолировать хост (см. раздел "Сетевая изоляция хостов с компонентом Endpoint Agent" на стр. 448) с компонентом Endpoint Agent, на котором обнаружено событие, от сети. Применяется для всех типов событий.
- **Создать правило запрета** (см. раздел "**Выполнение рекомендации по запрету запуска файла**" на стр. 382) – запретить запуск файла (см. раздел "Работа с политиками (правилами запрета)" на стр. 486), обнаруженного в событии. Применяется для всех типов событий кроме **Журнал событий ОС** и **Изменено имя хоста**.

- **Создать задачу** (см. раздел "**Выполнение рекомендации по созданию задачи**" на стр. 383) – создать задачу (см. раздел "Работа с задачами" на стр. 456). Применяется для всех типов событий кроме **Журнал событий ОС** и **Изменено имя хоста**.

Кроме того, вы можете выполнить действия по обработке события по ссылкам с именем файла, путем к файлу, MD5-хешем, SHA256-хешем файла и именем хоста при просмотре текстовой информации о событии в нижней части окна.

По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- Выполнить задачи:
  - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
  - **Завершить по уникальному PID** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
  - **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).
  - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Найти на TIP**.
- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 531).
- **Создать правило запрета** (см. раздел "**Сетевая изоляция хостов с компонентом Endpoint Agent**" на стр. 448).
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- Выполнить задачи:
  - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
  - **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).
  - **Поместить файл на карантин (см. раздел "Создание задачи помещения файла на карантин" на стр. 478).**
  - **Выполнить приложение** (см. раздел "**Создание задачи выполнения приложения**" на стр. 476).
- **Скопировать значение в буфер**.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** рекомендации по обработке событий не отображаются.

В этом разделе

Выполнение рекомендации по изоляции хоста 381
Выполнение рекомендации по запрету запуска файла 382
Выполнение рекомендации по созданию задачи 383

Выполнение рекомендации по изоляции хоста

► *Чтобы выполнить рекомендацию по изоляции хоста от сети:*

1. В рамке с рекомендациями выберите **Изолировать <имя хоста>**.

   Откроется окно параметров изоляции хоста из события, с которым вы работаете.
2. В поле **Отключить изоляцию через** введите количество часов от 1 до 9999, в течение которых будет действовать сетевая изоляция хоста.
3. В блоке параметров **Исключения для правила изоляции хоста** в списке **Направление трафика** выберите направление сетевого трафика, которое не должно быть заблокировано:
   - **Входящее/Исходящее**.
   - **Входящее**.
   - **Исходящее**.
4. В поле **IP** введите IP-адрес, сетевой трафик которого не должен быть заблокирован.

Если в роли компонента Endpoint Agent вы используете приложение Kaspersky Endpoint Agent, вы можете использовать прокси-сервер для соединения Kaspersky Endpoint Agent для Windows с Kaspersky Anti Targeted Attack Platform. При добавлении этого прокси-сервера в исключения сетевые ресурсы, к которым открыт доступ через прокси-сервер, также добавляются в исключения. Если в исключения добавлены сетевые ресурсы, соединение с которыми происходит через прокси-сервер, но при этом исключение для самого прокси-сервера не настроено, исключение не будет работать.

5. Если вы выбрали **Входящее** или **Исходящее**, в поле **Порты** введите порты подключения.
6. Если вы хотите добавить более одного исключения, нажмите на кнопку **Добавить** и повторите действия по заполнению полей **Направление трафика**, **IP** и **Порты**.
7. Нажмите на кнопку **Сохранить**.

Информация об изоляции хоста отобразится в разделе **Endpoint Agents** веб-интерфейса (см. раздел "Просмотр таблицы хостов с компонентом Endpoint Agent" на стр. 435).

Вы также можете создать правило сетевой изоляции по ссылке **Изолировать <имя хоста>** в информации об обнаружении (см. раздел «Просмотр информации об обнаружении» на стр. 351) и в разделе **Endpoint Agents** веб-интерфейса (см. раздел «Просмотр таблицы хостов с компонентом Endpoint Agent» на стр. 435).

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция изоляции хоста от сети недоступна.

Выполнение рекомендации по запрету запуска файла

► *Чтобы выполнить рекомендацию по запрету запуска файла:*

1. В рамке с рекомендациями выберите **Создать правило запрета**.

   Откроется окно создания правила запрета с MD5- или SHA256-хешем файла из события, с которым вы работаете.
2. Задайте значения следующих параметров:
   a. **Состояние** – состояние правила запрета:
      - Если вы хотите включить правило запрета, переведите переключатель в положение **Вкл**.
      - Если вы хотите отключить правило запрета, переведите переключатель в положение **Откл**.

   b. **Имя** – имя правила запрета.

   c. Если вы хотите, чтобы приложение выводило уведомление о срабатывании правила запрета пользователю компьютера, на который распространяется запрет, установите флажок **Показывать пользователю уведомление о блокировке запуска файла**.

   d. Если вы хотите изменить область применения правила запрета, настройте параметр **Запрет для**:
      - Если вы хотите применить правило запрета на всех хостах всех серверов, выберите вариант **Всех хостов**.

- Если вы хотите применить правило запрета на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите применить правило запрета.

  Этот вариант доступен только при включенном режиме распределенного решения и мультитенантности.

- Если вы хотите применить правило запрета на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

3. Нажмите на кнопку **Добавить**.

Запрет на запуск файла будет создан.

Информация о созданном запрете отобразится в разделе **Политики** веб-интерфейса (см. раздел "Просмотр таблицы правил запрета" на стр. 488).

Если вы установили флажок **Показывать пользователю уведомление о блокировке запуска файла**, при попытке запуска запрещенного файла пользователю будет показано уведомление о том, что сработало правило запрета запуска этого файла.
Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция запрета запуска файла недоступна.

Выполнение рекомендации по созданию задачи

► *Чтобы выполнить рекомендацию по созданию задачи:*

1. В рамке с рекомендациями по ссылке **Создать задачу** раскройте список типов задач.
2. Выберите один из типов задач:
   - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
   - **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).
   - **Запустить YARA-проверку** (см. раздел "**Создание задачи проверки хостов с помощью правил YARA**" на стр. 470).
   - **Управление службами** (см. раздел "**Создание задачи управления службами**" на стр. 473).
   - **Получить дамп памяти процесса** (см. раздел "**Создание задачи получения дампа памяти процесса**" на стр. 465).
   - **Получить метафайлы NTFS** (см. раздел "**Создание задачи получения метафайлов NTFS**" на стр. 464).
   - **Выполнить приложение** (см. раздел "**Создание задачи выполнения приложения**" на стр. 476).
   - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
   - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
   - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).
   - **Восстановить файл из карантина** (см. раздел "**Создание задачи восстановления файла из карантина**" на стр. 479).

Откроется окно создания задачи с предзаполненными данными (например, именем хоста, путем к файлу, MD5- или SHA256-хешем файла) из события, с которым вы работаете.

3. Если вы хотите изменить предзаполненные данные из события, внесите изменения в соответствующие поля.
4. Если вы хотите добавить комментарий к задаче, введите его в поле **Описание**.
5. Если вы создаете задачу **Завершить процесс**, **Удалить файл**, **Запустить YARA-проверку** или **Управление службами** и хотите изменить область применения задачи, настройте параметр **Задача для**:
   - Если вы хотите выполнить задачу на всех хостах всех серверов, выберите вариант **Всех хостов**.
   - Если вы хотите выполнить задачу на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите выполнить задачу.

     Этот вариант доступен только при включенном режиме распределенного решения и мультитенантности.
   - Если вы хотите выполнить задачу на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.
6. Нажмите на кнопку **Добавить**.

Задача будет создана.

Информация о созданной задаче отобразится в разделе **Задачи** веб-интерфейса (см. раздел "Просмотр таблицы задач" на стр. 457).

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция создания задачи недоступна.

Информация о событиях в дереве событий

Дерево событий отображается в верхней части окна информации о событии.

В дереве событий содержится следующая информация:

- Событие, информацию о котором вы просматриваете.

  Просматриваемое событие располагается справа.
- Родительский процесс.

  Родительский процесс располагается слева от просматриваемого события. Если для просматриваемого события нет родительского процесса, вместо него отображается имя хоста, на котором было зафиксировано просматриваемое событие (см. раздел "Просмотр информации о хосте в дереве событий" на стр. 386).

При нажатии на имя родительского процесса слева отображается процесс, который инициировал появление этого процесса и является родительским по отношению к нему. Если родительского процесса нет, отображается имя хоста.

Справа от имени каждого родительского процесса отображается общее количество событий, вызванных этим процессом. Вы можете просмотреть список событий (см. раздел "Просмотр информации о событиях, инициированных родительским процессом, в дереве событий" на стр. 385) и информацию о выбранном событии.

В этом разделе

Просмотр информации о родительском процессе в дереве событий 385

Просмотр информации о событиях, инициированных родительским процессом, в дереве событий 385

Просмотр информации о хосте в дереве событий 386

Просмотр информации о родительском процессе в дереве событий

► *Чтобы просмотреть информацию о родительском процессе для просматриваемого события:*

1. Выполните поиск событий в режиме конструктора или режиме исходного кода.

   Отобразится таблица событий.

2. Выберите событие, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией о событии. В верхней части окна отобразится дерево событий (см. раздел "Информация о событиях в дереве событий" на стр. 384).

3. Нажмите на имя родительского процесса.

   В нижней части окна на закладке **Сведения** отобразится информация о процессе, который является родительским по отношению к просматриваемому событию.

Просмотр информации о событиях, инициированных родительским процессом, в дереве событий

► *Чтобы просмотреть таблицу всех событий, инициированных родительским процессом:*

1. Выполните поиск событий в режиме конструктора или режиме исходного кода.

   Отобразится таблица событий.

2. Выберите событие, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией о событии. В верхней части окна информации о событии отобразится дерево событий (см. раздел "Информация о событиях в дереве событий" на стр. 384).

3. Нажмите на имя родительского процесса в дереве событий.

   В нижней части окна на закладке **Сведения** отобразится информация о событии, которое является родительским по отношению к просматриваемому событию.

4. Перейдите на закладку **События**.

   Отобразится таблица всех событий, инициированных родительским процессом. По умолчанию события в таблице отсортированы по времени: новые события располагаются вверху таблицы.

   Вы можете просмотреть информацию о событии, нажав на строку с этим событием. Узел события отобразится в дереве событий.

► *Чтобы просмотреть таблицу событий, сгруппированных по типу, выполните следующие действия:*

1. Выполните поиск событий в режиме конструктора или режиме исходного кода.

   Отобразится таблица событий.

2. Выберите событие, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией о событии. В верхней части окна информации о событии отобразится дерево событий.

3. Нажмите на раскрывающийся список справа от имени узла родительского процесса в дереве событий.

   Отобразится список всех событий, инициированных родительским процессом. По умолчанию события в списке сгруппированы по типу.

4. В дереве событий в раскрывающемся списка справа от имени родительского процесса выберите один из следующих элементов:

   - Если вы хотите просмотреть все события, инициированные родительским процессом, выберите **Все события**.

     Отобразится таблица всех событий, инициированных родительским процессом. По умолчанию события в таблице отсортированы по времени: новые события располагаются вверху таблицы.

   - Если вы хотите просмотреть все события одного типа, инициированные родительским процессом, выберите имя нужного типа событий.

     Отобразится таблица всех событий, инициированных родительским процессом и сгруппированных по типу.

   Вы можете просмотреть информацию о событии, нажав на строку с этим событием. Событие отобразится в дереве событий.

Просмотр информации о хосте в дереве событий

Если для просматриваемого события или родительского процесса нет процесса, инициировавшего его появление, вместо узла процесса в дереве событий отображается узел хоста, на котором было зафиксировано событие или был запущен родительский процесс.

► *Чтобы просмотреть информацию о хосте, на котором было зафиксировано событие или был запущен родительский процесс:*

1. Выполните поиск событий в режиме конструктора или режиме исходного кода.

   Отобразится таблица событий.

2. Выберите событие, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией о событии. В верхней части окна отобразится дерево событий (см. раздел "Информация о событиях в дереве событий" на стр. 384).

3. Нажмите на имя хоста в дереве событий.

   В нижней части окна отобразится информация о хосте, на котором было зафиксировано событие или был запущен родительский процесс.

Просмотр таблицы событий

Таблица событий отображается в разделе **Поиск угроз** окна веб-интерфейса приложения после выполнения поиска угроз по базе событий (см. раздел "Поиск угроз по базе событий" на стр. 366). Вы можете сортировать события (см. раздел "Сортировка событий в таблице" на стр. 373) в таблице по столбцам **Время события**, **Тип события**, **Хост** и **Имя пользователя**.

Если вы используете режим распределенного решения и мультитенантности, события в таблице сгруппированы по хостам выбранных серверов и тенантов.

В таблице событий содержится следующая информация:

1. **Время события** – дата и время обнаружения события.
2. **Тип события** – например, **Запущен процесс**.
3. **Имя хоста** – имя хоста, на котором было выполнено обнаружение.
4. **Сведения** – сведения о событии.
5. **Имя пользователя** – имя пользователя компьютера с компонентом Endpoint Agent, под учетной записью которого было обнаружено событие.

В таблице событий для каждого типа событий в столбце **Тип события** отображается свой набор данных в столбце **Сведения** (см. таблицу ниже).

*Таблица 37. Набор данных в столбце **Событие** для каждого типа событий в столбце **Сведения***

Тип события	Сведения
Запущен процесс	Имя файла процесса, который был запущен. SHA256- и MD5-хеш.
Загружен модуль	Имя динамической библиотеки, которая была загружена. SHA256- и MD5-хеш.
Удаленное соединение	URL-адрес, к которому была произведена попытка удаленного подключения. Имя файла, который пытался осуществить удаленное подключение.
Правило запрета	Имя файла приложения, запуск которого был заблокирован. SHA256- и MD5-хеш.
Заблокирован документ	Имя документа, запуск которого был заблокирован. SHA256- и MD5-хеш.
Изменен файл	Имя созданного файла. SHA256- и MD5-хеш.
Журнал событий ОС	Канал записи событий в системный журнал. Идентификатор типа события.
Изменение в реестре	Имя ключа в реестре. `<имя переменной в ключе>=<значение переменной>`.
Прослушан порт	Адрес сервера и порт. Имя файла процесса, который осуществляет прослушивание порта.
Загружен драйвер	Имя файла драйвера, который был загружен. SHA256- и MD5-хеш.
Обнаружение	Обнаружение.

Тип события	Сведения
Результат обработки обнаружения	Результат обработки обнаружения.
AMSI-проверка	Результат AMSI-проверки.
Интерпретированный запуск файла	Интерпретированный запуск файла.
Интерактивный ввод команд в консоли	Интерактивный ввод команд в консоли.

Если в роли компонента Endpoint Agent вы используете Kaspersky Endpoint Agent, то данные о событии **AMSI-проверка** доступны при интеграции Kaspersky Anti Targeted Attack Platform с Kaspersky Endpoint Agent для Windows версии 3.10 и выше и при интеграции Kaspersky Endpoint Agent с приложением Kaspersky Endpoint Security для Windows версий 11.5 и выше. Если приложение Kaspersky Endpoint Security для Windows не установлено на компьютер и не интегрирована с Kaspersky Endpoint Agent, информация о событии **AMSI-проверка** не записывается в базу событий и не отображается в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.
Если в роли компонента Endpoint Agent используется Kaspersky Endpoint Agent, сервер Central Node формирует событие **Обнаружение** и **Результат обработки обнаружения** на основе данных, полученных от приложений EPP. Если приложения EPP не установлены на компьютер и не интегрированы с Kaspersky Endpoint Agent, информация об этих событиях не записывается в базу событий и не отображается в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.

По ссылке с названием типа события, сведениями, дополнительной информацией и именем пользователя раскрывается список, в котором вы можете выбрать действие над объектом. В зависимости от значения в ячейке вы можете выполнить одно из следующих действий:

- Для всех значений в ячейке:
  - **Добавить в фильтр**.
  - **Исключить из фильтра**.
  - **Скопировать значение в буфер**.
- Имя хоста:
  - **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
  - **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
  - **Изолировать от сети** (см. раздел "**Сетевая изоляция хостов с компонентом Endpoint Agent**" на стр. 448).
- Имя файла:
  - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
  - **Завершить по уникальному PID** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).

- **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
- **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
- **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).
- **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).

- MD5-хеш:
  - **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
  - **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
  - **Найти на TIP**.
  - **Создать правило запрета**. (см. раздел "Работа с политиками (правилами запрета)" на стр. 486)
  - **Найти в Хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 531).
- SHA256-хеш:
  - **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
  - **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
  - **Найти на TIP**.
  - **Найти на virustotal.com**.
  - **Создать правило запрета**. (см. раздел "Работа с политиками (правилами запрета)" на стр. 486)
  - **Найти в Хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 531).

Настройка отображения таблицы событий

Вы можете настроить отображение столбцов, а также порядок их следования в таблице событий.

► *Чтобы настроить отображение таблицы событий:*

1. Выполните поиск событий в режиме конструктора или режиме исходного кода.

   Отобразится таблица событий.

2. В заголовочной части таблицы нажмите на кнопку ⚙.

   Отобразится окно **Настройка таблицы**.

3. Если вы хотите включить отображение столбца в таблице, установите флажок рядом с названием того параметра, который должен отображаться в таблице.

   Если вы не хотите, чтобы параметр отображался в таблице, снимите флажок.

   Должен быть установлен хотя бы один флажок.

4. Если вы хотите изменить порядок отображения столбцов в таблице, наведите курсор мыши на строку с нужным параметром, нажмите на кнопку ⠿ и переместите строку с параметром в нужное место.
5. Если вы хотите восстановить параметры отображения таблицы по умолчанию, нажмите на ссылку **По умолчанию**.
6. Нажмите на кнопку **Применить**.

Отображение таблицы событий будет настроено.

Просмотр информации о событии

► *Чтобы просмотреть информацию о событии:*

1. В окне веб-интерфейса приложения выберите раздел **Поиск угроз**, закладку **Конструктор** или **Редактор кода**.

   Откроется форма поиска событий.
2. Если вы используете режим распределенного решения и мультитенантности и хотите включить отображение событий по всем тенантам, включите переключатель **Искать по всем тенантам**.
3. Выполните поиск событий в режиме конструктора (см. раздел "Поиск событий в режиме конструктора" на стр. 367) или режиме исходного кода (см. раздел "Поиск событий в режиме исходного кода" на стр. 371).

   Отобразится таблица событий.
4. Выберите событие, информацию о котором вы хотите просмотреть.

Откроется окно с информацией о событии.

Информация о событии Запущен процесс

В окне с информацией о событиях типа **Запущен процесс** содержатся следующие сведения:

- Дерево событий (см. раздел "Информация о событиях в дереве событий" на стр. 384).
- Рекомендации по обработке события.
- Раздел **Запущен процесс**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Файл** – имя файла процесса.
  - **ID процесса** – идентификатор процесса.
  - **Параметры запуска** – параметры запуска процесса.

Если событие было записано в базу событий Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, вместо поля **Параметры запуска** отображается поле **Команда** – команда, с помощью которой был запущен процесс.

- **MD5** – MD5-хеш файла процесса.
- **SHA256** – SHA256-хеш файла процесса.
- **Размер** – размер файла процесса.
- **Время события** – время запуска процесса.
- **Время создания** – время создания файла процесса.
- **Время изменения** – время последнего изменения файла процесса.

- Раздел **Сведения**:
  - **Название приложения** – например, название операционной системы.
  - **Производитель** – например, производитель операционной системы.
  - **Описание файла** – например, Example File.
  - **Исходное имя файла** – например, ExampleFile.exe.
  - **Получатель сертификата** – организация, выпустившая цифровой сертификат файла.
  - **Результат проверки подписи** – например, "Недействительна" или "OK".
  - **Свойства** – атрибут файла по классификации Windows. Например, A (архив), D (директория) или S (системный).

  Если событие было записано в базу событий приложением Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, в разделе **Сведения** также отображаются следующие поля:

  - **Свойства** – свойства файла процесса.
  - **Тип процесса** – например, exec.
  - **Переменные окружения** – переменные окружения процесса.
  - **Настоящее имя пользователя** – имя пользователя, назначенное при регистрации в системе.
  - **Настоящее имя группы** – группа, к которой принадлежит пользователь.
  - **Действующее имя пользователя** – имя пользователя, которое использовалось для входа в систему.
  - **Действующее имя группы** – группа, к которой принадлежит пользователь, чье имя использовалось для входа в систему.
  - **Имя пользователя-владельца** – имя пользователя, создавшего файл процесса.
  - **Имя группы-владельца** – название группы, пользователи которой могут изменить или удалить файл процесса.
  - **Разрешенные привилегии файла** – разрешения, которые могут использоваться для доступа к файлу процесса. Данное поле не отображается, если событие было записано приложением Kaspersky Endpoint Security для Mac.
  - **Наследуемые привилегии файла** – разрешения, которые есть у группы пользователей для выполнения операций с родительским каталогом файла процесса. Данное поле не отображается, если событие было записано приложением Kaspersky Endpoint Security для Mac.

- **Актуальные привилегии файла** – разрешения, которые актуальны для файла процесса на данный момент. Данное поле не отображается, если событие было записано приложением Kaspersky Endpoint Security для Mac.

- Раздел **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.
  - **ID процесса** – идентификатор родительского процесса.
  - **Параметры запуска** – параметры запуска родительского процесса.

    Если событие было записано в базу событий Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, вместо поля **Параметры запуска** отображается поле **Команда** – команда, с помощью которой был запущен родительский процесс.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором был запущен процесс.
  - **IP хоста** – IP-адрес хоста, на котором был запущен процесс.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.
  - **Тип учетной записи** – тип учетной записи, под которой был запущен процесс. Например, администратор.
  - **Тип входа в систему** – например, с помощью запущенной службы.
  - **Имя пользователя** – имя пользователя, запустившего процесс.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

    Если событие было записано в базу событий приложением Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, в разделе **Сведения о системе** также отображается поле **Вход с удаленного хоста** – имя хоста, с которого был совершен удаленный вход в систему.

По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- Выполнить задачи:
  - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
  - **Завершить по уникальному PID** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).

- **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
- **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).
- **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).

- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, по ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- Выполнить задачу **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- Выполнить задачи:
  - **Собрать данные** → **Файл** (см. раздел "**Создание задачи получения файла**" на стр. 460), **Форензика** (см. раздел "**Создание задачи сбора форензики**" на стр. 461), **Образ диска** (см. раздел "**Создание задачи получения образа диска**" на стр. 466), **Дамп памяти** (см. раздел "**Создание задачи получения дампа оперативной памяти**" на стр. 469).
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Поместить файл на карантин.**
  - **Выполнить приложение**.
- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, по ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- Выполнить задачи:
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
  - **Выполнить приложение** (см. раздел "**Создание задачи выполнения приложения**" на стр. 476).
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.

- **Найти обнаружения**.
- **Найти на TIP**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 531).
- **Создать правило запрета** (см. раздел "**Сетевая изоляция хостов с компонентом Endpoint Agent**" на стр. 448).
- **Скопировать значение в буфер**.

Информация о событии Завершен процесс

В окне с информацией о событиях типа **Завершен процесс** содержатся следующие сведения:

- Дерево событий (см. раздел "Информация о событиях в дереве событий" на стр. 384).
- Рекомендации по обработке события.
- Раздел **Завершен процесс**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Файл** – имя файла процесса.
  - **ID процесса** – идентификатор процесса.
  - **Параметры запуска** – параметры запуска процесса.

    Если событие было записано в базу событий Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, вместо поля **Параметры запуска** отображается поле **Команда** – команда, с помощью которой был запущен процесс.
  - **MD5** – MD5-хеш файла процесса.
  - **SHA256** – SHA256-хеш файла процесса.
  - **Размер** – размер файла процесса.

- **Время события** – время завершения процесса.
- Раздел **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.
  - **ID процесса** – идентификатор родительского процесса.
  - **Параметры запуска** – параметры запуска родительского процесса.

    Если событие было записано в базу событий Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, вместо поля **Параметры запуска** отображается поле **Команда** – команда, с помощью которой был запущен родительский процесс.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором был запущен процесс.
  - **IP хоста** – IP-адрес хоста, на котором был запущен процесс.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.
  - **Тип учетной записи** – тип учетной записи, под которой был завершен процесс. Например, администратор.
  - **Имя пользователя** – имя пользователя, запустившего процесс.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

  Если событие было записано в базу событий Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, в разделе **Сведения о системе** также отображается поле **Вход с удаленного хоста** – имя хоста, с которого был совершен удаленный вход в систему.

По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- Выполнить задачи:
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
  - **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).
  - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).
- **Скопировать значение в буфер**.

- В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, по ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:
- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- Выполнить задачу **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- Выполнить задачи:
  - **Собрать данные** → **Файл** (см. раздел "**Создание задачи получения файла**" на стр. 460), **Форензика** (см. раздел "**Создание задачи сбора форензики**" на стр. 461), **Образ диска** (см. раздел "**Создание задачи получения образа диска**" на стр. 466), **Дамп памяти** (см. раздел "**Создание задачи получения дампа оперативной памяти**" на стр. 469).
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Поместить файл на карантин.**
  - **Выполнить приложение**.
- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, по ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- Выполнить задачи:
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
  - **Выполнить приложение** (см. раздел "**Создание задачи выполнения приложения**" на стр. 476).
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- **Найти на TIP**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 531).
- **Создать правило запрета** (см. раздел "**Сетевая изоляция хостов с компонентом Endpoint Agent**" на стр. 448).
- **Скопировать значение в буфер**.

Информация о событии Загружен модуль

В окне с информацией о событиях типа **Загружен модуль** содержатся следующие сведения:

- Дерево событий (см. раздел "Информация о событиях в дереве событий" на стр. 384).
- Рекомендации по обработке события.
- Раздел **Загружен модуль**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Файл** – имя файла загруженного модуля.
  - **MD5** – MD5-хеш файла загруженного модуля.
  - **SHA256** – SHA256-хеш файла загруженного модуля.
  - **Размер** – размер загруженного модуля.
  - **Время события** – время загрузки модуля.
- Раздел **Сведения**:
  - **Название приложения** – например, название операционной системы.
  - **Производитель** – например, производитель операционной системы.
  - **Описание файла** – например, Example File.
  - **Исходное имя файла** – например, Example File.
  - **Получатель сертификата** – организация, выпустившая цифровой сертификат файла.
  - **Результат проверки подписи** – например, "Подпись недействительна" или "Подпись OK".
  - **Время создания** – время создания загруженного модуля.

- **Время изменения** – дата последнего изменения загруженного модуля.
- **Следующая по пути обхода DLL** – поле содержит путь к библиотеке DLL, которая могла быть загружена вместо существующей библиотеки.

  Поле отображается при выполнении следующих условий:

  - Источник загруженной библиотеки DLL не является доверенным.
  - В папке по стандартному пути обхода есть одноименная библиотека с другим хешем.

  Если в роли компонента Endpoint Agent вы используете Kaspersky Endpoint Agent, Kaspersky Anti Targeted Attack Platform получает данные, необходимые для заполнения поля **Следующая по пути обхода DLL**, только при интеграции Kaspersky Anti Targeted Attack Platform с Kaspersky Endpoint Agent для Windows версии 3.10. При интеграции приложения с предыдущими версиями Kaspersky Endpoint Agent указанное поле не будет отображаться в информации о событии.

- Раздел **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором был загружен модуль.
  - **IP хоста** – IP-адрес хоста, на котором был загружен модуль.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

  - **Имя пользователя** – имя пользователя, загрузившего модуль.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

По ссылке с именем файла или путем к файлу в разделе **Загружен модуль** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- Выполнить задачи:
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
  - **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).

- **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).

- **Скопировать значение в буфер**.

По ссылке с именем файла или путем к файлу в разделе **Инициатор события** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- Выполнить задачи:
  - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
  - **Завершить по уникальному PID** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
  - **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).
  - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- Выполнить задачи:
  - **Собрать данные** → **Файл** (см. раздел "**Создание задачи получения файла**" на стр. 460), **Форензика** (см. раздел "**Создание задачи сбора форензики**" на стр. 461), **Образ диска** (см. раздел "**Создание задачи получения образа диска**" на стр. 466), **Дамп памяти** (см. раздел "**Создание задачи получения дампа оперативной памяти**" на стр. 469).
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Поместить файл на карантин.**
  - **Выполнить приложение**.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- **Найти на TIP**.
- **Найти в Хранилище**.
- **Создать правило запрета**.

- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 531).
- **Создать правило запрета** (см. раздел "**Сетевая изоляция хостов с компонентом Endpoint Agent**" на стр. 448).
- **Скопировать значение в буфер**.

Информация о событии Удаленное соединение

В окне с информацией о событиях типа **Удаленное соединение** содержатся следующие сведения:

- Дерево событий (см. раздел "Информация о событиях в дереве событий" на стр. 384).
- Рекомендации по обработке события.
- Раздел **Удаленное соединение**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Направление соединения** – направление соединения (входящее или исходящее).
  - **Удаленный IP-адрес** – IP-адрес хоста, на который была произведена попытка удаленного соединения.
  - **Локальный IP-адрес** – IP-адрес локального компьютера, с которого была произведена попытка удаленного соединения.
  - **Время события** – время попытки удаленного соединения.
- Раздел **Инициатор события**:
  - **Файл** – имя файла родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, с которого была произведена попытка удаленного соединения.
  - **IP хоста** – IP-адрес хоста, с которого была произведена попытка удаленного соединения.

Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

- **Имя пользователя** – имя пользователя, который пытался установить удаленное соединение.
- **Версия ОС** – версия операционной системы, используемой на хосте.

По ссылке с именем файла или путем к файлу в разделе **Удаленное соединение** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- Выполнить задачи:
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
  - **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).
  - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).
- **Скопировать значение в буфер**.

По ссылке с именем файла или путем к файлу в разделе **Инициатор события** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- Выполнить задачи:
  - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
  - **Завершить по уникальному PID** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
  - **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).
  - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.

- Выполнить задачи:
  - **Собрать данные** → **Файл** (см. раздел "**Создание задачи получения файла**" на стр. 460), **Форензика** (см. раздел "**Создание задачи сбора форензики**" на стр. 461), **Образ диска** (см. раздел "**Создание задачи получения образа диска**" на стр. 466), **Дамп памяти** (см. раздел "**Создание задачи получения дампа оперативной памяти**" на стр. 469).
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Поместить файл на карантин.**
  - **Выполнить приложение**.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- **Найти на TIP**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 531).
- **Создать правило запрета** (см. раздел "**Сетевая изоляция хостов с компонентом Endpoint Agent**" на стр. 448).
- **Скопировать значение в буфер**.

Информация о событии Правило запрета

В окне с информацией о событиях, в которых сработали правила запрета (см. раздел «Работа с политиками (правилами запрета)» на стр. 486) – событиях типа **Правило запрета** содержатся следующие сведения:

- Дерево событий (см. раздел "Информация о событиях в дереве событий" на стр. 384).
- Рекомендации по обработке события.
- Раздел **Правило запрета**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

По ссылке открывается информация о правиле ТАА (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

Поле отображается, если при создании события сработало правило ТАА (IOA).

- **Файл** – имя файла, запуск которого был запрещен.
- **Параметры запуска** – параметры, с которыми была произведена попытка запуска файла.
- **MD5** – MD5-хеш файла, запуск которого был запрещен.
- **SHA256** – SHA256-хеш файла, запуск которого был запрещен.
- **Размер** – размер файла, запуск которого был запрещен.
- **Время события** – время срабатывания запрета запуска файла.

- Раздел **Сведения**:
  - **Название приложения** – например, название операционной системы.
  - **Производитель** – например, производитель операционной системы.
  - **Описание файла** – например, Example File.
  - **Исходное имя файла** – например, ExampleFile.exe.
  - **Получатель сертификата** – организация, выпустившая цифровой сертификат файла.
  - **Результат проверки подписи** – например, "Подпись недействительна" или "Подпись ОК".
  - **Время создания** – время создания файла, запуск которого был запрещен.
  - **Время изменения** – дата последнего изменения файла, запуск которого был запрещен.
- Раздел **Инициатор события**:
  - **Файл** – имя файла родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
  - **ID процесса** – идентификатор родительского процесса.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором сработал запрет запуска файла.
  - **IP хоста** – IP-адрес хоста, на котором сработал запрет запуска файла.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

  - **Имя пользователя** – имя пользователя, под учетной записью которого был произведен запуск файла.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- Выполнить задачи:
  - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
  - **Завершить по уникальному PID** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
  - **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).
  - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- Выполнить задачи:
  - **Собрать данные** → **Файл** (см. раздел "**Создание задачи получения файла**" на стр. 460), **Форензика** (см. раздел "**Создание задачи сбора форензики**" на стр. 461), **Образ диска** (см. раздел "**Создание задачи получения образа диска**" на стр. 466), **Дамп памяти** (см. раздел "**Создание задачи получения дампа оперативной памяти**" на стр. 469).
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Поместить файл на карантин.**
  - **Выполнить приложение**.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- **Найти на TIP**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).

- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 531).
- **Создать правило запрета** (см. раздел "**Сетевая изоляция хостов с компонентом Endpoint Agent**" на стр. 448).
- **Скопировать значение в буфер**.

Информация о событии Заблокирован документ

В окне с информацией о событиях типа **Заблокирован документ** содержатся следующие сведения:

- Дерево событий (см. раздел "Информация о событиях в дереве событий" на стр. 384).
- Рекомендации по обработке события.
- Раздел **Заблокирован документ**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Файл** – имя заблокированного документа.
  - **MD5** – MD5-хеш заблокированного документа.
  - **SHA256** – SHA256-хеш заблокированного документа.
  - **Время события** – время блокирования документа.
  - **Файл процесса** – имя файла процесса, который попытался открыть документ.
  - **MD5 процесса** – MD5-хеш процесса, который попытался открыть документ.
  - **SHA256 процесса** – SHA256-хеш процесса, который попытался открыть документ.
- Раздел **Инициатор события**:
  - **Файл** – имя файла родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
  - **ID процесса** – идентификатор родительского процесса.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором был заблокирован документ.
  - **IP хоста** – IP-адрес хоста, на котором был заблокирован документ.

Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

- **Имя пользователя** – имя пользователя, попытавшегося открыть документ.
- **Версия ОС** – версия операционной системы, используемой на хосте.

По ссылке с именем файла или путем к файлу в разделе **Заблокирован документ** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- Выполнить задачи:
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
  - **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).
  - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).
- **Скопировать значение в буфер**.

По ссылке с именем файла или путем к файлу в разделе **Инициатор события** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- Выполнить задачи:
  - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
  - **Завершить по уникальному PID** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
  - **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).
  - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.

- Выполнить задачи:
  - **Собрать данные** → **Файл** (см. раздел "**Создание задачи получения файла**" на стр. 460), **Форензика** (см. раздел "**Создание задачи сбора форензики**" на стр. 461), **Образ диска** (см. раздел "**Создание задачи получения образа диска**" на стр. 466), **Дамп памяти** (см. раздел "**Создание задачи получения дампа оперативной памяти**" на стр. 469).
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Поместить файл на карантин.**
  - **Выполнить приложение**.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- **Найти на TIP**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 531).
- **Создать правило запрета** (см. раздел "**Сетевая изоляция хостов с компонентом Endpoint Agent**" на стр. 448).
- **Скопировать значение в буфер**.

Информация о событии Изменен файл

В окне с информацией о событиях типа **Изменен файл** содержатся следующие сведения:

- Дерево событий (см. раздел "Информация о событиях в дереве событий" на стр. 384).
- Рекомендации по обработке события.
- В зависимости от типа операции, которая была проведена с файлом, в информации о событии отображается одно из следующих названий раздела:
  - **Создан файл**.
  - **Изменен файл**.

- **Переименован файл**.
- **Удален файл**.
- **Изменены атрибуты файла**.
- **Прочитан файл**.

В разделе отображается следующая информация:

- **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

  По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

  Поле отображается, если при создании события сработало правило TAA (IOA).
- **Файл** – имя созданного, удаленного или измененного файла.
- **MD5** – MD5-хеш созданного, удаленного или измененного файла.
- **SHA256** – SHA256-хеш созданного, удаленного или измененного файла.
- **Размер** – размер созданного, удаленного или измененного файла.
- **Время события** – время обнаружения события.
- **Время создания** – время создания файла.
- **Время изменения** – время последнего изменения файла.
- **Предыдущая версия** – имя предыдущей версии файла.

  Поле **Предыдущая версия** отображается в информации о событии только для операции типа **Переименован файл**.

- **Удалить после перезагрузки** – статус файла, предназначенного к удалению.

  Если файл, к которому была применена операция "удалить", открыт в каком-либо приложении или задействован в других процессах, он будет удален по завершении этих процессов после перезагрузки хоста. В этом случае в поле **Удалить после перезагрузки** отображается Да.

  Если файл, к которому была применена операция "удалить", был удален сразу, в поле **Удалить после перезагрузки** отображается Нет.

  Поле **Удалить после перезагрузки** отображается в информации о событии только для операции типа **Удален файл**.

Если событие было записано в базу событий приложением Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, в разделе также отображаются следующие поля:

- **Тип файла** – расширение созданного, удаленного или измененного файла.
- **Флаги открытия файла** – значение флагов открытия созданного, удаленного или измененного файла.
- **Имя пользователя-владельца** – имя пользователя, создавшего файл.

- **Имя группы-владельца** – название группы, пользователи которой могут изменить или удалить файл.
- **Разрешенные привилегии файла** – разрешения, которые могут использоваться для доступа к созданному, удаленному или измененному файлу. Данное поле не отображается, если событие было записано приложением Kaspersky Endpoint Security для Mac.
- **Наследуемые привилегии файла** – разрешения, которые есть у группы пользователей для выполнения операций с родительским каталогом созданного, удаленного или измененного файла. Данное поле не отображается, если событие было записано приложением Kaspersky Endpoint Security для Mac.
- **Актуальные привилегии файла** – разрешения, которые актуальны для созданного или измененного файла на данный момент. Данное поле не отображается, если событие было записано приложением Kaspersky Endpoint Security для Mac.

- Раздел **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.

  Если событие было записано в базу событий приложением Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, в разделе **Инициатор события** также отображаются следующие поля:
  - **Переменные окружения** – переменные окружения процесса.
  - **Настоящее имя пользователя** – имя пользователя, назначенное ему при регистрации в системе.
  - **Настоящее имя группы** – группа, к которой принадлежит пользователь.
  - **Действующее имя пользователя** – имя пользователя, которое было использовано для входа в систему.
  - **Действующее имя группы** – группа, к которой принадлежит пользователь, имя которого использовалось для входа в систему.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором был создан файл.
  - **IP хоста** – IP-адрес хоста, на котором был создан файл.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.
  - **Имя пользователя** – имя пользователя, создавшего файл.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

Если событие было записано в базу событий приложением Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, в разделе **Сведения о системе** также отображается поле **Вход с удаленного хоста** – имя хоста, с которого был совершен удаленный вход в систему.

По ссылке с именем файла или путем к файлу в разделе со сведениями о файле, с которым была произведена операция, раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- Выполнить задачи:
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
  - **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).
  - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).
- **Скопировать значение в буфер**.

По ссылке с именем файла или путем к файлу в разделе **Инициатор события** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- Выполнить задачи:
  - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
  - **Завершить по уникальному PID** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
  - **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).
  - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).
- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, по ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- Выполнить задачу **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.

- **Найти обнаружения**.
- Выполнить задачи:
  - **Собрать данные** → **Файл** (см. раздел "**Создание задачи получения файла**" на стр. 460), **Форензика** (см. раздел "**Создание задачи сбора форензики**" на стр. 461), **Образ диска** (см. раздел "**Создание задачи получения образа диска**" на стр. 466), **Дамп памяти** (см. раздел "**Создание задачи получения дампа оперативной памяти**" на стр. 469).
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Поместить файл на карантин.**
  - **Выполнить приложение**.
- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac, по ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- Выполнить задачи:
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
  - **Выполнить приложение** (см. раздел "**Создание задачи выполнения приложения**" на стр. 476).
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- **Найти на TIP**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 531).
- **Создать правило запрета** (см. раздел "**Сетевая изоляция хостов с компонентом Endpoint Agent**" на стр. 448).
- **Скопировать значение в буфер**.

Информация о событии Журнал событий ОС

В окне с информацией о событиях типа **Журнал событий ОС** содержатся следующие сведения:

- Дерево событий (см. раздел "Информация о событиях в дереве событий" на стр. 384).
- Рекомендации по обработке события.
- Раздел **Журнал событий ОС**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Время события** – время обнаружения события.
  - **ID события безопасности** – идентификатор типа события безопасности в журнале Windows.

  Если событие было записано в базу событий приложением Kaspersky Endpoint Security для Linux, в разделе **Журнал событий ОС** также отображаются следующие поля:
  - **Тип события** – тип события.
  - **Результат операции** – например, **Успешно** или **Сбой**.
- Раздел **Информация о событии**, содержащий данные из системного журнала. Состав данных зависит от типа события Windows.

  > Раздел **Информация о событии** не отображается в информации о событиях, записанных в базу событий приложением Kaspersky Endpoint Security для Linux.

- Раздел **Инициатор события**:
  - **Файл** – имя файла процесса.
  - **ID процесса** – идентификатор процесса.
  - **Команда** – команда, с помощью которой был запущен родительский процесс.
  - **Переменные окружения** – переменные окружения процесса.
  - **Настоящее имя пользователя** – имя пользователя, назначенное при регистрации в системе.
  - **Настоящее имя группы** – группа, к которой принадлежит пользователь.

  > Раздел **Инициатор события** не отображается в информации о событиях, записанных в базу событий приложением Kaspersky Endpoint Agent для Windows или Kaspersky Endpoint Security для Windows.

- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором произошло событие.

- **IP хоста** – IP-адрес хоста, на котором произошло событие.

  Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

  Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

- **Имя пользователя** – имя пользователя, который запустил процесс, инициировавший запись в системный журнал.
- **Версия ОС** – версия операционной системы, используемой на хосте.

  В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Linux, также отображается поле **Вход с удаленного хоста** – имя компьютера, с которого был совершен удаленный вход в систему.

В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Linux, по ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- Выполнить задачу **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- Выполнить задачи:
  - **Собрать данные** → **Файл** (см. раздел "**Создание задачи получения файла**" на стр. 460), **Форензика** (см. раздел "**Создание задачи сбора форензики**" на стр. 461), **Образ диска** (см. раздел "**Создание задачи получения образа диска**" на стр. 466), **Дамп памяти** (см. раздел "**Создание задачи получения дампа оперативной памяти**" на стр. 469).
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Поместить файл на карантин.**
  - **Выполнить приложение**.
- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий приложением Kaspersky Endpoint Security для Linux, по ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).

- Выполнить задачи:
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
  - **Выполнить приложение** (см. раздел "**Создание задачи выполнения приложения**" на стр. 476).
- **Скопировать значение в буфер**.

Информация о событии Изменение в реестре

В окне с информацией о событиях типа **Изменение в реестре** содержатся следующие сведения:

- Дерево событий (см. раздел "Информация о событиях в дереве событий" на стр. 384).
- Рекомендации по обработке события.
- Раздел **Изменение в реестре**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Путь к ключу** – путь к разделу реестра, в котором произошло изменение.
  - **Имя параметра** – например, RegistrySizeLimit.
  - **Значение параметра** – значение параметра реестра.
  - **Тип параметра** – например, REG_DWORD.
  - **Время события** – время внесения изменения в реестр.

    При изменении имени или параметра ключа реестра могут отображаться дополнительные поля с информацией о состоянии ключа реестра до его изменения:
    - поле **Предыдущий путь к ключу** отображается при изменении имени ключа реестра;
    - поле **Предыдущее значение параметра** отображается при изменении значения параметра реестра;
    - поле **Предыдущий тип параметра** отображается при изменении типа параметра реестра.

    > Если в качестве компонента Endpoint Agent вы используете приложение Kaspersky Endpoint Agent, Kaspersky Anti Targeted Attack Platform получает данные, необходимые для заполнения полей **Предыдущий путь к ключу**, **Предыдущее значение параметра**, **Предыдущий тип параметра**, только при интеграции Kaspersky Anti Targeted Attack Platform с приложением Kaspersky Endpoint Agent для Windows версии 3.10 и выше. При интеграции приложения с предыдущими версиями Kaspersky Endpoint Agent указанные поля не будут отображаться в информации о событии.
- Раздел **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.

По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- **Скопировать значение в буфер**.

Выполнить задачи:

- **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
- **Завершить по уникальному PID** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
- **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
- **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
- **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).
- **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).

- **MD5** – MD5-хеш файла родительского процесса.

  По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти события**.
  - **Найти обнаружения**.
  - **Найти на TIP**.
  - **Найти в Хранилище**.
  - **Создать правило запрета**.

  Скопировать значение в буфер.

- **SHA256** – SHA256-хеш файла родительского процесса.

  По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти события**.
  - **Найти обнаружения**.
  - **Найти на TIP**.
  - **Найти в Хранилище**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.

- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором было произведено изменение в реестре.

    По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).

- **Найти обнаружения** (см. раздел "**Просмотр обнаружений**" на стр. 350).
- **Скопировать значение в буфер**.

Выполнить задачи:

- **Собрать данные** → **Файл** (см. раздел "**Создание задачи получения файла**" на стр. 460), **Форензика** (см. раздел "**Создание задачи сбора форензики**" на стр. 461), **Образ диска** (см. раздел "**Создание задачи получения образа диска**" на стр. 466), **Дамп памяти** (см. раздел "**Создание задачи получения дампа оперативной памяти**" на стр. 469).
- **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
- **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
- **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).
- **Выполнить приложение** (см. раздел "**Создание задачи выполнения приложения**" на стр. 476).

- **IP хоста** – IP-адрес хоста, на котором было произведено изменение в реестре.

Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

- **Имя пользователя** – имя пользователя, совершившего изменение в реестре.
- **Версия ОС** – версия операционной системы, используемой на хосте.

Вы можете получать информацию о модификации выбранного ключа реестра, отредактировав или заменив конфигурационный файл Kaspersky Anti Targeted Attack Platform. Для редактирования и замены конфигурационного файла приложения требуется обратиться в Службу технической поддержки.

Настоятельно не рекомендуется выполнять какие-либо операции с конфигурационным файлом Kaspersky Anti Targeted Attack Platform в режиме Technical Support Mode без консультации или указания сотрудников Службы технической поддержки.

Информация о событии Прослушан порт

В окне с информацией о событиях типа **Прослушан порт** содержатся следующие сведения:

- Дерево событий (см. раздел "Информация о событиях в дереве событий" на стр. 384).
- Рекомендации по обработке события.
- Раздел **Прослушан порт**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

Поле отображается, если при создании события сработало правило TAA (IOA).

- **Локальный порт** – порт, который был прослушан.
- **Локальный IP-адрес** – IP-адрес сетевого интерфейса, порт которого был прослушан.
- **Время события** – время прослушивания порта.

- Раздел **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.

    По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
    - **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
    - **Скопировать значение в буфер**.

    Выполнить задачи:

    - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
    - **Завершить по уникальному PID** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
    - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
    - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
    - **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).
    - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).
  - **MD5** – MD5-хеш файла родительского процесса.

    По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события**.
    - **Найти обнаружения**.
    - **Найти на TIP**.
    - **Найти в Хранилище**.
    - **Создать правило запрета**.
    - **Скопировать значение в буфер**.
  - **SHA256** – SHA256-хеш файла родительского процесса.

    По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события**.
    - **Найти обнаружения**.
    - **Найти на TIP**.

- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, порт которого был прослушан.

    По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
    - **Найти обнаружения** (см. раздел "**Просмотр обнаружений**" на стр. 350).
    - **Скопировать значение в буфер**.

    Выполнить задачи:

    - **Собрать данные** → **Файл** (см. раздел "**Создание задачи получения файла**" на стр. 460), **Форензика** (см. раздел "**Создание задачи сбора форензики**" на стр. 461), **Образ диска** (см. раздел "**Создание задачи получения образа диска**" на стр. 466), **Дамп памяти** (см. раздел "**Создание задачи получения дампа оперативной памяти**" на стр. 469).
    - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
    - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
    - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).
    - **Выполнить приложение** (см. раздел "**Создание задачи выполнения приложения**" на стр. 476).
  - **IP хоста** – IP-адрес хоста, порт которого был прослушан.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.
  - **Имя пользователя** – имя пользователя, от имени которого было совершено прослушивание порта.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

Информация о событии Загружен драйвер

В окне с информацией о событиях типа **Загружен драйвер** содержатся следующие сведения:

- Дерево событий (см. раздел "Информация о событиях в дереве событий" на стр. 384).
- Рекомендации по обработке события.
- Раздел **Загружен драйвер**:

- **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

  По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

  Поле отображается, если при создании события сработало правило TAA (IOA).
- **Файл** – имя файла загруженного драйвера.
- **MD5** – MD5-хеш файла загруженного драйвера.
- **SHA256** – SHA256-хеш файла загруженного драйвера.
- **Размер** – размер загруженного драйвера.
- **Время события** – время загрузки драйвера.

- Раздел **Сведения**:
  - **Название приложения** – например, название операционной системы.
  - **Производитель** – например, производитель операционной системы.
  - **Описание файла** – например, Example File.
  - **Исходное имя файла** – например, ExampleFile.exe.
  - **Получатель сертификата** – организация, выпустившая цифровой сертификат файла.
  - **Результат проверки подписи** – например, "Подпись недействительна" или "Подпись OK".
  - **Время создания** – время создания загруженного драйвера.
  - **Время изменения** – время последнего изменения загруженного драйвера.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на который был загружен драйвер.
  - **IP хоста** – IP-адрес хоста, на который был загружен драйвер.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.
  - **Имя пользователя** – имя пользователя, загрузившего драйвер.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

По ссылке с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- Выполнить задачи:

- **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
- **Завершить по уникальному PID** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
- **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
- **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
- **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).
- **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).

- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- Выполнить задачи:
  - **Собрать данные** → **Файл** (см. раздел "**Создание задачи получения файла**" на стр. 460), **Форензика** (см. раздел "**Создание задачи сбора форензики**" на стр. 461), **Образ диска** (см. раздел "**Создание задачи получения образа диска**" на стр. 466), **Дамп памяти** (см. раздел "**Создание задачи получения дампа оперативной памяти**" на стр. 469).
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Поместить файл на карантин.**
  - **Выполнить приложение**.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- **Найти на TIP**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 531).

- **Создать правило запрета** (см. раздел "**Сетевая изоляция хостов с компонентом Endpoint Agent**" на стр. 448).
- **Скопировать значение в буфер**.

Информация о событии Обнаружение

В окне с информацией о событии типа **Обнаружение** содержатся следующие сведения:

- Дерево событий (см. раздел "Информация о событиях в дереве событий" на стр. 384).
- Рекомендации по обработке события.
- На закладке **Сведения** в разделе **Обнаружение**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Обнаружено** – имя обнаруженного объекта.

    По ссылке с именем объекта раскрывается список, в котором вы можете выбрать одно из следующих действий:
    - **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
    - **Просмотреть на Kaspersky Threats**.
    - **Скопировать значение в буфер**.
  - **Последнее действие** – последнее действие над обнаруженным объектом.
  - **Имя объекта** – полное имя файла, в котором обнаружен объект.
  - **MD5** – MD5-хеш файла, в котором обнаружен объект.
  - **SHA256** – SHA256-хеш файла, в котором обнаружен объект.
  - **Тип объекта** – тип объекта (например, файл).
  - **Режим обнаружения** – режим проверки, в котором выполнено обнаружение.
  - **Время события** – дата и время события.
  - **ID записи** – идентификатор записи об обнаружении в базе.
  - **Версия баз** – версия баз, с помощью которых выполнено обнаружение.
  - **Содержание** – содержание скрипта, переданного на проверку.

    Вы можете скачать эти данные, нажав на кнопку **Сохранить в файл**.
- На закладке **Сведения** в разделе **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.

    По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- **Скопировать значение в буфер**.

Выполнить задачи:

- **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
- **Завершить по уникальному PID** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
- **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
- **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
- **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).
- **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).

- **ID процесса** – идентификатор родительского процесса.
- **Параметры запуска** – параметры запуска родительского процесса.
- **MD5** – MD5-хеш файла родительского процесса.
- **SHA256** – SHA256-хеш файла родительского процесса.

- На закладке **Сведения** в разделе **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором выполнено обнаружение.

    По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
    - **Найти обнаружения** (см. раздел "**Просмотр обнаружений**" на стр. 350).
    - **Скопировать значение в буфер**.

    Выполнить задачи:

    - **Собрать данные** → **Файл** (см. раздел "**Создание задачи получения файла**" на стр. 460), **Форензика** (см. раздел "**Создание задачи сбора форензики**" на стр. 461), **Образ диска** (см. раздел "**Создание задачи получения образа диска**" на стр. 466), **Дамп памяти** (см. раздел "**Создание задачи получения дампа оперативной памяти**" на стр. 469).
    - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
    - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
    - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).
    - **Выполнить приложение** (см. раздел "**Создание задачи выполнения приложения**" на стр. 476).

  - **IP хоста** – IP-адрес хоста, на котором выполнено обнаружение.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

- **Имя пользователя** – учетная запись пользователя, от имени которой было совершено действие над обнаруженным объектом.
- **Версия ОС** – версия операционной системы, используемой на хосте.

- На закладке **История** в таблице:
  - **Тип** – тип события: **Обнаружение** или **Результат обработки обнаружения**.
  - **Описание** – описание события.
  - **Время** – дата и время обнаружения и результата обработки обнаружения.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- **Найти на TIP**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 531).
- **Создать правило запрета** (см. раздел "**Сетевая изоляция хостов с компонентом Endpoint Agent**" на стр. 448).
- **Скопировать значение в буфер**.

Информация о событии Результат обработки обнаружения

В окне с информацией о событии типа **Результат обработки обнаружения** содержатся следующие сведения:

- Дерево событий (см. раздел "Информация о событиях в дереве событий" на стр. 384).
- Рекомендации по обработке события.
- На закладке **Сведения** в блоке параметров **Результат обработки обнаружения**:

- **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

  По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

  Поле отображается, если при создании события сработало правило TAA (IOA).

- **Обнаружено** – имя обнаруженного объекта.

  По ссылке с именем объекта раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
  - **Просмотреть на Kaspersky Threats**.
  - **Скопировать значение в буфер**.

- **Последнее действие** – последнее действие над обнаруженным объектом.
- **MD5** – MD5-хеш файла, в котором обнаружен объект.
- **SHA256** – SHA256-хеш файла, в котором обнаружен объект.
- **Тип объекта** – тип объекта (например, файл).
- **Имя объекта** – полное имя файла, в котором обнаружен объект.
- **Режим обнаружения** – режим проверки, в котором выполнено обнаружение.
- **Время события** – дата и время события.
- **ID записи** – идентификатор записи об обнаружении в базе.
- **Версия баз** – версия баз, с помощью которых выполнено обнаружение.

- На закладке **Сведения** в блоке параметров **Инициатор события**:

  - **Файл** – путь к файлу родительского процесса.

    По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
    - **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
    - **Скопировать значение в буфер**.

    Выполнить задачи:

    - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
    - **Завершить по уникальному PID** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
    - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
    - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
    - **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).
    - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).

  - **ID процесса** – идентификатор родительского процесса.

- **Параметры запуска** – параметры запуска родительского процесса.
- **MD5** – MD5-хеш файла родительского процесса.
- **SHA256** – SHA256-хеш файла родительского процесса.

- На закладке **Сведения** в блоке параметров **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором выполнено обнаружение.

    По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
    - **Найти обнаружения** (см. раздел "**Просмотр обнаружений**" на стр. 350).
    - **Скопировать значение в буфер**.

    Выполнить задачи:

    - **Собрать данные** → **Файл** (см. раздел "**Создание задачи получения файла**" на стр. 460), **Форензика** (см. раздел "**Создание задачи сбора форензики**" на стр. 461), **Образ диска** (см. раздел "**Создание задачи получения образа диска**" на стр. 466), **Дамп памяти** (см. раздел "**Создание задачи получения дампа оперативной памяти**" на стр. 469).
    - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
    - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
    - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).

    Выполнить приложение (см. раздел "**Создание задачи выполнения приложения**" на стр. 476).
  - **IP хоста** – IP-адрес хоста, на котором выполнено обнаружение.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.
  - **Имя пользователя** – учетная запись пользователя, от имени которой было совершено действие над обнаруженным объектом.
  - **Версия ОС** – версия операционной системы, используемой на хосте.
- На закладке **История** в таблице:
  - **Тип** – тип события **Результат обработки обнаружения**.
  - **Описание** – описание события.
  - **Время** – дата и время результата обработки обнаружения.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.

- **Найти на TIP**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 531).
- **Создать правило запрета** (см. раздел "**Сетевая изоляция хостов с компонентом Endpoint Agent**" на стр. 448).
- **Скопировать значение в буфер**.

Информация о событии Интерпретированный запуск файла

В окне с информацией о событиях типа **Интерпретированный запуск файла** содержатся следующие сведения:

- Дерево событий (см. раздел "Информация о событиях в дереве событий" на стр. 384).
- Рекомендации по обработке события.
- Раздел **Интерпретированный запуск файла**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Файл** – имя файла.
  - **MD5** – MD5-хеш файла.
  - **SHA256** – SHA256-хеш файла.
  - **Размер** – размер файла.
  - **Время создания** – время создания файла.
  - **Время изменения** – время последнего изменения файла.
- Раздел **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.

- **SHA256** – SHA256-хеш файла родительского процесса.
- **ID процесса** – идентификатор родительского процесса.

- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором был запущен файл.
  - **IP хоста** – IP-адрес хоста, на котором был запущен файл.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

  - **Имя пользователя** – имя пользователя, под учетной записью которого был запущен файл.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

По ссылке с именем файла или путем к файлу в разделе **Интерпретированный запуск файла** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- Выполнить задачи:
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
  - **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).
  - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).
- **Скопировать значение в буфер**.

По ссылке с именем файла или путем к файлу в разделе **Инициатор события** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- Выполнить задачи:
  - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
  - **Завершить по уникальному PID** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
  - **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).
  - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).

- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- Выполнить задачи:
  - **Собрать данные** → **Файл** (см. раздел "**Создание задачи получения файла**" на стр. 460), **Форензика** (см. раздел "**Создание задачи сбора форензики**" на стр. 461), **Образ диска** (см. раздел "**Создание задачи получения образа диска**" на стр. 466), **Дамп памяти** (см. раздел "**Создание задачи получения дампа оперативной памяти**" на стр. 469).
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Поместить файл на карантин.**
  - **Выполнить приложение**.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- **Найти на TIP**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 531).
- **Создать правило запрета** (см. раздел "**Сетевая изоляция хостов с компонентом Endpoint Agent**" на стр. 448).
- **Скопировать значение в буфер**.

Информация о событии AMSI-проверка

В окне с информацией о событии типа **AMSI-проверка** содержатся следующие сведения:

- Дерево событий (см. раздел "Информация о событиях в дереве событий" на стр. 384).

- Рекомендации по обработке события.
- В разделе **AMSI-проверка**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Время события** – дата и время события.
  - **Тип содержимого** – тип скрипта.

    В приложении предусмотрено два типа скриптов:
    - Если скрипт представлен в виде текста, в поле **Тип содержимого** отображается тип скрипта *Текст*.
    - Если скрипт представлен в другой форме, в поле **Тип содержимого** отображается тип скрипта *Двоичный код*.
  - **Содержание** – содержание скрипта, переданного на проверку.

    Вы можете скопировать эти данные, нажав на кнопку **Скопировать в буфер**, если данные представлены в виде текста, или скачать файл с данными, нажав на кнопку **Сохранить в файл**, если данные представлены в другой форме.

    > Поле **Содержание** отображается в информации о событии, если приложение регистрирует признаки целевых атак.
- В разделе **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.

    По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:
    - **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
    - **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
    - **Скопировать значение в буфер**.

    Выполнить задачи:
    - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
    - **Завершить по уникальному PID** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
    - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
    - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
    - **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).
    - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).
  - **MD5** – MD5-хеш файла родительского процесса.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- **Найти на TIP**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

- **SHA256** – SHA256-хеш файла родительского процесса.

  По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти события**.
  - **Найти обнаружения**.
  - **Найти на TIP**.
  - **Найти в Хранилище**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.

- В разделе **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором выполнено обнаружение.

    По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
    - **Найти обнаружения** (см. раздел "**Просмотр обнаружений**" на стр. 350).
    - **Скопировать значение в буфер**.

    Выполнить задачи:

    - **Собрать данные** → **Файл** (см. раздел "**Создание задачи получения файла**" на стр. 460), **Форензика** (см. раздел "**Создание задачи сбора форензики**" на стр. 461), **Образ диска** (см. раздел "**Создание задачи получения образа диска**" на стр. 466), **Дамп памяти** (см. раздел "**Создание задачи получения дампа оперативной памяти**" на стр. 469).
    - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
    - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
    - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).
    - **Выполнить приложение** (см. раздел "**Создание задачи выполнения приложения**" на стр. 476).

  - **IP хоста** – IP-адрес хоста, на котором выполнено обнаружение.

Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

- **Имя пользователя** – учетная запись пользователя, от имени которой было совершено изменение в реестре.
- **Версия ОС** – версия операционной системы, используемой на хосте.

Информация о событии Интерактивный ввод команд в консоли

В окне с информацией о событиях типа **Интерактивный ввод команд в консоли** содержатся следующие сведения:

- Дерево событий (см. раздел "Информация о событиях в дереве событий" на стр. 384).
- Рекомендации по обработке события.
- Раздел **Интерактивный ввод команд в консоли**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Тип ввода** – тип ввода команд, которые были переданы консольному приложению.

    В приложении предусмотрено два типа ввода команд:
    - Если команды в консольном приложении были введены пользователем, в поле **Тип ввода** отображается тип ввода команд *Консоль*.
    - Если команды были переданы в консольное приложение из другого приложения через коммуникационный шлюз (пайп), в поле **Тип ввода** отображается тип ввода команд *Канал.*

    Если в роли компонента Endpoint Agent вы используете приложение Kaspersky Endpoint Agent, Kaspersky Anti Targeted Attack Platform получает данные, необходимые для заполнения поля **Команда**, только при интеграции Kaspersky Anti Targeted Attack Platform с приложением Kaspersky Endpoint Agent для Windows версии 3.10. При интеграции приложения с предыдущими версиями приложения Kaspersky Endpoint Agent указанное поле не будет отображаться в информации о событии.

    - **Текст команды** – текст, введенный в командную строку (например, CMD) на хосте с приложением Kaspersky Endpoint Agent.

    Вы можете скопировать этот текст, нажав на кнопку **Скопировать в буфер**, расположенную в поле **Текст команды**.

- **Время события** – время обнаружения события.
- Раздел **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.

    По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
    - **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
    - **Скопировать значение в буфер**.

    Выполнить задачи:

    - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
    - **Завершить по уникальному PID** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
    - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
    - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460).
    - **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).
    - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).
  - **MD5** – MD5-хеш файла родительского процесса.

    По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события**.
    - **Найти обнаружения**.
    - **Найти на TIP**.
    - **Найти в Хранилище**.
    - **Создать правило запрета**.
    - **Скопировать значение в буфер**.
  - **SHA256** – SHA256-хеш файла родительского процесса.

    По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события**.
    - **Найти обнаружения**.
    - **Найти на TIP**.
    - **Найти в Хранилище**.
    - **Создать правило запрета**.
    - **Скопировать значение в буфер**.
- Раздел **Сведения о системе**:

- **Имя хоста** – имя хоста, на котором была введена команда.

  По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
  - **Найти обнаружения** (см. раздел "**Просмотр обнаружений**" на стр. 350).
  - **Скопировать значение в буфер**.

  Выполнить задачи:

  - **Собрать данные** → **Файл** (см. раздел "**Создание задачи получения файла**" на стр. 460), **Форензика** (см. раздел "**Создание задачи сбора форензики**" на стр. 461), **Образ диска** (см. раздел "**Создание задачи получения образа диска**" на стр. 466), **Дамп памяти** (см. раздел "**Создание задачи получения дампа оперативной памяти**" на стр. 469).
  - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 469).
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 477).
  - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478).
  - **Выполнить приложение** (см. раздел "**Создание задачи выполнения приложения**" на стр. 476).

- **IP хоста** – IP-адрес хоста, на котором была введена команда.

  Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

  Приложение не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

- **Имя пользователя** – учетная запись пользователя, от имени которой была введена команда.
- **Версия ОС** – версия операционной системы, используемой на хосте.

Работа с информацией о хостах с компонентом Endpoint Agent

Приложение, выступающее в роли компонента Endpoint Agent (см. раздел "Компонент Endpoint Agent" на стр. 68), устанавливается на отдельные компьютеры (далее также "хосты"), входящие в IT-инфраструктуру организации. Приложение осуществляет постоянное наблюдение за процессами, запущенными на этих хостах, открытыми сетевыми соединениями и изменяемыми файлами.

Пользователи с ролью **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности**, **Аудитор**, **Локальный администратор** и **Администратор** могут оценить регулярность получения данных с хостов с компонентом Endpoint Agent, на закладке **Endpoint Agents** окна веб-интерфейса сервера Central Node в рамках тех тенантов, к данным которых у них есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса приложения" на стр. 200). Если вы используете режим

распределенного решения и мультитенантности, то в веб-интерфейсе сервера PCN отображается список хостов с компонентом Endpoint Agent для PCN и всех подключенных SCN.

Пользователи с ролью **Локальный администратор** и **Администратор** могут настроить отображение регулярности получения данных с хостов с компонентом Endpoint Agent в рамках тех тенантов, к данным которых у них есть доступ.

В случае возникновения подозрительной сетевой активности пользователь с ролью **Старший сотрудник службы безопасности** может изолировать от сети (см. раздел "Сетевая изоляция хостов с компонентом Endpoint Agent" на стр. 448) любой из хостов с компонентом Endpoint Agent в рамках тех тенантов, к данным которых у него есть доступ. При этом соединение между сервером с компонентом Central Node и хостом с компонентом Endpoint Agent не будет прервано.

Для оказания поддержки при неполадках в работе компонента Endpoint Agent специалисты Службы технической поддержки (см. раздел «Обращение в Службу технической поддержки» на стр. 670) могут попросить вас в отладочных целях выполнить следующие действия (в том числе в режиме Technical Support Mode (см. раздел «Начало работы с приложением в режиме Technical Support Mode» на стр. 189)):

- Активировать функциональность получения расширенной диагностической информации.
- Изменить параметры отдельных компонентов приложения.
- Изменить параметры хранения и отправки получаемой диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

Специалисты Службы технической поддержки сообщат вам необходимую для выполнения перечисленных действий информацию (описание последовательности шагов, изменяемые параметры, конфигурационные файлы, скрипты, дополнительные возможности командной строки, отладочные модули, специализированные утилиты и так далее), а также состав получаемых в отладочных целях данных. Полученная расширенная диагностическая информация сохраняется на компьютере пользователя. Автоматическая пересылка полученных данных в "Лабораторию Касперского" не выполняется.

Перечисленные выше действия должны выполняться только под руководством специалистов Службы технической поддержки по полученным от них инструкциям. Самостоятельное изменение параметров работы приложения способами, не описанными в настоящем руководстве, может привести к замедлению и сбоям в работе операционной системы, снижению уровня защиты компьютера, а также к нарушению доступности и целостности обрабатываемой информации.

kaspersky

В этом разделе

Просмотр таблицы хостов с компонентом Endpoint Agent 435

Настройка отображения таблицы хостов с компонентом Endpoint Agent 437

Просмотр информации о хосте 437

Фильтрация и поиск хостов с компонентом Endpoint Agent по имени хоста 439

Фильтрация и поиск хостов с компонентом Endpoint Agent, изолированных от сети 440

Фильтрация и поиск хостов с компонентом Endpoint Agent по именам серверов PCN и SCN 440

Фильтрация и поиск хостов с компонентом Endpoint Agent по IP-адресу компьютера 441

Фильтрация и поиск хостов с компонентом Endpoint Agent по версии операционной системы на компьютере 442

Фильтрация и поиск хостов с компонентом Endpoint Agent по версии компонента 442

Фильтрация и поиск хостов с компонентом Endpoint Agent по их активности 443

Быстрое создание фильтра хостов с компонентом Endpoint Agent 444

Сброс фильтра хостов с компонентом Endpoint Agent 444

Удаление хостов с компонентом Endpoint Agent 444

Настройка показателей активности компонента Endpoint Agent 445

Поддерживаемые интерпретаторы и процессы 446

Просмотр таблицы хостов с компонентом Endpoint Agent

Таблица хостов с компонентом Endpoint Agent находится в разделе **Endpoint Agents** окна веб-интерфейса приложения.

Если вы используете режим распределенного решения и мультитенантности, в таблице содержится информация о хостах с компонентом Endpoint Agent, подключенных к PCN и всем серверам SCN.

В таблице могут отображаться следующие данные:

- Количество хостов и показатели активности компонента Endpoint Agent:
  - **Критическое бездействие** – количество хостов, от которых последние данные были получены очень давно.
  - **Предупреждение** – количество хостов, от которых последние данные были получены давно.
  - **Нормальная активность** – количество хостов, от которых последние данные были получены недавно.
- **Хост** – имя хоста с компонентом Endpoint Agent.
- **Серверы** – имя сервера, к которому подключен хост с компонентом Endpoint Agent.

  Поле отображается, если вы используете режим распределенного решения и мультитенантности.
- **IP** – IP-адрес хоста, на который установлен компонент Endpoint Agent.
- **ОС** – версия операционной системы, установленной на хосте с компонентом Endpoint Agent.

- **Версия** – версия установленного компонента Endpoint Agent.
- **Активность** – показатель активности компонента Endpoint Agent.
  - **Нормальная активность** – хосты, от которых последние данные были получены недавно.
  - **Предупреждение** – хосты, от которых последние данные были получены давно.
  - **Критическое бездействие** – хосты, от которых последние данные были получены очень давно.
- **Последнее подключение** – дата и время последнего подключения компонента Endpoint Agent к серверу Central Node.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- Выполнить задачи:
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Завершить по уникальному PID**.
  - **Получить файл**.
  - **Собрать форензику**
  - **Поместить файл на карантин**.
  - **Выполнить приложение**.
- **Новое правило запрета**.
- **Изолировать от сети**.
- **Найти события**.
- **Найти обнаружения**.
- **Скопировать значение в буфер**.

Список доступных действий зависит от типа (для Windows или Linux), версии и показателя активности компонента Endpoint Agent.

По ссылке с IP-адресом раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Найти обнаружения**.
- **Скопировать значение в буфер**.

По ссылке в любом другом столбце таблицы раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скопировать значение в буфер**.

Настройка отображения таблицы хостов с компонентом Endpoint Agent

Вы можете настроить отображение столбцов, а также порядок их следования в таблице хостов с компонентом Endpoint Agent.

► *Чтобы настроить отображение таблицы хостов с компонентом Endpoint Agent:*

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.
2. В заголовочной части таблицы нажмите на кнопку .
3. Отобразится окно **Настройка таблицы**.
4. Если вы хотите включить отображение столбца в таблице, установите флажок рядом с названием того параметра, который должен отображаться в таблице.

   Если вы не хотите, чтобы параметр отображался в таблице, снимите флажок.

   Должен быть установлен хотя бы один флажок.

5. Если вы хотите изменить порядок отображения столбцов в таблице, наведите курсор мыши на строку с нужным параметром, нажмите на кнопку и переместите строку с параметром в нужное место.
6. Если вы хотите восстановить параметры отображения таблицы по умолчанию, нажмите на ссылку **По умолчанию**.
7. Нажмите на кнопку **Применить**.

Отображение таблицы хостов с компонентом Endpoint Agent будет настроено.

Просмотр информации о хосте

► *Чтобы просмотреть информацию о хосте с компонентом Endpoint Agent:*

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.
2. Выберите хост, информацию о котором вы хотите просмотреть.

Откроется окно с информацией о хосте.

Окно содержит следующую информацию:

- Блок рекомендаций:
  - **Обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331) – ссылка, по которой открывается раздел **Обнаружения** с условием поиска, содержащим выбранный хост.

- **События** (см. раздел "**Поиск угроз по базе событий**" на стр. 366) – ссылка, по которой открывается раздел **Поиск угроз** с условием поиска, содержащим выбранный хост.
- **События, по которым сработали правила запрета** – ссылка, по которой открывается раздел **Поиск угроз** с условием поиска, содержащим выбранный хост и тип события **Правило запрета**.

Ссылка **События, по которым сработали правила запрета** не отображается в информации о хостах, на которых в роли компонента Endpoint Agent используется приложение Kaspersky Endpoint Security для Linux.

- На закладке **Сведения**, в разделе **Хост** отображается следующая информация:
  - **Имя** – имя хоста с компонентом Endpoint Agent.
  - **IP** – IP-адрес хоста, на который установлен компонент Endpoint Agent.
  - **ОС** – версия операционной системы хоста, на который установлен компонент Endpoint Agent.
- На закладке **Сведения**, в разделе **Endpoint Agent** отображается следующая информация:
  - **Версия** – версия установленного компонента Endpoint Agent.
- **Активность** – показатель активности компонента Endpoint Agent (см. раздел "Настройка показателей активности компонента Endpoint Agent" на стр. 293). Может иметь следующие значения:
  - **Нормальная активность** – хосты, от которых последние данные были получены недавно.
  - **Предупреждение** – хосты, от которых последние данные были получены давно.
  - **Критическое бездействие** – хосты, от которых последние данные были получены очень давно.
- **Сервер** – имя сервера SCN или PCN. Отображается только в режиме распределенного решения и мультитенантности.
- **Подключен к серверу** – имя сервера Central Node.
- **Последнее подключение** – время последнего соединения с сервером Central Node, SCN или PCN.
- **Лицензия** – например, "OK".
- На закладке **Правила запрета** (см. раздел "**Работа с политиками (правилами запрета)**" на стр. 486) вы можете просмотреть, запуск или открытие файлов с какими MD5- или SHA256-хешами были запрещены на хосте. Отображается следующая информация:
  - **Имя** – имя файла.
  - **Состояние** – состояние правила запрета.
  - **Хеш** – алгоритм хеширования.

Закладка **Правила запрета** не отображается в информации о хостах с приложением Kaspersky Endpoint Security для Linux.

- На закладке **Задачи (см. раздел "Работа с задачами" на стр. 456)** вы можете просмотреть, какие задачи были запущены на хосте. Отображается следующая информация:
  - **Время создания** – дата и время создания задачи.
  - **Имя** – название задачи.
  - **Сведения** – полный путь к файлу или потоку данных, для которого создана задача.

- **Состояние** – статус выполнения задачи.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Выполнить задачи:
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Получить файл**.
  - **Собрать форензику.**
  - **Поместить файл на карантин**.
  - **Выполнить приложение**.
- **Новое правило запрета**.
- **Изолировать от сети**.
- **Найти события**.
- **Найти обнаружения**.
- **Скопировать значение в буфер**.

> Для хостов с приложением Kaspersky Endpoint Security для Linux в списке, который раскрывается по ссылке с именем хоста, отображаются только **Получить файл**, **Выполнить приложение**, **Найти события** и **Найти обнаружения**.

По ссылке с IP-адресом раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти обнаружения**.
- **Скопировать значение в буфер**.

Фильтрация и поиск хостов с компонентом Endpoint Agent по имени хоста

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по имени хоста:*

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **Хост** откройте окно настройки фильтрации.
3. Если вы хотите, чтобы отобразились только изолированные хосты, установите флажок **Показывать только изолированные Endpoint Agents**.
4. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.

5. В поле ввода укажите один или несколько символов имени хоста.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
7. Если вы хотите удалить условие фильтрации, нажмите на кнопку справа от поля.
8. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с компонентом Endpoint Agent, изолированных от сети

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent, изолированные от сети:*

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **Хост** откройте окно настройки фильтрации.
3. Установите флажок **Показывать только изолированные Endpoint Agents**.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с компонентом Endpoint Agent по именам серверов PCN и SCN

Если вы используете режим распределенного решения и мультитенантности, вы можете отфильтровать или найти хосты с компонентом Endpoint Agent по именам серверов PCN и SCN, к которым подключены эти хосты.

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по именам серверов PCN и SCN:*

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.

Откроется таблица хостов.

2. По ссылке **Серверы** откройте окно настройки фильтрации.
3. Установите флажки рядом с теми именами серверов, по которым вы хотите отфильтровать или найти хосты с компонентом Endpoint Agent.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с компонентом Endpoint Agent по IP-адресу компьютера

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по IP-адресу компьютера, на котором установлено приложение:*

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **IP** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов IP-адреса компьютера. Вы можете ввести IP-адрес компьютера или маску подсети в формате IPv4 (например, `192.0.0.1` или `192.0.0.0/16`).
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
6. Если вы хотите удалить условие фильтрации, нажмите на кнопку справа от поля.
7. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с компонентом Endpoint Agent по версии операционной системы на компьютере

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по версии операционной системы, установленной на компьютере:*

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **ОС** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов версии операционной системы.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
6. Если вы хотите удалить условие фильтрации, нажмите на кнопку справа от поля.
7. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с компонентом Endpoint Agent по версии компонента

Вы можете отфильтровать хосты по версии приложения, которое используется в роли компонента Endpoint Agent.

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по версии компонента:*

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **Версия** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.

4. В поле ввода укажите один или несколько символов версии приложение, которое используется в роли компонента Endpoint Agent.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
6. Если вы хотите удалить условие фильтрации, нажмите на кнопку справа от поля.
7. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с компонентом Endpoint Agent по их активности

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по их активности:*

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **Активность** откройте окно настройки фильтрации.

   Установите флажки рядом с одним или несколькими показателями активности:
   - **Нормальная активность**, если вы хотите найти хосты, от которых последние данные были получены недавно.
   - **Предупреждение**, если вы хотите найти хосты, от которых последние данные были получены давно.
   - **Критическое бездействие**, если вы хотите найти хосты, от которых последние данные были получены очень давно.
3. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Быстрое создание фильтра хостов с компонентом Endpoint Agent

► *Чтобы быстро создать фильтр хостов с компонентом Endpoint Agent:*

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. Выполните следующие действия по быстрому добавлению условий фильтрации в создаваемый фильтр:

   a. Наведите курсор мыши на ссылку с тем значением столбца таблицы, которое вы хотите добавить в качестве условия фильтрации.

   b. Нажмите на левую клавишу мыши.

      Откроется список действий над значением.

   c. В открывшемся списке выберите одно из следующих действий:

      - **Добавить в фильтр**, если вы хотите включить это значение в условие фильтрации.
      - **Исключить из фильтра**, если вы хотите исключить это значение из условия фильтрации.

3. Если вы хотите добавить несколько условий фильтрации в создаваемый фильтр, выполните действия по быстрому добавлению каждого из условий фильтрации в создаваемый фильтр.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Сброс фильтра хостов с компонентом Endpoint Agent

► *Чтобы сбросить фильтр хостов с компонентом Endpoint Agent по одному или нескольким условиям фильтрации:*

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.
2. Нажмите на кнопку ☒ справа от того заголовка столбца таблицы, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Удаление хостов с компонентом Endpoint Agent

Чтобы удалить один или несколько хостов из таблицы **Endpoint Agents**:

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.
2. Установите флажки рядом с одним или несколькими хостами, которые вы хотите удалить. Вы можете выбрать все хосты, установив флажок в строке с заголовками столбцов.

   В нижней части окна отобразится панель управления.

3. Нажмите на кнопку **Удалить**.
4. В открывшемся окне подтверждения действия нажмите на кнопку **Да**.

Выбранные хосты будут удалены из таблицы **Endpoint Agents**.

При удалении хостов в веб-интерфейсе Kaspersky Anti Targeted Attack Platform происходят следующие изменения:

- Для удаленного хоста нельзя создать задачу (см. раздел "Работа с задачами" на стр. 456), правило запрета (см. раздел "Работа с политиками (правилами запрета)" на стр. 486) и правило сетевой изоляции (см. раздел "Сетевая изоляция хостов с компонентом Endpoint Agent" на стр. 448).
- Если для хоста ранее было создано правило запрета, при удалении этого хоста его имя в окне просмотра правила (см. раздел "Просмотр правила запрета" на стр. 490) (поле **Запрет для**) будет скрыто. Правило продолжит действовать.

  При повторном подключении этого хоста к серверу Central Node имя хоста будет восстановлено в поле **Запрет для** и правило запрета снова будет на него распространяться.
- Если для хоста ранее было создано правило сетевой изоляции, оно продолжит действовать до истечения времени, указанного в правиле.

  При повторном подключении этого хоста к серверу Central Node правило снова будет распространяться на этот хост.
- Метаданные объектов, помещенных на карантин на удаленном хосте, удаляются из карантина Kaspersky Anti Targeted Attack Platform (см. раздел "Просмотр таблицы объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent" на стр. 545).

  При повторном подключении этого хоста к серверу Central Node метаданные объектов в карантине Kaspersky Anti Targeted Attack Platform **не** восстанавливаются. Вы можете избежать переполнения карантина на хосте, очистив его с помощью командной строки или через Kaspersky Security Center. Подробнее см. в справке приложения, которое используется в роли компонента Endpoint Agent.
- Если объект был помещен на карантин по задаче **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 478) только на одном хосте и этот хост был удален, в окне просмотра задачи (см. раздел "Просмотр информации о задаче" на стр. 459) кнопка **Восстановить все** будет неактивна, так как восстановить файл на удаленном хосте нельзя.

Поиск событий (см. раздел "Поиск угроз по базе событий" на стр. 366) по имени удаленного хоста остается доступным.

Настройка показателей активности компонента Endpoint Agent

Пользователи с ролью **Локальный администратор** и **Администратор** могут определить, какой период бездействия приложения, которое используется в роли компонента Endpoint Agent, считать нормальной, низкой и очень низкой активностью, а также настроить показатели активности приложения. Пользователям с ролью **Аудитор** доступен только просмотр параметров показателей активности приложения. Пользователи с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** могут просмотреть показатели активности приложения в столбце **Активность** таблицы хостов с компонентом Endpoint Agent в разделе **Endpoint Agents** окна веб-интерфейса приложения.

► *Чтобы настроить показатели активности компонента Endpoint Agent, выполните следующие действия:*

1. Войдите в веб-интерфейс приложения под учетной записью **Локальный администратор**, **Администратор** или **Старший сотрудник службы безопасности**.
2. В окне веб интерфейса приложения выберите раздел **Параметры**, подраздел **Endpoint Agents**.
3. В полях под названием раздела введите количество дней бездействия хостов с компонентом Endpoint Agent, которое вы хотите отображать как **Предупреждение** и **Критическое бездействие**.
4. Нажмите на кнопку **Применить**.

Показатели активности компонента Endpoint Agent будут настроены.

Поддерживаемые интерпретаторы и процессы

Приложение Kaspersky Endpoint Agent контролирует запуск скриптов следующими интерпретаторами:

- cmd.exe;
- reg.exe;
- regedit.exe;
- regedt32.exe;
- cscript.exe;
- wscript.exe;
- mmc.exe;
- msiexec.exe;
- mshta.exe;
- rundll32.exe;
- runlegacycplelevated.exe;
- control.exe;
- explorer.exe;
- regsvr32.exe;
- wwahost.exe;
- powershell.exe;
- java.exe и javaw.exe (только при запуске с опцией –jar);
- InstallUtil.exe;
- msdt.exe;
- python.exe;
- ruby.exe;
- rubyw.exe.

Информация о процессах, контролируемых приложением Kaspersky Endpoint Agent, представлена в таблице ниже.

Таблица 38. Процессы и расширения файлов, которые они открывают

Процесс	Расширения файлов
winword.exe	rtf doc dot docm docx dotx dotm docb
excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
acrord32.exe	pdf
wordpad.exe	docx pdf
chrome.exe	pdf
MicrosoftEdge.exe	pdf

Сетевая изоляция хостов с компонентом Endpoint Agent

В рамках действия по реагированию на угрозы пользователи с ролью **Старший сотрудник службы безопасности** могут на время расследования инцидента изолировать хосты, на которых обнаружены объекты, требующие вашего внимания.

Сетевая изоляция не является самостоятельным действием по реагированию на угрозу. Сотруднику службы безопасности требуется расследовать инцидент самостоятельно за период действия сетевой изоляции хоста. Вы можете настроить период действия сетевой изоляции хоста при создании правила сетевой изоляции (см. раздел "Создание правила сетевой изоляции" на стр. 449).

Если в роли компонента Endpoint Agent вы используете приложение Kaspersky Endpoint Agent для Windows, сетевая изоляция доступна для хостов с приложением Kaspersky Endpoint Agent версии 3.8 и следующих версий.

Для корректной работы изолированного хоста рекомендуется выполнять следующие условия:

- Создать на хосте учетную запись локального администратора или сохранить данные доменной учетной записи в кеш перед включением правила сетевой изоляции.
- Не заменять сертификат и IP-адрес сервера с компонентом Central Node при включенном правиле сетевой изоляции.

Изолированным хостам доступны по сети следующие ресурсы:

- Сервер с компонентом Central Node.
- Источник обновлений баз приложения (сервер обновлений "Лаборатории Касперского" или пользовательский источник).
- Серверы службы KSN.
- Хосты, добавленные в исключения правила сетевой изоляции (см. раздел "Добавление исключения из правила сетевой изоляции" на стр. 450).

Если компонент Endpoint Agent на хосте отключен, а также в течение некоторого времени после включения компонента или после перезагрузки компьютера с компонентом, сетевая изоляция этого хоста может не действовать.
При применении сетевой изоляции действует ряд ограничений (см. раздел "Ограничения, действующие при сетевой изоляции" на стр. 451).

kaspersky

В этом разделе

Создание правила сетевой изоляции 449
Добавление исключения из правила сетевой изоляции 450
Удаление правила сетевой изоляции 451
Ограничения, действующие при сетевой изоляции 451

Создание правила сетевой изоляции

► *Чтобы создать правило сетевой изоляции:*

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. Выберите хост, для которого вы хотите включить или отключить правило сетевой изоляции.

   Откроется окно с информацией о хосте.

3. Нажмите на кнопку **Изолировать**.
4. В поле **Отключить изоляцию через** введите количество часов от 1 до 9999, в течение которых будет действовать сетевая изоляция хоста.
5. В блоке параметров **Исключения для правила изоляции хоста** в списке **Направление трафика** выберите направление сетевого трафика, которое не должно быть заблокировано:
   - **Входящее/Исходящее**.
   - **Входящее**.
   - **Исходящее**.
6. В поле **IP** введите IP-адрес, сетевой трафик которого не должен быть заблокирован.

   Если в роли компонента Endpoint Agent вы используете приложение Kaspersky Endpoint Agent, вы можете использовать прокси-сервер для соединения Kaspersky Endpoint Agent для Windows с Kaspersky Anti Targeted Attack Platform. При добавлении этого прокси-сервера в исключения сетевые ресурсы, к которым открыт доступ через прокси-сервер, также добавляются в исключения. Если в исключения добавлены сетевые ресурсы, соединение с которыми происходит через прокси-сервер, но при этом исключение для самого прокси-сервера не настроено, исключение не будет работать.

7. Если вы выбрали **Входящее** или **Исходящее**, в поле **Порты** введите порты подключения.
8. Если вы хотите добавить более одного исключения, нажмите на кнопку **Добавить** и повторите действия по заполнению полей **Направление трафика**, **IP** и **Порты**.
9. Нажмите на кнопку **Сохранить**.

Хост будет изолирован от сети.

Вы также можете создать правило сетевой изоляции по ссылке **Изолировать <имя хоста>** в информации о событии (см. раздел "Информация о событиях" на стр. 378) и в информации об обнаружении (см. раздел "Просмотр обнаружений" на стр. 350).

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция создания правила сетевой изоляции недоступна.
Для хостов с приложением Kaspersky Endpoint Security 11.4 для Linux в роли компонента Endpoint Agent функция сетевой изоляции не предусмотрена.

Добавление исключения из правила сетевой изоляции

► *Чтобы добавить исключение в ранее созданное правило сетевой изоляции:*

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. Выберите хост, изолированный от сети, для которого вы хотите создать исключение из правила сетевой изоляции.

   Откроется окно с информацией о хосте.

3. По ссылке **Добавить в исключения** раскройте блок параметров **Исключения для правила изоляции хоста**.
4. Выберите направление сетевого трафика, которое не должно быть заблокировано:
   - **Входящее/Исходящее**.
   - **Входящее**.
   - **Исходящее**.
5. В поле **IP** введите IP-адрес, сетевой трафик которого не должен быть заблокирован.
6. Если вы выбрали **Входящее** или **Исходящее**, в поле **Порты** введите порты подключения.
7. Если вы хотите добавить более одного исключения, нажмите на кнопку **Добавить** и повторите действия по заполнению полей **Направление трафика**, **IP** и **Порты**. Нажмите на кнопку **Сохранить**.

Исключение из правила сетевой изоляции будет добавлено.

Если в роли компонента Endpoint Agent вы используете приложение Kaspersky Endpoint Agent для Windows, вы можете использовать прокси-сервер для соединения Kaspersky Endpoint Agent с Kaspersky Anti Targeted Attack Platform. При добавлении этого прокси-сервера в исключения сетевые ресурсы, к которым открыт доступ через прокси-сервер, также добавляются в исключения. Если в исключения добавлены сетевые ресурсы, соединение с которыми происходит через прокси-сервер, но при этом исключение для самого прокси-сервера не настроено, исключение не будет работать.
Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция создания исключения из правила сетевой изоляции недоступна.

Удаление правила сетевой изоляции

► *Чтобы удалить правило сетевой изоляции:*

1. В окне веб-интерфейса приложения выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. Нажатием левой клавиши мыши по имени хоста, для которого вы хотите удалить правило сетевой изоляции, раскройте меню действий над этим хостом.

3. Выберите действие **Удалить правило изоляции хоста**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Правило сетевой изоляции хоста будет удалено.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция удаления правила сетевой изоляции недоступна.

Ограничения, действующие при сетевой изоляции

При применении сетевой изоляции действует ряд ограничений:

- При включении правила сетевой изоляции на хосте прерываются все текущие соединения, а также становится недоступно VPN-подключение.
- Если администратор приложения заменяет сертификат сервера с компонентом Central Node при включенном правиле сетевой изоляции, то отключение правила становится недоступно.
- Приложение блокирует соединение изолированных хостов с сервером Active Directory. Если параметры операционной системы требуют подключения к службам Active Directory для авторизации, то пользователь изолированного хоста не сможет войти в систему.

Автоматическая отправка файлов с хостов с компонентом Endpoint Agent на проверку в Sandbox по правилам TAA (IOA) "Лаборатории Касперского"

Если функция включена, приложение может автоматически отправлять файлы с хостов с компонентом Endpoint Agent на проверку компоненту Sandbox в соответствии с правилами TAA (IOA) "Лаборатории Касперского". Отправка файлов на проверку осуществляется по следующему принципу:

1. Kaspersky Anti Targeted Attack Platform проверяет базу событий и отмечает события, соответствующие правилам TAA (IOA).
2. При наличии соответствующих условий в правилах TAA (IOA), Kaspersky Anti Targeted Attack Platform отправляет файлы на проверку компоненту Sandbox.

Запросы на отправку файлов на проверку компоненту Sandbox не отображаются в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.

3. По результатам проверки приложение может записать обнаружения в базу обнаружений.

   Вы можете просмотреть созданные обнаружения, отфильтровав их по показателю **Сведения** (см. раздел "**Фильтрация и поиск обнаружений по полученной информации**" на стр. 338) – **Автоотправка в Sandbox**.

При включении автоматической отправки файлов на проверку компоненту Sandbox объем обрабатываемого компонентом трафика может значительно увеличиться. Если сервер с компонентом Sandbox не рассчитан на увеличение нагрузки, часть объектов из очереди запросов на обработку будет заменена запросами на обработку файлов, отправленных на проверку автоматически.

Чтобы избежать потери объектов из очереди запросов на обработку, вы можете выполнить следующие действия:

- Развернуть дополнительные серверы Sandbox.
- Отключить функцию (см. раздел "Включение и отключение автоматической отправки файлов с хостов с компонентом Endpoint Agent на проверку компоненту Sandbox" на стр. 453) автоматической отправки файлов на проверку компоненту Sandbox.
- Добавить в исключения (см. раздел "Добавление правила ТАА (IOA) в исключения" на стр. 579) правила ТАА (IOA), по которым Kaspersky Anti Targeted Attack Platform наиболее часто отправляет файлы на проверку компоненту Sandbox.

  Информация о правилах, по которым Kaspersky Anti Targeted Attack Platform наиболее часто отправляет файлы на проверку компоненту Sandbox, отображается на виджете (см. раздел "О виджетах и схемах расположения виджетов" на стр. 324) **Отправлено в Sandbox по правилам ТАА**. Вы можете добавить этот виджет на текущую схему расположения виджетов (см. раздел "Добавление виджета на текущую схему расположения виджетов" на стр. 325).

  При добавлении правила в исключения прекращается также разметка событий (см. раздел "Информация о событиях" на стр. 378) и создание обнаружений (см. раздел "Просмотр таблицы обнаружений" на стр. 331) по этому правилу.

Список файлов, которые могут быть отправлены автоматически на проверку компоненту Sandbox, приведен в таблице ниже.

Таблица 39. Список файлов, которые могут быть отправлены автоматически на проверку компоненту Sandbox

Тип события	Тип файла
Запущен процесс	Файл запущенного процесса и файл родительского процесса.
Загружен модуль	Файл загруженного модуля и файл родительского процесса.
Удаленное соединение	Файл родительского процесса.
Правило запрета	Файл приложения, запуск которого был заблокирован, и файл родительского процесса.

Тип события	Тип файла
Заблокирован документ	Файл документа, запуск которого был заблокирован, и файл родительского процесса.
Изменен файл	Созданный, удаленный или измененный файл и файл родительского процесса.
Журнал событий ОС	Файл процесса (только для Linux).
Изменение в реестре	Файл родительского процесса.
Прослушан порт	Файл родительского процесса.
Загружен драйвер	Файл загруженного драйвера.
Обнаружение	Обнаруженный файл и файл родительского процесса (если есть).
Результат обработки обнаружения	Обнаруженный файл и файл родительского процесса (если есть).
AMSI-проверка	Файл процесса.
Интерпретированный запуск файла	Файла, который был запущен, и файл родительского процесса.
Интерактивный ввод команд в консоли	Файл родительского процесса.

Информация о файлах, отправленных на проверку компоненту Sandbox, не отображаются в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.

В этом разделе

Включение и отключение автоматической отправки файлов с хостов с компонентом Endpoint Agent на проверку компоненту Sandbox 453

Включение и отключение автоматической отправки файлов с хостов с компонентом Endpoint Agent на проверку компоненту Sandbox

► *Чтобы включить или отключить автоматическую отправку файлов на проверку компоненту Sandbox по правилам TAA (IOA) "Лаборатории Касперского":*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Endpoint Agents**.
2. В блоке параметров **Автоматическая отправка файлов в Sandbox** выполните следующие действия:

- Установите флажок **Отправлять файлы**,если хотите включить автоматическую отправку файлов.

  По умолчанию функция включена.

- Снимите флажок **Отправлять файлы**, если хотите отключить автоматическую отправку файлов.

  Отключение функции не влияет на работу правил TAA (IOA): будет отключена только автоматическая отправка файлов.

3. Нажмите на кнопку **Применить**.

Автоматическая отправка файлов на проверку компоненту Sandbox по правилам TAA (IOA) "Лаборатории Касперского" будет включена или отключена.

В режиме распределенного решения и мультитенантности параметры автоматической отправки файлов на проверку компоненту Sandbox по правилам TAA (IOA) "Лаборатории Касперского", заданные на сервере PCN, распространяются на подключенные к этому серверу PCN серверы SCN. При необходимости вы можете включить или отключить автоматическую отправку файлов на каждом выбранном сервере SCN отдельно.

Выбор операционных систем для проверки объектов в Sandbox

Пользователи с ролью **Старший сотрудник службы безопасности** могут выбрать набор операционных систем (см. раздел "Выбор операционных систем для проверки объектов в Sandbox" на стр. 455), на основе которого будут формироваться задачи на проверку объектов для компонента Sandbox. На сервере Sandbox должны быть установлены виртуальные машины (см. раздел "Установка и настройка образов операционных систем и приложений для работы компонента Sandbox" на стр. 221), которые соответствуют выбранному набору.

Вы можете просматривать список серверов Sandbox и виртуальных машин, развернутых на сервере (см. раздел "Просмотр таблицы серверов с компонентом Sandbox" на стр. 454).

Пользователи с ролью **Аудитор** могут просматривать список серверов Sandbox (см. раздел "Просмотр таблицы серверов с компонентом Sandbox" на стр. 298) и параметры набора операционных систем. Для пользователей с ролью **Сотрудник службы безопасности** этот раздел недоступен.

Просмотр таблицы серверов с компонентом Sandbox

Для пользователей с ролью **Сотрудник службы безопасности** просмотр таблицы серверов с компонентом Sandbox недоступен.

Пользователи с ролью **Старший сотрудник службы безопасности** могут просматривать таблицу серверов с компонентом Sandbox.

► *Чтобы просмотреть таблицу серверов с компонентом Sandbox:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Серверы Sandbox**.
2. Выберите закладку **Серверы**.

Отобразится таблица со списком серверов Sandbox.

Таблица содержит следующую информацию:

- **IP и имя** – IP-адрес или полное доменное имя сервера с компонентом Sandbox.
- **Авторизация** – статус запроса на подключение к компоненту Sandbox.
- **Состояние** – состояние подключения к компоненту Sandbox.
- **Отпечаток сертификата** – отпечаток сертификата сервера с компонентом Sandbox.
- **Виртуальные машины** – список виртуальных машин, созданных на сервере.

Выбор операционных систем для проверки объектов в Sandbox

► *Чтобы выбрать набор операционных систем:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Серверы Sandbox**.
2. Выберите закладку **Параметры**.
3. В блоке параметров **Набор ОС** выберите один из вариантов:
   - **Windows 7, Windows 10**.
   - **CentOS 7.8, Windows 7, Windows 10**.
   - **Astra Linux 1.7, Windows 7, Windows 10**.
   - **Пользовательские**.
4. Если вы выбрали **Пользовательские**, в блоке параметров **Состав набора** установите флажки напротив операционных систем, которые вы хотите использовать в наборе.

   Пользовательские операционные системы отображаются в списке, если виртуальные машины с этими операционными системами были установлены на сервере Sandbox. Преднастроенные операционные системы всегда отображаются в списке, но если виртуальные машины с этими операционными системами не развернуты, рядом с названием операционной системы отображается статус **Неизвестно**.

Kaspersky Anti Targeted Attack Platform будет создавать задачи на проверку объектов в Sandbox в соответствии с выбранным набором.

Если набор операционных систем, установленных на сервере Sandbox, не совпадает с набором, выбранным на сервере Central Node, объекты не отправляются на проверку этому серверу Sandbox. При подключении к серверу Central Node нескольких серверов Sandbox приложение отправляет объекты на проверку тем серверам Sandbox, на которых установлены операционные системы, соответствующие выбранному на Central Node набору.

Вы можете изменить набор операционных систем в ходе эксплуатации приложения. В этом случае вам нужно убедиться, что конфигурация сервера Sandbox соответствует аппаратным требованиям (см. раздел "Аппаратные и программные требования" на стр. 27).

В режиме распределенного решения и мультитенантности настройки набора операционных систем, заданные на сервере PCN, не распространяются на подключенные к нему серверы SCN. Вы можете выбрать набор операционных систем для каждого сервера PCN и SCN отдельно.

Работа с задачами

Пользователи с ролью **Старший сотрудник службы безопасности**, создающие задачи на сервере, обладают неограниченными правами (root) доступа для всех хостов с компонентом Endpoint Agent, подключенных к этому серверу.

При работе в веб-интерфейсе приложения пользователи с ролью **Старший сотрудник службы безопасности** могут работать с файлами и приложениями на хостах путем создания и удаления задач.

В режиме распределенного решения и мультитенантности задачи **Завершить процесс**, **Собрать форензику**, **Получить ключ реестра**, **Запустить YARA-проверку**, **Управление службами**, **Выполнить приложение**, **Удалить файл**, **Восстановить файл из карантина**, **Поместить файл на карантин** могут быть одного из следующих типов:

- **Глобальный** – созданные на сервере PCN. Действие этих задач распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Задачи относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
- **Локальный** – созданные на сервере SCN. Действие этих задач распространяется только на хосты, подключенные к этому серверу SCN. Задачи относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

Задачи **Получить файл**, **Получить дамп памяти процесса**, **Получить метафайлы NTFS**, **Получить образ диска**, **Получить дамп памяти** выполняются только на указанном хосте, независимо от режима работы приложения.

Максимальное время выполнение задачи составляет 24 часа. Если за это время задача не успела завершиться, ее выполнение останавливается.

Пользователи с ролью **Старший сотрудник службы безопасности** могут работать со всеми задачами в рамках тех тенантов, к данным которых у них есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса приложения" на стр. 200).

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Пользователи с ролью **Аудитор** могут просматривать таблицу задач (см. раздел "Просмотр таблицы задач" на стр. 457) и информацию о выбранной задаче (см. раздел "Просмотр информации о задаче" на стр. 459).

kaspersky

В этом разделе

Просмотр таблицы задач 457
Просмотр информации о задаче 459
Создание задачи получения файла 460
Создание задачи сбора форензики 461
Создание задачи получения ключа реестра 463
Создание задачи получения метафайлов NTFS 464
Создание задачи получения дампа памяти процесса 465
Создание задачи получения образа диска 466
Создание задачи получения дампа оперативной памяти 469
Создание задачи завершения процесса 469
Создание задачи проверки хостов с помощью правил YARA 470
Создание задачи управления службами 473
Создание задачи выполнения приложения 476
Создание задачи удаления файла 477
Создание задачи помещения файла на карантин 478
Создание задачи восстановления файла из карантина 479
Создание копии задачи 480
Удаление задач 480
Фильтрация задач по времени создания 481
Фильтрация задач по типу 482
Фильтрация задач по имени 483
Фильтрация задач по имени и пути к файлу 483
Фильтрация задач по описанию 484
Фильтрация задач по имени сервера 485
Фильтрация задач по имени пользователя, создавшего задачу 485
Фильтрация задач по состоянию обработки 486
Сброс фильтра задач 486

Просмотр таблицы задач

Таблица задач содержит список созданных задач и находится в разделе **Задачи** окна веб-интерфейса приложения. Вы можете просматривать все задачи или только задачи, созданные вами (текущим пользователем).

Вы можете включить или отключить отображение задач, созданных вами с помощью переключателя **Только мои** в правом верхнем углу окна. По умолчанию отображение задач, созданных текущим пользователем, включено.

В таблице задач содержится следующая информация:

- **Время** – дата и время создания задачи.
- **Тип** – тип задачи в зависимости от режима работы приложения и сервера, на котором была создана задача.

  Задачи могут быть одного из следующих типов:

  - **Глобальный** – созданные на сервере PCN. Действие этих задач распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Задачи относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
  - **Локальный** – созданные на сервере SCN. Действие этих задач распространяется только на хосты, подключенные к этому серверу SCN. Задачи относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
- **Имя** – название задачи.

  По ссылке с названием типа задачи раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Добавить в фильтр**.
  - **Исключить из фильтра**.
  - **Скопировать значение в буфер**.
- **Сведения** – полный путь к файлу или потоку данных, для которого создана задача, или путь к общему сетевому ресурсу.

  По ссылке со сведениями о пути к файлу или потоку данных раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Добавить в фильтр**.
  - **Исключить из фильтра**.
  - **Скопировать значение в буфер**.
- **Серверы** – имя сервера с ролью PCN или SCN, на котором выполняется задача.

  Поле отображается, если вы используете режим распределенного решения и мультитенантности.
- **Хосты** – имя хоста, на котором выполняется задача.

  Поле отображается, только если вы используете отдельный сервер Central Node.
- **Автор** – имя пользователя, создавшего задачу.

  > Если вы включили отображение задач, созданных только текущим пользователем, столбец не отображается.

- **Состояние** – статус выполнения задачи.

  Задача может иметь один из следующих статусов:

  - **Ожидает**.

- **В обработке**.
- **Завершено**.

Просмотр информации о задаче

► *Чтобы просмотреть информацию о задаче:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.
2. Выберите задачу, информацию о которой вы хотите просмотреть.

Откроется окно с информацией о задаче.

Окно может содержать следующую информацию в зависимости от типа задачи:

- **Состояние** – статус выполнения задачи.
- **Описание** – описание задачи.
- **Путь к файлу** – путь к файлу или потоку данных.
- **Тип информации** – тип собранных данных.
- **Путь к ключу реестра** – путь к ключу реестра, который требуется получить.
- **ID процесса** – идентификатор процесса.
- **Маска** – маска файлов, которые включены в список данных.
- **Метафайлы** – метафайлы NTFS, которые требуется получить.
- **Том** – имя диска, с которого требуется получить метафайлы, образ диска или дамп памяти.
- **Путь к общему ресурсу** – путь к общему сетевому ресурсу.
- **Сохраненный файл** – ссылка на файл, полученный в результате выполнения задачи.
- **Максимальный уровень вложенности** – максимальный уровень вложенности папок, в которых приложение ищет файлы.
- **Исключения** – папки, в которых запрещены поиск или проверка файлов.
- **Область проверки** – папки, в которых проводится проверка по правилам YARA.
- **Действие** – действие, которое было выполнено над службой.

  В приложении доступны следующие операции со службами:

  - **Запустить**.
  - **Остановить**.
  - **Приостановить**.
  - **Продолжить**.
  - **Удалить**.
  - **Изменить тип запуска**.
- **Максимальное время проверки** – максимальное время выполнения задачи, по истечении которого проверка завершается.

- **SHA256** – SHA256-хеш файла, который вы хотите получить.
- **Запущено от имени** – параметр запуска приложения от имени локальной системы.
- **Автор** – имя пользователя, создавшего задачу.
- **Тенант** – название тенанта. Отображается, только когда вы используете режим распределенного решения и мультитенантности.
- **Время создания** – время создания задачи.
- **Время завершения** – время завершения задачи.
- **Отчет** – результат выполнения задачи на выбранных хостах.

Создание задачи получения файла

Вы можете получить файл с выбранных хостов с компонентом Endpoint Agent. Для этого вам нужно создать задачу получения файла.

Размер файла, который требуется получить, не должен превышать 100 МБ. Если размер файла превышает 100 МБ, задача завершается ошибкой.

► *Чтобы создать задачу получения файла:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и в раскрывающемся списке **Собрать данные** выберите **Файл**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Путь к файлу** – путь к файлу, который вы хотите получить.

      Если запрашиваемый файл связан с дополнительными потоками данных NTFS, в результате выполнения задачи вы получите все файлы потоков данных NTFS, с которыми связан запрашиваемый файл.

      Вы также можете указать путь к альтернативному потоку данных этого файла. В этом случае вы получите только файлы указанного потока.

      При создании задачи приложение не проверяет на корректность указанный путь к файлу, который вы хотите получить.

   b. **MD5/SHA256** – MD5- или SHA256-хеш файла, который вы хотите получить. Поле не является обязательным.

   c. Если вы хотите отказаться от проверки файла, снимите флажок **Отправить на проверку**.

      По умолчанию флажок установлен.

   d. **Описание** – описание задачи. Поле не является обязательным.

   e. **Хост** – имя или IP-адрес хоста.

Вы можете указать только один хост.

4. Нажмите на кнопку **Добавить**.

Будет создана задача получения файла. Задача запускается автоматически после создания.

Файл, полученный в результате выполнения задачи, будет помещен в Хранилище. Если задача получения файла завершилась успешно, вы можете скачать полученный файл на ваш локальный компьютер (см. раздел "Скачивание объектов из Хранилища" на стр. 539).

Если вы используете режим распределенного решения и мультитенантности, архив помещается в Хранилище того сервера Central Node, к которому подключен хост, указанный в поле **Хост**.

Вы также можете скачать полученный файл из окна с отчетом о выполнении задачи.

► *Чтобы скачать полученный файл из окна с отчетом о выполнении задачи:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Откройте задачу получения файла, который вы хотите скачать.
3. В разделе **Отчет** нажмите на имя или IP-адрес хоста.

   Откроется окно с информацией о файле.

4. Нажмите на кнопку **Скачать**.

Файл будет сохранен на ваш локальный компьютер в папку загрузки браузера.

Для пользователей с ролью **Аудитор** функция создания задачи получения файла недоступна.
У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи сбора форензики

Вы можете получить списки файлов, процессов и точек автозапуска с выбранных хостов с компонентом Endpoint Agent. Для этого нужно создать задачу сбора форензики.

► *Чтобы создать задачу сбора форензики:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и в раскрывающемся списке **Собрать данные** выберите **Форензика**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Тип информации** – тип собираемых данных. Установите флажок напротив одного, нескольких или всех параметров:

      - **Список процессов**, если хотите получить список процессов, запущенных на хосте в момент выполнения задачи.
      - **Список точек автозапуска**, если хотите получить список точек автозапуска.

В список точек автозапуска включаются данные о приложениях, добавленных в папку автозагрузки или зарегистрированных в разделах реестра Run, а также о приложениях, которые запускаются автоматически при загрузке хоста с компонентом Endpoint Agent и при входе пользователя в систему на указанных хостах.

Список поддерживаемых точек автозапуска

- **Список файлов**, если хотите получить список файлов, хранящихся в выбранной папке или во всех папках хоста в момент выполнения задачи.

b. Если вы установили флажок **Список файлов**, в блоке параметров **Тип источника** выберите один из вариантов:

- **Все локальные диски**, если вы хотите, чтобы в список файлов были включены файлы, хранящиеся во всех папках локальных дисков на момент выполнения задачи.
- **Директория**, если вы хотите, чтобы в список файлов были включены файлы, хранящиеся в указанной папке и следующих по пути папках диска на момент выполнения задачи.

c. Если вы выбрали **Директория**, в поле **Начальная директория** укажите путь к папке, с которой начнется поиск файлов.

Вы можете использовать следующие префиксы:

- Системные переменные окружения.
- Пользовательские переменные окружения.

  При использовании пользовательских переменных окружения в список файлов будет включена информация о файлах в папках всех пользователей, определивших указанные переменные окружения. Если пользовательские переменные окружения переопределяет системные, в список файлов будет включена информация о файлах в папках по значению системных переменных окружения.

d. **Хосты** – IP-адрес или имя хоста, на который хотите назначить задачу.

Вы можете указать несколько хостов.

> Если в роли компонента Endpoint Agent используется Kaspersky Endpoint Agent, задача получения сбора форензики может быть назначена только на хосты с приложением Kaspersky Endpoint Agent для Windows версии 3.10 и выше. Получение списка точек автозапуска доступно только на хостах с Kaspersky Endpoint Agent для Windows версии 3.12 и выше.

При необходимости вы можете указать следующие параметры поиска файлов в папках:

- **Маска** – маска файлов, которые должны быть включены в список файлов.
- **Альтернативные потоки данных** – флажок, включающий запись информации об альтернативных потоках данных в список файлов.

  Если запрашиваемый файл связан с дополнительными потоками данных NTFS, в результате выполнения задачи вы получите все файлы потоков данных NTFS, с которыми связан запрашиваемый файл.

  По умолчанию флажок установлен.
- **Максимальный уровень вложенности** – максимальный уровень вложенности папок, в которых приложение будет искать файлы.
- **Исключения** – путь к папкам, в которых вы хотите запретить поиск информации о файлах.

- **Описание** – описание задачи.

4. Нажмите на кнопку **Добавить**.

Задача сбора форензики будет создана. Задача запускается автоматически после создания.

В результате выполнения задачи приложение помещает в Хранилище ZIP-архив, который содержит файл с выбранными данными. Если задача завершилась успешно, вы можете скачать архив на ваш локальный компьютер (см. раздел "Скачивание объектов из Хранилища" на стр. 539).

Для пользователей с ролью **Аудитор** функция создания задачи сбора форензики недоступна.
У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи получения ключа реестра

Вы можете получить ключ реестра с выбранных хостов с компонентом Endpoint Agent. Для этого нужно создать задачу получения ключа реестра.

► *Чтобы создать задачу получения ключа реестра:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и в раскрывающемся списке **Собрать данные** выберите **Ключ реестра**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Путь к ключу реестра** – путь к ключу реестра, который вы хотите получить.

      Вы можете указать путь к ключу реестра в одном из следующих форматов:

      - Корневой относительный путь.

        Например, \REGISTRY\MACHINE\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator.

      - Относительный путь с указанием полного имени раздела.

        Например, HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator.

      - Относительный путь с аббревиатурой вместо полного имени раздела.

        Например, HKLM\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator.

      Если вы хотите получить данные из ветки HKEY_CURRENT_USER, вам требуется указать ветку HKEY_USERS и SID пользователя: HKEY_USERS\<SID пользователя>.

   b. **Описание** – описание задачи. Поле не является обязательным.

   c. **Хосты** – имя или IP-адрес хоста, на который вы хотите назначить задачу.

      Вы можете указать несколько хостов.

Если в роли компонента Endpoint Agent используется Kaspersky Endpoint Agent, задача получения ключа реестра может быть назначена только на хосты с приложением Kaspersky Endpoint Agent для Windows версии 3.13 и выше.

4. Нажмите на кнопку **Добавить**.

Задача получения ключа реестра будет создана. Задача запускается автоматически после создания.

В результате выполнения задачи приложение помещает в Хранилище ZIP-архив, который содержит файл в формате .reg, содержащий список всех ключей реестра и их значений, расположенных по указанному при создании задачи пути. Вы можете скачать архив на ваш локальный компьютер (см. раздел "Скачивание объектов из Хранилища" на стр. 539).

Если при выполнении задачи произошел сбой, в файл архива записывается описание ошибки.

Для пользователей с ролью **Аудитор** функция создания этой задачи недоступна.
У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи получения метафайлов NTFS

Вы можете получить метафайлы NTFS с выбранных хостов с компонентом Endpoint Agent. Для этого нужно создать задачу получения метафайлов NTFS.

► *Чтобы создать задачу получения метафайлов NTFS:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и в раскрывающемся списке **Собрать данные** выберите **Метафайлы NTFS**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Метафайлы** – список метафайлов, которые вы можете получить с помощью задачи. Выберите требуемый метафайл, установив напротив него флажок.

      Вы можете выбрать несколько метафайлов.

   b. **Том** – имя диска, с которого вы хотите получить метафайлы.

      По умолчанию в поле указан системный диск. Вы можете указать путь к другому диску в формате `<буква диска>:`.

   c. **Описание** – описание задачи. Поле не является обязательным.

   d. **Хост** – имя или IP-адрес хоста, на который вы хотите назначить задачу.

      Вы можете указать только один хост.

Если в роли компонента Endpoint Agent используется Kaspersky Endpoint Agent, задача получения метафайлов NTFS может быть назначена только на хосты с приложением Kaspersky Endpoint Agent для Windows версии 3.13 и выше.

4. Нажмите на кнопку **Добавить**.

   Задача получения метафайлов NTFS будет создана. Задача запускается автоматически после создания.

В результате выполнения задачи приложение помещает в Хранилище ZIP-архив, который содержит выбранные метафайлы. Вы можете скачать архив на ваш локальный компьютер (см. раздел "Скачивание объектов из Хранилища" на стр. 539).

Если при выполнении задачи произошел сбой, в файл архива записывается описание ошибки.

Если вы используете режим распределенного решения и мультитенантности, архив помещается в Хранилище того сервера Central Node, к которому подключен хост, указанный в поле **Хост**.

Загрузка выбранных метафайлов может привести к заполнению Хранилища и ротации объектов в нем. Если размер метафайла превышает размер Хранилища, метафайл не загружается

Для пользователей с ролью **Аудитор** функция создания этой задачи недоступна. У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи получения дампа памяти процесса

Вы можете получить дамп памяти процесса с выбранных хостов с компонентом Endpoint Agent. Для этого нужно создать задачу получения дампа памяти процесса.

► *Чтобы создать задачу получения дампа памяти процесса:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и в раскрывающемся списке **Собрать данные** выберите **Дамп памяти процесса**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **ID процесса** – идентификатор процесса, для которого вы хотите получить дамп памяти.

   b. **MD5/SHA256** – MD5-, SHA256-хеш файла процесса, для которого вы хотите получить дамп памяти. Поле не является обязательным.

   c. **Описание** – описание задачи. Поле не является обязательным.

   d. **Хост** – имя или IP-адрес хоста, на который вы хотите назначить задачу.

      Вы можете указать только один хост

Если в роли компонента Endpoint Agent используется Kaspersky Endpoint Agent, задача получения дампа памяти процесса может быть назначена только на хосты с приложением Kaspersky Endpoint Agent для Windows версии 3.13 и выше.

4. Нажмите на кнопку **Добавить**.

   Задача получения дампа памяти процесса будет создана. Задача запускается автоматически после создания.

В результате выполнения задачи приложение помещает в Хранилище ZIP-архив, который содержит файл с информацией о процессе и файл дампа памяти процесса. Вы можете скачать архив на ваш локальный компьютер (см. раздел "Скачивание объектов из Хранилища" на стр. 539).

Если при выполнении задачи произошел сбой, в файл архива записывается описание ошибки.

Если вы используете режим распределенного решения и мультитенантности, архив помещается в Хранилище того сервера Central Node, к которому подключен хост, указанный в поле **Хост**.

Для пользователей с ролью **Аудитор** функция создания этой задачи недоступна.
У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи получения образа диска

Вы можете получить образ диска с выбранного хоста с компонентом Endpoint Agent для Windows. Для этого нужно создать задачу получения образа диска.

Файл, полученный в результате выполнения задачи, можно сохранить только в общем сетевом ресурсе.

► *Чтобы создать задачу получения образа диска:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и в раскрывающемся списке **Собрать данные** выберите **Образ диска**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Путь к общему ресурсу** – путь к общему сетевому ресурсу.

      Вам нужно указать путь в формате Universal Naming Convention (UNC): `\\server\share\path`.

      Если последняя в пути папка с указанным именем отсутствует, Kaspersky Endpoint Agent создает ее. В случае неуспешного создания в веб-интерфейсе Kaspersky Anti Targeted Attack Platform отобразится ошибка.

   b. **Имя пользователя** – имя пользователя учетной записи для доступа к общему сетевому ресурсу.

   c. **Пароль** – пароль учетной записи для доступа к общему сетевому ресурсу.

d. В блоке параметров **Тип диска** выберите один из вариантов:

- **Логический**.
- **Физический**.

e. Если вы выбрали **Логический**, в поле **Том** введите букву диска без двоеточия и слеша или переменную `%SystemDrive%`.

f. Если вы выбрали **Физический**, в поле **Физический диск** введите номер диска.

g. Установите флажок **Разбить файл на части**, если вы хотите, чтобы при сохранении файл был разделен на несколько частей.

h. Если вы установили флажок, в поле **Размер части, ГБ** укажите минимальный размер части сохраняемого файла.

Минимальный размер части должен быть более одного гигабайта.

i. **Описание** – описание задачи. Поле не является обязательным.

j. **Хост** – IP-адрес или имя хоста, на который хотите назначить задачу.

4. Нажмите на кнопку **Добавить**.

Задача получения образа диска будет создана. Задача запускается автоматически после создания.

В результате выполнения задачи приложение помещает в общий сетевой ресурс архив, который содержит файл или файлы в формате EWF или RAW. Вы можете конвертировать файлы из формата RAW в формат EWF (см. раздел "Конвертация файла из формата RAW в формат EWF" на стр. 467).

Если в роли компонента Endpoint Agent используется Kaspersky Endpoint Agent, вы можете назначить задачу только на хосты с Kaspersky Endpoint Agent для Windows версии 3.14 и выше.
Для пользователей с ролью **Аудитор** функция создания задач недоступна.
У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Конвертация файла из формата RAW в формат EWF

Kaspersky Endpoint Security сохраняет образ диска в формате RAW. Также файлы могут быть помещены в архив. Для конвертации файлов из формата RAW в формат EWF разработан специальный скрипт на языке Python. Скрипт постоянно выполняет поиск файлов в формате RAW в заданной папке. При обнаружении таких файлов скрипт автоматически конвертирует файлы в формат EWF.

Скрипт convert_to_ewf_monitor.py https://aes.s.kaspersky-labs.com/endpoints/keswin11/12.1.0.506/russian-21.13.5.506.0.4.0/3731303234367c44454c7c4e554c4c/convert_to_ewf_12.1.0.506.zip

Для работы скрипта на компьютере должно быть установлено следующее ПО:

- Библиотека для доступа к файлам Expert Witness Compression Format (EWF) – libewf.

  Библиотеке libewf является ПО с открытым кодом.

  Рекомендуется разместить файлы библиотеки и файл скрипта в одной папке.
- Интерпретатор Python.

► *Чтобы включить конвертацию файлов образов дисков:*

1. Запустите интерпретатор командной строки.
2. Перейдите в папку, в которой расположен скрипт.
3. Выполните команду:

```
py convert_to_ewf_monitor.py --source <full path to the source files folder> [additional settings]
```

Таблица 40. Параметры скрипта конвертации в EWF

Параметр	Описание
`--source <full path to folder>`	Полный путь к папке, в которой скрипт выполняет поиск исходных файлов. Скрипт также выполняет поиск файлов в подпапках по указанному пути. Это обязательный параметр.
`--destination <full path to folder>`	Полный путь к папке, в которую скрипт сохраняет сконвертированные файлы. При этом структура папок сохраняется. По умолчанию скрипт сохраняет сконвертированные файлы в папке, которая указана для параметра `source`.
`--delete`	Удаление исходных файлов после успешной конвертации. Если сконвертировать файлы не удалось, скрипт пропустит удаление исходных файлов, и вы сможете повторить попытку.
`--ewftool <full path to folder>`	Полный путь к файлу ewfacquirestream.exe. Путь следует указывать с названием файла. По умолчанию скрипт пытается обнаружить файл ewfacquirestream.exe в папке, в которой расположен сам скрипт.
`--name_mask <regular expressions>`	Регулярные выражения для поиска исходных файлов для конвертации. Вы можете использовать этот параметр, если вам нужно конвертировать отдельные файлы. По умолчанию скрипт выполняет поиск с помощью регулярного выражения `^diskdump_`.
`--convert_single_dump`	Поиск одного файла для конвертации. После успешной конвертации одного файла скрипт завершает свою работу.
`--workers_num <number of files>`	Максимальное количество исходных файлов, которое скрипт может конвертировать одновременно. С помощью этого параметра вы можете оптимизировать производительность скрипта. По умолчанию скрипт может конвертировать до четырех файлов одновременно.
`--log_level <log level>`	Уровень ведения журнала. По умолчанию скрипт ведет журнал DEBUG.
`--log_path <full path to folder>`	Полный путь для сохранения файлов журнала. Путь следует указывать с названием файла журнала. По умолчанию скрипт показывает события в консоли интерпретатора.

Пример:

```
PS D:\Folder\Script\> py convert_to_ewf_monitor.py --source E:/Folder --destination E:/EWF --delete --log_path E:/Folder/Logs.txt
```

Создание задачи получения дампа оперативной памяти

Вы можете получить дамп оперативной памяти с выбранного хоста с компонентом Endpoint Agent. Для этого нужно создать задачу получения дампа памяти.

Файл, полученный в результате выполнения задачи, можно сохранить только в общем сетевом ресурсе.

► *Чтобы создать задачу получения дампа памяти:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и в раскрывающемся списке **Собрать данные** выберите **Дамп памяти**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Путь к общему ресурсу** – путь к общему сетевому ресурсу.

      Вам нужно указать путь в формате Universal Naming Convention (UNC): `\\server\share\path`.

      Если последняя в пути папка с указанным именем отсутствует, Kaspersky Endpoint Agent создает ее. В случае неуспешного создания в веб-интерфейсе Kaspersky Anti Targeted Attack Platform отобразится ошибка.

   b. **Имя пользователя** – имя пользователя учетной записи для доступа к общему сетевому ресурсу.

   c. **Пароль** – пароль учетной записи для доступа к общему сетевому ресурсу.

   d. **Описание** – описание задачи. Поле не является обязательным.

   e. **Хост** – IP-адрес или имя хоста, на который хотите назначить задачу.

4. Нажмите на кнопку **Добавить**.

Задача получения дампа оперативной памяти будет создана. Задача запускается автоматически после создания.

В результате выполнения задачи приложение помещает в общий сетевой ресурс файл в формате RAW или архив, который содержит файл в формате RAW.

> Если в роли компонента Endpoint Agent вы используете приложение Kaspersky Endpoint Agent, вы можете назначить задачу только на хосты с Kaspersky Endpoint Agent для Windows версии 3.14 и выше.
> Для пользователей с ролью **Аудитор** функция создания задач недоступна.
> У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи завершения процесса

Если вы считаете, что запущенный на компьютере процесс может угрожать безопасности компьютера или локальной сети организации, вы можете завершить его.

► *Чтобы создать задачу завершения процесса:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Завершить процесс**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Путь к файлу** – путь к файлу процесса, который вы хотите завершить.

      Вы также можете указать путь к альтернативному потоку данных этого файла. В этом случае будут завершены только процессы указанного потока данных. Процессы остальных потоков этого файла будут выполняться.

   b. **MD5/SHA256** – MD5-, SHA256-хеш файла процесса, который вы хотите завершить. Поле не является обязательным.

   c. **Описание** – описание задачи. Поле не является обязательным.

   d. **Задача для** – область применения задачи:

      - Если вы хотите выполнить задачу на всех хостах всех серверов, выберите вариант **Всех хостов**.
      - Если вы хотите выполнить задачу на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите выполнить задачу.

        Этот вариант доступен только при включенном режиме распределенного решения и мультитенантности.

      - Если вы хотите выполнить задачу на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

4. Нажмите на кнопку **Добавить**.

Будет создана задача завершения процесса. Задача запускается автоматически после создания.

Для пользователей с ролью **Аудитор** функция создания задачи завершения процесса недоступна.
У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи проверки хостов с помощью правил YARA

Вы можете проверять хосты компонентом Endpoint Agent с помощью правил YARA. Для этого требуется создать задачу **Запустить YARA-проверку**. Вы можете создать задачу следующими способами:

- В разделе **Задачи**.

  В этом случае при создании задачи вам потребуется выбрать правила YARA, с помощью которых вы хотите проверить хосты.

- В разделе **Пользовательские правила**, подразделе **YARA**.

  В этом случае создается задача для проверки хостов по выбранным правилам YARA.

► *Чтобы создать задачу проверки хостов с компонентом Endpoint Agent с помощью правил YARA в разделе **Задачи**:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Запустить YARA-проверку**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Выбрать правила** – имя правила. Вы можете ввести название правила или несколько знаков из названия правила и выбрать правило в списке.

      Вы можете добавить несколько правил.

   b. **Проверить** – область проверки. Выберите один из следующих вариантов:

      - **ОЗУ**, если вы хотите проверить процессы, запущенные на момент выполнения задачи.

        Приложение не проверяет процессы с низким уровнем приоритета.

      - **Точки автозапуска**, если вы хотите проверить точки автозапуска, полученные в результате выполнения задачи **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461).

        Если в качестве компонента Endpoint Agent вы используете приложение Kaspersky Endpoint Agent, эта функция доступна только при интеграции с Kaspersky Endpoint Agent 3.13 и выше.
        Для проверки точек автозапуска вам требуется указать хосты, для которых ранее была выполнена задача **Собрать форензику**.

      - **Указанные директории**, если вы хотите проверить файлы, хранящиеся в указанной папке и во всех вложенных папках на момент выполнения задачи.

      - **Все локальные диски**, если вы хотите проверить файлы, хранящиеся во всех папках локальных дисков на момент выполнения задачи.

        Проверка всех локальных дисков может создать повышенную нагрузку на хост.

   c. Если вы выбрали **ОЗУ**, при необходимости выполните следующие действия:

      - В поле **Процессы** укажите короткие имена процессов или маску файлов, которые хотите проверить.

        Приложение проверяет все запущенные на хосте процессы с одинаковыми именами.

        Если поле **Процессы** не заполнено, приложение проверяет все процессы, запущенные на момент выполнения задачи, кроме процессов с PID ниже 10 и процессов, указанных в поле **Исключения**.

      - В поле **Исключения** укажите короткие имена процессов или маску файлов, которые хотите исключить из проверки.

Если на хосте запущено несколько процессов с одинаковыми именами, приложение исключит из проверки все эти процессы.

d. Если вы выбрали **Точки автозапуска**, в поле **Тип проверки** выберите тип проверки:

- **Быстрая**.

  В этом случае проверяются все точки автозапуска, кроме COM-объектов.

- **Полная**.

  В этом случае проверяются все точки автозапуска и связанные с ними файлы.

> Если в качестве компонента Endpoint Agent вы используете приложение Kaspersky Endpoint Security для Windows, вне зависимости от выбранного параметра выполняется полная проверка.

e. Если вы выбрали **Указанные директории**, выполните следующие действия:

- В поле **Указанные директории** укажите путь к директории в формате C:\<имя директории>*.
- В поле **Исключения** укажите путь к директории в формате C:\<имя директории>*.

f. **Максимальное время проверки** – максимальное время проверки.

По истечении указанного времени проверка завершится, даже если хосты были проверены не по всем правилам. В отчете о выполнении задачи указываются результаты, актуальные на момент завершения проверки.

g. **Описание** – описание задачи. Поле необязательно для заполнения.

h. **Задача для** – область применения задачи:

- Если вы хотите выполнить задачу на всех хостах всех серверов, выберите вариант **Всех хостов**.
- Если вы хотите выполнить задачу на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите выполнить задачу.

  Этот вариант доступен только при включенном режиме распределенного решения и мультитенантности.

- Если вы хотите выполнить задачу на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

> Если в роли компонента Endpoint Agent вы используете приложение Kaspersky Endpoint Agent, задача проверки хостов с Kaspersky Endpoint Agent по правилам YARA может быть назначена только на хосты с приложением Kaspersky Endpoint Agent для Windows версии 3.12 и выше. При одновременном назначении задачи на хосты с Kaspersky Endpoint Agent 3.12 и более ранними версиями приложения задача выполняется только на хостах с Kaspersky Endpoint Agent 3.12.

► *Чтобы создать задачу проверки хостов с компонентом Endpoint Agent с помощью правил YARA в разделе **Пользовательские правила**, подразделе **YARA**:*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **YARA**.
2. Установите флажки слева от правил, с помощью которых вы хотите проверить хосты.

   В нижней части окна отобразится панель управления.
3. Нажмите на кнопку **Запустить YARA-проверку**.
4. Выполните шаг 3 инструкции, приведенной выше.

Создание задачи будет завершено. Задача запускается автоматически после создания.

Если по результатам проверки будут обнаружены угрозы, Kaspersky Anti Targeted Attack Platform создаст соответствующие обнаружения.

Для пользователей с ролью **Аудитор** создание задачи проверки хостов с помощью правил YARA недоступно.
У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи управления службами

Вы можете удаленно запускать, останавливать, приостанавливать и продолжать работу службы, а также удалить службу или изменить ее тип запуска на выбранных хостах с компонентом Endpoint Agent. Для этого нужно создать задачу управления службами.

► *Чтобы создать задачу управления службами:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.
2. Нажмите на кнопку **Добавить** и выберите **Управление службами**.

   Откроется окно создания задачи.
3. Задайте значения следующих параметров:
   a. **Имя службы** – укажите имя службы.
   b. **MD5/SHA256** – MD5- или SHA256-хеш службы. Поле необязательно для заполнения.

      Если вы указали хеш службы, которая загружается из DLL, Kaspersky Anti Targeted Attack Platform сравнивает указанный хеш одновременно с хешем библиотеки службы DLL и хешем процесса svchost.
   c. **Действие** – выберите операцию, которую вы хотите произвести со службой.

      В приложении доступны следующие операции со службами:
      - **Запустить**.
      - **Остановить**.
      - **Приостановить**.

- **Продолжить**.
- **Удалить**.
- **Изменить тип запуска**.

> При удалении службы процессы, которые были запущены этой службой, продолжают работать до перезагрузки системы или завершении работы процесса.

d. Если вы выбрали **Изменить тип запуска**, в поле **Тип запуска** выберите тип запуска службы.

e. **Описание** – описание задачи. Поле необязательно для заполнения.

f. **Задача для** – область применения задачи:

- Если вы хотите выполнить задачу на всех хостах всех серверов, выберите вариант **Всех хостов**.
- Если вы хотите выполнить задачу на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите выполнить задачу.

  Этот вариант доступен только при включенном режиме распределенного решения и мультитенантности.
- Если вы хотите выполнить задачу на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

> Если в качестве компонента Endpoint Agent вы используете приложение Kaspersky Endpoint Agent, вы можете назначить задачу только на хосты с Kaspersky Endpoint Agent для Windows версии 3.12 и выше. Хосты с Kaspersky Endpoint Agent для Windows более ранних версий отображаются в списке хостов, но недоступны для выбора.

4. Нажмите на кнопку **Добавить**.

Задача управления службами будет создана. Задача запускается автоматически после создания.

Настоятельно не рекомендуется останавливать, приостанавливать, а также удалять или изменять тип запуска служб, влияющих на работоспособность хоста.

Список служб, с которыми не рекомендуется проводить операции:

- AVP*.
- BFE.
- CertPropSvc.
- CoreMessagingRegistrar.
- CryptSvc.
- DcomLaunch.
- Dhcp.
- DispBrokerDesktopSvc.
- EventLog.
- EventSystem.
- LanmanServer.
- LanmanWorkstation.
- LSM.
- mpssvc.
- Netlogon.
- Netman.
- PlugPlay.
- PolicyAgent.
- Power.
- ProfSvc.
- RasMan.
- RpcEptMapper.
- RpcSs.
- SamSs.
- SCardSvr.
- SecurityHealthService.
- SessionEnv.
- Spooler.
- SstpSvc.
- TermService.
- UmRdpService.
- UserManager.
- UsoSvc.
- VaultSvc.
- W32Time.
- WebClient.
- Winmgmt.
- WlanSvc.
- wscsvc.

Для пользователей с ролью **Аудитор** создание задачи управления службами недоступно.
У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи выполнения приложения

Вы можете создать задачу запуска приложения или выполнения команды.

> Если при выполнении задачи файл стандартного вывода или файл вывода ошибок достигает размера 100 КБ, часть данных из файла удаляется. Файл будет содержать не все данные.

► *Чтобы создать задачу запуска приложения или выполнения команды:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Выполнить приложение**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. В полях **Путь к файлу** и **Рабочий каталог** ниже введите значения одним из следующих способов:

      - В поле **Путь к файлу** введите полный путь к исполняемому файлу (например, `C:\Windows\System32\ipconfig.exe`). Поле **Рабочий каталог** оставьте пустым.

        > При создании задачи приложение не проверяет на корректность указанный путь к исполняемому файлу.

      - В поле **Путь к файлу** введите имя и расширение исполняемого файла (например, `ipconfig.exe`). В поле **Рабочий каталог** укажите рабочую директорию (например, `C:\Windows\System32\`).

   b. В поле **Аргументы** введите дополнительные параметры запуска файла или выполнения команды (например, аргумент `/all`).

   c. В поле **Описание** введите описание задачи. Поле не является обязательным.

   d. Настройте параметр **Задача для** – область применения задачи:

      - Если вы хотите выполнить задачу на всех хостах всех серверов, выберите вариант **Всех хостов**.
      - Если вы хотите выполнить задачу на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите выполнить задачу.

        Этот вариант доступен только при включенном режиме распределенного решения и мультитенантности.

      - Если вы хотите выполнить задачу на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

4. Нажмите на кнопку **Добавить**.

Будет создана задача запуска приложения или выполнения команды. Задача запускается автоматически после создания.

Пример:

► *Чтобы выполнить команду `ipconfig /all` на хосте с IP-адресом `10.10.10.1`, выполните следующие действия:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Выполнить приложение**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. В полях **Путь к файлу** и **Рабочий каталог** ниже введите значения одним из следующих способов:

      - В поле **Путь к файлу** введите `C:\Windows\System32\ipconfig.exe`. Поле **Рабочий каталог** оставьте пустым.
      - В поле **Путь к файлу** введите `ipconfig.exe`. В поле **Рабочий каталог** введите `C:\Windows\System32\`.

   b. В поле **Аргументы** введите `/all`.

   c. В поле **Описание** введите описание задачи.

   d. Выберите область применения задачи **Выбранных хостов**.

   e. В поле **Хосты** введите несколько символов IP-адреса `10.10.10.1`, и когда этот IP-адрес появится в раскрывающемся списке результатов поиска ниже, выберите его.

4. Нажмите на кнопку **Добавить**.

Для пользователей с ролью **Аудитор** функция создания задачи запуска приложения или выполнения команды недоступна.
У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи удаления файла

► *Чтобы создать задачу удаления файла:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Удалить файл**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Путь к файлу** – путь к файлу, который вы хотите удалить.

Вы также можете указать путь к альтернативному потоку данных этого файла. В этом случае будет удален только указанный поток данных. Остальные потоки данных этого файла останутся без изменений.

b. **MD5/SHA256** – MD5- или SHA256-хеш файла, который вы хотите удалить. Поле не является обязательным.

c. **Описание** – описание задачи. Поле не является обязательным.

d. **Задача для** – область применения задачи:

- Если вы хотите выполнить задачу на всех хостах всех серверов, выберите вариант **Всех хостов**.
- Если вы хотите выполнить задачу на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите выполнить задачу.

  Этот вариант доступен только при включенном режиме распределенного решения и мультитенантности.
- Если вы хотите выполнить задачу на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

4. Нажмите на кнопку **Добавить**.

Будет создана задача удаления файла. Задача запускается автоматически после создания.

Если файл заблокирован другим процессом, то задача будет отображаться со статусом *Выполнено*, но сам файл будет удален только после перезагрузки хоста. Рекомендуется проверить успешность удаления файла после перезагрузки хоста.
Удаление файла с подключенного сетевого диска не поддерживается.
Для пользователей с ролью **Аудитор** создание задачи удаления файла недоступно.
У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи помещения файла на карантин

Если вы считаете, что на компьютере с компонентом Endpoint Agent находится зараженный или возможно зараженный файл, вы можете изолировать его, поместив на карантин.

► *Чтобы создать задачу помещения файла на карантин:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Поместить файл на карантин**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Путь к файлу** – путь к файлу, который вы хотите поместить на карантин.

   b. **MD5/SHA256** – MD5- или SHA256-хеш файла, который вы хотите поместить на карантин. Поле не является обязательным.

c. **Описание** – описание задачи. Поле не является обязательным.

d. **Хосты** – имя или IP-адрес хоста, на который вы хотите назначить задачу.

   Вы можете указать несколько хостов.

e. Нажмите на кнопку **Добавить**.

Будет создана задача помещения файла на карантин. Задача запускается автоматически после создания.

В результате выполнения задачи:

- Файл будет удален из папки компьютера, в которой он находится, и перемещен в директорию карантина на этом компьютере, указанную при настройке приложение, которое используется в качестве компонента Endpoint Agent.
- В списке задач раздела **Задачи** веб-интерфейса приложения появится информация о выполнении этой задачи.
- В списке файлов раздела **Хранилище** подраздела **Карантин** появится информация о помещении файла на карантин.

Если файл заблокирован другим процессом, то задача будет отображаться со статусом *Выполнено*, но сам файл будет помещен на карантин только после перезагрузки хоста. Рекомендуется проверить успешность выполнения задачи после перезагрузки хоста.

Задача помещения файла на карантин может завершиться с ошибкой **Доступ запрещен**, если вы пытаетесь поместить на карантин исполняемый файл и он запущен в настоящий момент.
Чтобы решить проблему, создайте задачу завершения процесса (см. раздел "Создание задачи завершения процесса" на стр. 469) для этого файла, а затем повторите попытку создания задачи помещения файла на карантин.

Для пользователей с ролью **Аудитор** функция создания задачи помещения файла на карантин недоступна.
У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи восстановления файла из карантина

Если вы считаете, что изолированный ранее файл безопасен, вы можете восстановить его из карантина (см. раздел "Работа с объектами в Хранилище и на карантине" на стр. 531) на хост.

► *Чтобы создать задачу восстановления файла из карантина:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Восстановить файл из карантина**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:
   a. **Описание** – описание задачи. Поле не является обязательным.
   b. **Поиск файлов** – имя файла, находящегося в карантине.
4. Нажмите на кнопку **Добавить**.

Будет создана задача восстановления файла из карантина. Задача запускается автоматически после создания.

После восстановления файла из карантина на хост метаданные о файле останутся в таблице объектов, помещенных в Хранилище.

В режиме распределенного решения и мультитенантности файл, помещенный на карантин (см. раздел "Создание задачи помещения файла на карантин" на стр. 478) сервера SCN, нельзя восстановить на сервере PCN. Вы можете восстановить файл на том сервере SCN, где была создана задача для помещения файла на карантин.
Для пользователей с ролью **Аудитор** функция создания задачи восстановления файла из карантина недоступна.
У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание копии задачи

► *Чтобы скопировать задачу:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.
2. Откройте задачу, которую вы хотите скопировать.
3. Нажмите на кнопку **Скопировать**.

   Откроется окно создания задачи. Все параметры задачи будут скопированы.
4. Если вы хотите изменить параметры задачи, внесите изменения для одного или нескольких параметров в зависимости от типа копируемой задачи.
5. Нажмите на кнопку **Добавить**.

Будет создана копия выбранной задачи.

Для пользователей с ролью **Аудитор** функция создания копии задачи недоступна.
У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Удаление задач

Если вы удалите задачу в процессе ее выполнения, результат выполнения задачи может не сохраниться.

Если вы удалите успешно выполненную задачу загрузки файла, файл будет удален.

► *Чтобы удалить задачу:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.
2. Откройте задачу, которую вы хотите удалить.
3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.
4. Нажмите на кнопку **Да**.

Задача будет удалена.

► *Чтобы удалить все или несколько задач:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.
2. Установите флажки напротив задач, которые вы хотите удалить.

   Вы можете выбрать все задачи, установив флажок в строке с заголовками столбцов.
3. В панели управления в нижней части окна нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.
4. Нажмите на кнопку **Да**.

Выбранные задачи будут удалены.

Для пользователей с ролью **Аудитор** функция удаления задачи недоступна.
У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Фильтрация задач по времени создания

► *Чтобы отфильтровать задачи по времени их создания:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.
2. По ссылке **Время** откройте меню фильтрации задач.
3. Выберите один из следующих периодов отображения задач:
   - **Все**, если вы хотите, чтобы приложение отображало в таблице все созданные задачи.
   - **Прошедший час**, если вы хотите, чтобы приложение отображало в таблице задачи, созданные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы приложение отображало в таблице задачи, созданные за предыдущий день.

- **Пользовательский диапазон**, если вы хотите, чтобы приложение отображало в таблице задачи, созданные за указанный вами период.

4. Если вы выбрали период отображения задач **Пользовательский диапазон**, выполните следующие действия:

   a. В открывшемся календаре укажите даты начала и конца периода отображения задач.

   b. Нажмите на кнопку **Применить**.

   Календарь закроется.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по типу

Если вы используете режим распределенного решения и мультитенантности, вы можете отфильтровать задачи по их типу.

► *Чтобы отфильтровать задачи по их типу:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.

2. По ссылке **Тип** откройте меню фильтрации задач.
3. Выберите один из следующих вариантов отображения задач:

   - **Все**, если вы хотите, чтобы отображались все задачи независимо от типа.
   - **Глобальный**, если вы хотите, чтобы отображались только задачи, созданные на сервере PCN. Действие этих задач распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Задачи относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
   - **Локальный**, если вы хотите, чтобы отображались только задачи, созданные на сервере SCN. Действие этих задач распространяется только на хосты, подключенные к этому серверу SCN. Задачи относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по имени

► *Чтобы отфильтровать задачи по имени:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.
2. По ссылке **Имя** откройте меню фильтрации задач.
3. Установите один или несколько флажков:
   - **Завершить процесс**.
   - **Выполнить приложение**.
   - **Собрать форензику**.
   - **Запустить YARA-проверку**.
   - **Управление службами**.
   - **Получить файл**.
   - **Удалить файл**.
   - **Поместить файл на карантин**.
   - **Восстановить файл**.
4. Нажмите на кнопку **Применить**.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по имени и пути к файлу

Вы можете фильтровать задачи по показателю **Сведения** – имя и путь к файлу или потоку данных.

► *Чтобы отфильтровать задачи по имени и пути к файлу или потоку данных:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.
2. По ссылке **Сведения** откройте окно настройки фильтрации задач.
3. В правом раскрывающемся списке выберите **Сведения**.
4. В левом раскрывающемся списке выберите один из следующих операторов фильтрации задач:
   - **Содержит**.
   - **Не содержит**.
   - **Равняется**.
   - **Не равняется**.

5. В поле ввода укажите один или несколько символов имени или пути к файлу.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
7. Нажмите на кнопку **Применить**.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по описанию

Вы можете фильтровать задачи по показателю **Описание** – описание задачи, которое было добавлено на этапе создания задачи.

► *Чтобы отфильтровать задачи по описанию:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.
2. По ссылке **Сведения** откройте окно настройки фильтрации задач.
3. В левом раскрывающемся списке выберите **Описание**.
4. В правом раскрывающемся списке выберите один из следующих операторов фильтрации задач:
   - **Содержит**.
   - **Не содержит**.
   - **Равняется**.
   - **Не равняется**.
5. В поле ввода укажите один или несколько символов имени или пути к файлу.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
7. Нажмите на кнопку **Применить**.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по имени сервера

Если вы используете режим распределенного решения и мультитенантности, вы можете отфильтровать задачи по серверам, на которые распространяется действие задач.

► *Чтобы отфильтровать задачи по серверам, на которые распространяется действие задач:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.
2. По ссылке **Серверы** откройте меню фильтрации задач.
3. Установите флажки рядом с именами тех серверов, задачи по которым вы хотите отобразить.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по имени пользователя, создавшего задачу

Фильтрация задач по имени пользователя, создавшего задачу, доступна только при отображении всех задач. Если вы включили отображение задач, созданных только текущим пользователем, фильтрация задач по имени пользователя недоступна.

► *Чтобы отфильтровать задачи по имени пользователя, создавшего задачу:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.
2. По ссылке **Автор** откройте меню фильтрации задач.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации задач:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов имени пользователя.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по состоянию обработки

► *Чтобы отфильтровать задачи по состоянию их обработки пользователем:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.
2. По ссылке **Состояние** откройте меню фильтрации задач.
3. Установите один или несколько флажков:
   - **Ожидает**.
   - **В обработке**.
   - **Завершено**.
4. Нажмите на кнопку **Применить**.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра задач

► *Чтобы сбросить фильтр задач по одному или нескольким условиям фильтрации:*

1. В окне веб-интерфейса приложения выберите раздел **Задачи**.

   Откроется таблица задач.
2. Нажмите на кнопку ☒ справа от того заголовка столбца таблицы, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Работа с политиками (правилами запрета)

При работе в веб-интерфейсе приложения пользователи с ролью **Старший сотрудник службы безопасности** могут управлять правилами запрета запуска файлов и процессов на выбранных хостах с помощью политик. Например, вы можете запретить запуск приложений, использование которых считаете небезопасным, на выбранном хосте с компонентом Endpoint Agent. Приложение идентифицирует файлы по их хешу с помощью алгоритмов хеширования MD5 и SHA256. Вы можете создавать, включать и отключать, удалять и изменять правила запрета. Кроме того, по ссылке с названием алгоритма хеширования в таблице правил запрета вы можете выполнять такие действия по поиску объектов, событий или обнаружений, по

которым сработали правила запрета, как **Найти события**, **Найти обнаружения**, **Найти на TIP** или **Найти на virustotal.com**.

В режиме распределенного решения и мультитенантности правила запрета могут быть следующих типов:

- **Глобальный** – созданные на PCN. Действие этих правил запрета распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Правила запрета относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
- **Локальный** – созданные на сервере SCN. Действие этих правил запрета распространяется только на хосты, подключенные к этому серверу SCN. Правила запрета относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

Пользователи с ролью **Старший сотрудник службы безопасности** могут создавать, редактировать, удалять, включать и отключать, а также импортировать правила запрета в рамках тех тенантов, к данным которых у них есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса приложения" на стр. 200).

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к политикам.

Пользователи с ролью **Аудитор** могут просматривать таблицу правил запрета запуска файлов и процессов, а также информацию о выбранном правиле запрета без возможности редактирования.

Все изменения в правилах запрета применяются на хостах после установки авторизованного соединения с выбранными хостами. Если соединение с хостами отсутствует, на хостах продолжают действовать старые правила запрета. Изменения в правилах запрета не влияют на уже запущенные процессы.

Правила запрета могут быть созданы автоматически на основе предустановленных политик (далее также "предустановок"), добавленных по умолчанию. При включенных предустановках приложение создает правило запрета на основе обнаружения компонента Sandbox со средним или высоким уровнем важности. Созданное правило запрета блокирует запуск файла по его MD5-хешу. Пользователи с ролью **Старший сотрудник службы безопасности** могут включать и отключать предустановки.

Предустановки не поддерживаются в режиме распределенного решения и мультитенантности.

Для правил запрета, которые были созданы автоматически или импортированы, доступны такие же операции, что и для правил, созданных вручную.

На каждый хеш файла можно создать только одно правило запрета.
Максимальное поддерживаемое количество правил запрета в системе составляет 50 000.

Правила запрета действуют, только когда компонент Endpoint Agent запущен на хосте. Если попытка запуска файла будет совершена до запуска компонента или после завершения работы компонента на хосте, то запуск файла не будет заблокирован.

Управление правилами запрета запуска файлов и процессов на выбранных хостах с помощью политик доступно только при интеграции компонента Endpoint Agent с сервером Central Node и осуществляется только через веб-интерфейс Kaspersky Anti Targeted Attack Platform.
Если в роли компонента Endpoint Agent вы используете Kaspersky Endpoint Security для Windows, вам нужно учитывать, что приложение поддерживает запрет запуска определенного набора расширений файлов офисного формата и набора интерпретаторов скриптов.

В этом разделе

Просмотр таблицы правил запрета 488
Настройка отображения таблицы правил запрета 489
Просмотр правила запрета 490
Создание правила запрета 491
Импорт правил запрета 492
Включение и отключение правила запрета 493
Включение и отключение предустановок 494
Удаление правил запрета 494
Фильтрация правил запрета по имени 495
Фильтрация правил запрета по типу 495
Фильтрация правил запрета по хешу файла 496
Фильтрация правил запрета по имени сервера 496
Сброс фильтра правил запрета 497

Просмотр таблицы правил запрета

Таблица правил запрета находится в разделе **Политики** окна веб-интерфейса приложения.

В таблице содержится следующая информация:

1. **Тип** – тип правила в зависимости от режима работы приложения и роли сервера, на котором оно создано:
   - **Глобальный** – созданные на PCN. Действие этих правил запрета распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Правила запрета относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
   - **Локальный** – созданные на сервере SCN. Действие этих правил запрета распространяется только на хосты, подключенные к этому серверу SCN. Правила запрета относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
2. **Имя** – имя правила запрета.
3. **Автор** – имя пользователя, под учетной записью которого было создано правило.

4. **Хеш файла** – алгоритм хеширования, применяющийся для идентификации файла.

   Идентификация файла может осуществляться по одному из следующих алгоритмов хеширования:

   - **MD5**.
   - **SHA256**.

   По ссылке с названием алгоритма хеширования раскрывается список, в котором вы можете посмотреть хеш файла, а также выбрать одно из следующих действий:

   - **Добавить в фильтр**.
   - **Исключить из фильтра**.
   - **Найти на TIP**.
   - **Найти на virustotal.com** (для SHA256).
   - **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).

     В результате выполнения этого действия откроется раздел **Поиск угроз** с событиями, уже отфильтрованными по выбранному вами хешу.
   - **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).

     В результате выполнения этого действия откроется раздел **Обнаружения** с обнаружениями, уже отфильтрованными по выбранному вами хешу.
   - **Включить правило запрета** (см. раздел "**Включение и отключение правила запрета**" на стр. 493).
   - **Отключить правило запрета** (см. раздел "**Включение и отключение правила запрета**" на стр. 493).
   - **Удалить правило запрета** (см. раздел "**Удаление правил запрета**" на стр. 494).
   - **Скопировать значение в буфер**.
5. **Серверы** – имена серверов с ролью PCN или SCN, на которые распространяется правило запрета.

   Поле отображается, если вы используете режим распределенного решения и мультитенантности.
6. **Хосты** – имя сервера с компонентом Central Node, на хосты которого распространяется правило запрета.

   Поле отображается, только когда вы используете отдельный сервер Central Node.
7. **Состояние** – текущее состояние правила запрета.

   Правило запрета может находиться в одном из следующих состояний:

   - **Включено**.
   - **Выключено**.

Настройка отображения таблицы правил запрета

Вы можете настроить отображение столбцов, а также порядок их следования в таблице правил запрета.

► *Чтобы настроить отображение таблицы правил запрета:*

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

Откроется таблица правил запрета.

2. В заголовочной части таблицы нажмите на кнопку .

   Отобразится окно **Настройка таблицы**.

3. Если вы хотите включить отображение столбца в таблице, установите флажок рядом с названием того параметра, который должен отображаться в таблице.

   Если вы не хотите, чтобы параметр отображался в таблице, снимите флажок.

   Должен быть установлен хотя бы один флажок.

4. Если вы хотите изменить порядок отображения столбцов в таблице, наведите курсор мыши на строку с нужным параметром, нажмите на кнопку и переместите строку с параметром в нужное место.

5. Если вы хотите восстановить параметры отображения таблицы по умолчанию, нажмите на ссылку **По умолчанию**.

6. Нажмите на кнопку **Применить**.

Отображение таблицы правил запрета будет настроено.

Просмотр правила запрета

► *Чтобы просмотреть правило запрета:*

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. Выберите правило запрета, которое вы хотите просмотреть.

Правило запрета содержит следующую информацию:

- **События** (см. раздел "**Информация о событиях**" на стр. 378) – ссылка, по которой открывается раздел **Поиск угроз** с условием поиска, содержащим выбранное вами правило запрета.
- **Состояние** – текущее состояние правила запрета.

  Правило запрета может находиться в одном из следующих состояний:

  - **Включено**.
  - **Выключено**.
- Закладка **Сведения** со следующей информацией:
  - **MD5/SHA256** – хеш файла, запрещенного к запуску.

    По ссылке **MD5/SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти на TIP**.
    - **Найти события**.
    - **Найти обнаружения**.

- **Скопировать значение в буфер**.
- **Имя** – имя правила запрета или файла, запрещенного к запуску.
- **Тип** – тип правила в зависимости от режима работы приложения и роли сервера, на котором оно создано:
  - **Глобальный** – созданные на PCN. Действие этих правил запрета распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Правила запрета относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
  - **Локальный** – созданные на сервере SCN. Действие этих правил запрета распространяется только на хосты, подключенные к этому серверу SCN. Правила запрета относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
- **Уведомление** – состояние параметра **Показывать пользователю уведомление о блокировке запуска файла**.
- **Запрет для** – список хостов, на которые распространяется правило запрета.

  Если запрет действует на всех хостах, отображается надпись **Всех хостов**.

- Закладка **Журнал изменений** содержит список изменений запрета: время изменения, имя пользователя, изменившего запрет, и действия над запретом.

Создание правила запрета

► *Чтобы создать правило запрета:*

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.
2. Нажмите на кнопку **Добавить**.
3. Выберите **Создать правило**.

   Откроется окно создания правила запрета.
4. Задайте значения следующих параметров:
   a. **Состояние** – состояние правила запрета:
      - Если вы хотите включить правило запрета, переведите переключатель в положение **Вкл**.
      - Если вы хотите отключить правило запрета, переведите переключатель в положение **Откл**.

   b. **MD5/SHA256** – MD5- или SHA256-хеш файла или потока данных, запуск которого вы хотите запретить.

   c. **Имя** – имя правила запрета.

   d. Если вы хотите, чтобы приложение выводило уведомление о срабатывании правила запрета пользователю компьютера, на который распространяется запрет, установите флажок **Показывать пользователю уведомление о блокировке запуска файла**.

   > Если вы установили флажок **Показывать пользователю уведомление о блокировке запуска файла**, при попытке запуска запрещенного файла пользователю будет показано уведомление о том, что сработало правило запрета запуска этого файла.

e. **Запрет для** – область применения правила запрета:

- Если вы хотите применить правило запрета на всех хостах всех серверов, выберите вариант **Всех хостов**.
- Если вы хотите применить правило запрета на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите применить правило запрета.

  Этот вариант доступен только при включенном режиме распределенного решения и мультитенантности.
- Если вы хотите применить правило запрета на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

Если в роли компонента Endpoint Agent вы используете приложение Kaspersky Endpoint Security для Linux, функция создания правила запрета недоступна. Если при создании правила запрета в качестве области применения правила вы выберете хост с приложением Kaspersky Endpoint Security для Linux или все хосты, правило запрета не будет применено или будет применено только к хостам с приложениями Kaspersky Endpoint Agent для Windows и Kaspersky Endpoint Security для Windows.

5. Нажмите на кнопку **Добавить**.

Будет создан запрет на запуск файла.

Вы также можете импортировать правила запрета (см. раздел "Импорт правил запрета" на стр. 492).

Для пользователей с ролью **Аудитор** функция создания правила запрета на запуск файла недоступна. У пользователей с ролью **Сотрудник службы безопасности** нет доступа к правилам запрета.

Импорт правил запрета

Вы можете импортировать файл с MD5- и SHA256-хешами файлов, запуск которых хотите запретить. Для каждого хеша Kaspersky Anti Targeted Attack Platform создаст отдельное правило запрета.

Максимальный размер импортируемого файла - 10 МБ. На одной строке должен располагаться только один хеш.

► *Чтобы импортировать правила запрета:*

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.
2. Нажмите на кнопку **Добавить**.
3. Выберите **Импортировать правила**.

   Откроется окно импорта правил запрета.

4. Задайте значения следующих параметров:
   a. **Состояние** – состояние правила запрета:
      - Если вы хотите включить все импортированные правила запрета, переведите переключатель в положение **Вкл**.
      - Если вы хотите отключить все импортированные правила запрета, переведите переключатель в положение **Откл**.
   b. Если вы хотите, чтобы приложение выводило уведомление о срабатывании правил запрета пользователю компьютера, на который распространяется запрет, установите флажок **Показывать пользователю уведомление о блокировке запуска файла**.

   Поле **Запрет для** недоступно для редактирования. По умолчанию правила запрета, созданные на сервере PCN, распространяются на все хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN (если вы используете режим распределенного решения и мультитенантности).

5. Загрузите файл с хешами файлов, для которых вы хотите создать правила запрета, с помощью кнопки **Обзор**.

   Откроется окно выбора файлов.
6. Выберите файл, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.
7. Нажмите на кнопку **Добавить**.

Правила будут импортированы.

Для пользователей с ролью **Аудитор** функция импорта правил запрета на запуск файла недоступна.
У пользователей с ролью **Сотрудник службы безопасности** нет доступа к правилам запрета.

Включение и отключение правила запрета

► *Чтобы включить или отключить правило запрета:*

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.
2. В строке с правилом запрета, которое вы хотите включить или отключить, в столбце **Состояние** выполните одно из следующих действий:
   - Если вы хотите включить правило запрета, переведите переключатель в положение **Включено**.

     Выбранное вами правило запрета будет включено.
   - Если вы хотите отключить правило запрета, переведите переключатель в положение **Выключено**.

     Выбранное вами правило запрета будет отключено.

Для пользователей с ролью **Аудитор** функция включения и отключения правил запрета недоступна.
У пользователей с ролью **Сотрудник службы безопасности** нет доступа к правилам запрета запуска файлов и процессов на выбранных хостах с помощью политик.

Включение и отключение предустановок

► *Чтобы включить или отключить предустановки:*

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.
2. Выберите закладку **Предустановки**.
3. В строке с предустановкой, которую вы хотите включить или отключить, в столбце **Состояние** переведите переключатель в положение **Включено** или **Выключено**.

Предустановка будет включена или отключена. При отключении предустановки все ранее автоматически созданные правила запрета сохранятся.

Удаление правил запрета

Вы можете удалить одно или несколько правил запрета, а также все правила запрета сразу.

► *Чтобы удалить одно правило запрета:*

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.
2. Нажмите на правило запрета, которое вы хотите удалить.

   Откроется окно сведений о правиле запрета.
3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.
4. Нажмите на кнопку **Да**.

Правило запрета будет удалено.

► *Чтобы удалить все или несколько правил запрета:*

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.
2. Установите флажки напротив правил запрета, которые вы хотите удалить.

   Вы можете выбрать все правила запрета, установив флажок в строке с заголовками столбцов.
3. В панели управления в нижней части окна нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.
4. Нажмите на кнопку **Да**.

Выбранные правила запрета будут удалены.

Для пользователей с ролью **Аудитор** функция удаления правил запрета недоступна.
У пользователей с ролью **Сотрудник службы безопасности** нет доступа к правилам запрета запуска файлов и процессов на выбранных хостах с помощью политик.

Фильтрация правил запрета по имени

► *Чтобы отфильтровать правила запрета по имени:*

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.
2. По ссылке **Имя** откройте меню фильтрации запретов.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации запретов:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов имени правила запрета.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице правил запрета отобразятся только правила запрета, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация правил запрета по типу

Если вы используете режим распределенного решения и мультитенантности, вы можете отфильтровать правила запрета по их типу.

► *Чтобы отфильтровать правила запрета по типу:*

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.
2. По ссылке **Тип** откройте меню фильтрации правил запрета.
3. Выберите один из следующих вариантов отображения правил запрета:
   - **Все**, если вы хотите, чтобы отображались все правила запрета независимо от типа.

- **Глобальный**, если вы хотите, чтобы отображались только правила запрета, созданные на PCN. Действие этих правил запрета распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Правила запрета относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе приложения.
- **Локальный**, если вы хотите, чтобы отображались только правила запрета, созданные на сервере SCN. Действие этих правил запрета распространяется только на хосты, подключенные к этому серверу SCN. Правила запрета относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе приложения.

В таблице правил запрета отобразятся только правила запрета, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация правил запрета по хешу файла

► *Чтобы отфильтровать правила запрета по хешу файла:*

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.
2. По ссылке **Хеш файла** откройте меню фильтрации правил запрета.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации запретов:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов хеша файла.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице правил запрета отобразятся только правила запрета, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация правил запрета по имени сервера

Если вы используете режим распределенного решения и мультитенантности, вы можете отфильтровать правила запрета по серверам, на которые распространяется действие правил запрета.

► *Чтобы отфильтровать правила запрета по имени сервера:*

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.
2. По ссылке **Серверы** откройте меню фильтрации правил запрета.
3. Установите флажки напротив тех серверов, по которым вы хотите отфильтровать правила запрета.
4. Нажмите на кнопку **Применить**.

В таблице правил запрета отобразятся только правила запрета, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра правил запрета

► *Чтобы сбросить фильтр правил запрета по одному или нескольким условиям фильтрации:*

1. В окне веб-интерфейса приложения выберите раздел **Политики**.

   Откроется таблица правил запрета.
2. Нажмите на кнопку ☒ справа от того заголовка столбца таблицы правил запрета, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице правил запрета отобразятся только правила запрета, соответствующие заданным вами условиям.

Работа с пользовательскими правилами

Вы можете настроить дополнительную защиту IT-инфраструктуры организации с помощью пользовательских правил **TAA** (см. раздел "**Работа с пользовательскими правилами TAA (IOA)**" на стр. 500), **IDS** (см. раздел "**Работа с пользовательскими правилами IDS**" на стр. 520), **IOC** (см. раздел "**Работа с пользовательскими правилами IOC**" на стр. 512) и **YARA** (см. раздел "**Работа с пользовательскими правилами YARA**" на стр. 524).

Пользователи с ролью **Старший сотрудник службы безопасности** могут работать с пользовательскими правилами **TAA**, **IDS**, **IOC** и **YARA**: загружать и удалять файлы правил, просматривать списки правил, редактировать выбранные правила.

Пользователи с ролью **Аудитор** могут просматривать списки пользовательских правил **TAA**, **IDS**, **IOC** и **YARA** и свойства выбранных правил без возможности редактирования.

Пользователи с ролью **Сотрудник службы безопасности** могут просматривать списки пользовательских правил **TAA**, **IOC** и **YARA** и свойства выбранных правил без возможности редактирования.

В этом разделе

Об использовании индикаторов компрометации (IOC) и атаки (IOA) для поиска угроз 499

Работа с пользовательскими правилами TAA (IOA) 500

Работа с пользовательскими правилами IOC 512

Работа с пользовательскими правилами IDS 520

Работа с пользовательскими правилами YARA 524

Об использовании индикаторов компрометации (IOC) и атаки (IOA) для поиска угроз

Kaspersky Anti Targeted Attack Platform использует для поиска угроз два типа индикаторов – *IOC* (Indicator of Compromise, или индикатор компрометации) и *IOA* (Indicator of Attack, или индикатор атаки).

Индикатор IOC – это набор данных о вредоносном объекте или действии. Kaspersky Anti Targeted Attack Platform использует IOC-файлы открытого стандарта описания индикаторов компрометации OpenIOC. IOC-файлы содержат набор индикаторов, при совпадении с которыми приложение считает событие обнаружением. Вероятность обнаружения может повыситься, если в результате проверки были найдены точные совпадения данных об объекте с несколькими IOC-файлами.

Индикатор IOA – это правило (далее также "правило TAA (IOA)"), содержащее описание подозрительного поведения в системе, которое может являться признаком целевой атаки. Kaspersky Anti Targeted Attack Platform проверяет базу событий (см. раздел "Информация о событиях" на стр. 378) приложения и отмечает события, которые совпадают с поведением, описанным в правилах TAA (IOA). При проверке используется технология *потоковой проверки*, при которой объекты, загружаемые из сети, проверяются непрерывно в режиме реального времени.

Правила TAA (IOA), сформированные специалистами "Лаборатории Касперского", используются в работе технологии TAA (Targeted Attack Analyzer) и обновляются вместе с базами приложения. Они не отображаются в интерфейсе приложения и не могут быть отредактированы.

Вы можете добавлять пользовательские правила IOC (см. раздел "Работа с пользовательскими правилами IOC" на стр. 512) и TAA (IOA) (см. раздел "Работа с пользовательскими правилами TAA (IOA)" на стр. 500), используя IOC-файлы открытого стандарта описания OpenIOC, а также создавать правила TAA (IOA) на основе условий поиска по базе событий (см. раздел "Создание правила TAA (IOA) на основе условий поиска событий" на стр. 377).

Сравнительные характеристики индикаторов компрометации (IOC) и атаки (IOA) приведены в таблице ниже.

Таблица 41. Сравнительные характеристики индикаторов IOC и IOA

Сравнительная характеристика	Индикаторы IOC в пользовательских правилах IOC	Индикаторы IOA в пользовательских правилах TAA (IOA)	Индикаторы IOA в правилах TAA (IOA), сформированных специалистами "Лаборатории Касперского"
Область проверки	Компьютеры с компонентом Endpoint Agent	База событий приложения	База событий приложения
Механизм проверки	Периодическая проверка	Потоковая проверка	Потоковая проверка
Возможность добавить в исключения из проверки	Нет.	Не требуется. Пользователи с ролью **Старший сотрудник службы безопасности** могут изменить (см. раздел "Изменение правила TAA (IOA)" на стр. 511) текст индикатора в пользовательских правилах TAA (IOA) согласно требуемым условиям.	Есть.

Если вы используете режим распределенного решения и мультитенантности, в разделе отображаются данные по выбранному вами тенанту.

Работа с пользовательскими правилами TAA (IOA)

Пользовательские правила TAA (IOA) создаются на основе условий поиска по базе событий. Например, если вы хотите, чтобы Kaspersky Anti Targeted Attack Platform формировала обнаружения по событиям запуска приложения, которое вы считаете небезопасным, на компьютерах с компонентом Endpoint Agent, вы можете выполнить следующие действия:

1. Сформировать поисковый запрос по базе событий (см. раздел "Поиск угроз по базе событий" на стр. 366).
2. Создать правило TAA (IOA) на основе условий поиска событий (см. раздел "Создание правила TAA (IOA) на основе условий поиска событий" на стр. 377).

   При поступлении на сервер Central Node событий, соответствующих созданному правилу TAA (IOA), Kaspersky Anti Targeted Attack Platform сформирует обнаружения.

Вы также можете создать правило TAA (IOA) на основе одного или нескольких условий поиска событий из выбранного IOC-файла. Для этого вам требуется выполнить следующие действия:

1. Загрузить в веб-интерфейс Kaspersky Anti Targeted Attack Platform IOC-файл с индикаторами компрометации для вредоносного приложения (см. раздел "Загрузка IOC-файла" на стр. 516).
2. Найти события, соответствующие условиям выбранного IOC-файла (см. раздел "Поиск событий по IOC-файлу" на стр. 518).
3. Создать на основе одного или нескольких условий поиска событий из выбранного IOC-файла правило TAA (IOA) (см. раздел "Создание правила TAA (IOA) на основе условий поиска событий" на стр. 377).

В режиме распределенного решения и мультитенантности правила TAA (IOA) могут быть одного из следующих типов:

- **Глобальный** – созданные на сервере PCN. По этим правилам производится проверка событий на этом сервере PCN и на всех серверах SCN, подключенных к этому серверу PCN. Проверяемые события относятся к тенантам, в рамках которых пользователь работает в веб-интерфейсе программы.
- **Локальный** – созданные на сервере SCN. По этим правилам производится проверка событий на этом сервере SCN. Проверяемые события относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

Различия между пользовательскими правилами и правилами "Лаборатории Касперского" представлены в таблице ниже.

Таблица 42. Сравнительные характеристики правил ТАА (IOA)

Сравнительная характеристика	Пользовательские правила ТАА (IOA)	Правила ТАА (IOA) "Лаборатории Касперского"
Наличие рекомендаций по реагированию на событие	Нет	Есть Вы можете посмотреть рекомендации в информации об обнаружении (см. раздел "Просмотр обнаружений" на стр. 350)
Соответствие технике в базе MITRE ATT&CK	Нет	Есть Вы можете посмотреть описание техники по классификации MITRE в информации об обнаружении (см. раздел "Просмотр обнаружений" на стр. 350)
Отображение в таблице правил ТАА (IOA)	Да	Нет
Способ отключить проверку базы по этому правилу	Отключить правило (см. раздел "Включение и отключение использования правил ТАА (IOA)" на стр. 510)	Добавить правило в исключения ТАА (см. раздел "Добавление правила ТАА (IOA) в исключения" на стр. 579)
Возможность удалить или добавить правило	Вы можете удалить (см. раздел "Удаление правил ТАА (IOA)" на стр. 511) или добавить (см. раздел "Создание правила ТАА (IOA) на основе условий поиска событий" на стр. 377) правило в веб-интерфейсе приложения	Правила обновляются вместе с базами приложения и не могут быть удалены пользователем
Поиск обнаружений и событий, в которых сработали правила ТАА (IOA) (на стр. 507)	По ссылкам **Обнаружения** и **События** в окне с информацией о правиле ТАА (IOA) (см. раздел "Просмотр информации о правиле ТАА (IOA)" на стр. 506)	По ссылкам **Обнаружения** и **События** в окне с информацией об обнаружении (см. раздел "Информация в блоке Результаты проверки" на стр. 354)

Пользователи с ролью **Старший сотрудник службы безопасности** могут создавать (см. раздел "Создание правила ТАА (IOA) на основе условий поиска событий" на стр. 377), импортировать (см. раздел "Импорт правила ТАА (IOA)" на стр. 505), удалять (см. раздел "Удаление правил ТАА (IOA)" на стр. 511), включать и выключать (см. раздел "Включение и отключение использования правил ТАА (IOA)" на стр. 510) правила ТАА (IOA), а также добавлять правила ТАА (IOA) "Лаборатории Касперского" в исключения из проверки. Пользователи с ролями **Сотрудник службы безопасности** и **Аудитор** могут использовать правила ТАА (IOA) для поиска признаков целевых атак (см. раздел "Поиск обнаружений и событий, в которых сработали правила ТАА (IOA)" на стр. 507), зараженных и возможно зараженных объектов в базе событий (см. раздел "Информация о событиях" на стр. 378) и обнаружений (см. раздел "Просмотр таблицы обнаружений" на стр. 331), а также просматривать таблицу правил ТАА (IOA) (см. раздел "Просмотр таблицы правил ТАА

(IOA)" на стр. 503) и информацию о правилах ТАА (IOA) (см. раздел "Просмотр информации о правиле ТАА (IOA)" на стр. 506).

В этом разделе

Просмотр таблицы правил ТАА (IOA) 503

Создание правила ТАА (IOA) на основе условий поиска событий 504

Импорт правила ТАА (IOA) 505

Просмотр информации о правиле ТАА (IOA) 506

Поиск обнаружений и событий, в которых сработали правила ТАА (IOA) 507

Фильтрация и поиск правил ТАА (IOA) 508

Сброс фильтра правил ТАА (IOA) 510

Включение и отключение использования правил ТАА (IOA) 510

Изменение правила ТАА (IOA) 511

Удаление правил ТАА (IOA) 511

Просмотр таблицы правил ТАА (IOA)

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Таблица пользовательских правил ТАА (IOA) содержит информацию о правилах ТАА (IOA), используемых для проверки событий и создания обнаружений, и находится в разделе **Пользовательские правила**, подразделе **ТАА** окна веб-интерфейса приложения.

В таблице содержится следующая информация:

1. – степень важности, которая будет присвоена обнаружению, произведенному с использованием этого правила ТАА (IOA).

   Степень важности может иметь одно из следующих значений:

   - – **Низкая**.
   - – **Средняя**.
   - – **Высокая**.

2. **Тип** – тип правила в зависимости от режима работы приложения и роли сервера, на котором оно создано:

   - **Глобальный** – созданные на сервере PCN. По этим правилам производится проверка событий на этом сервере PCN и на всех серверах SCN, подключенных к этому серверу PCN. Проверяемые события относятся к тенантам, в рамках которых пользователь работает в веб-интерфейсе программы.

- **Локальный** – созданные на сервере SCN. По этим правилам производится проверка событий на этом сервере SCN. Проверяемые события относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

3. **Надежность** – уровень надежности в зависимости от вероятности ложных срабатываний правила:
   - **Высокая**.
   - **Средняя**.
   - **Низкая**.

   Чем выше надежность, тем меньше вероятность ложных срабатываний
4. **Имя** – название правила.
5. **Серверы** – имя сервера с ролью PCN или SCN, на который распространяется правило.

   Столбец отображается, если вы используете режим распределенного решения и мультитенантности.
6. **Обнаружения** – требование сохранять информацию об обнаружении на основе совпадения события из базы с критериями правила.
   - **Включено** – для события создается запись в таблице обнаружений с указанием технологии Targeted Attack Analyzer (TAA).
   - **Выключено** – не отображается в таблице обнаружений.
7. **Состояние** – состояние использования правила при проверке событий:
   - **Включено** – правило используется.
   - **Выключено** – правило не используется.

Создание правила TAA (IOA) на основе условий поиска событий

► *Чтобы создать правило TAA (IOA) на основе условий поиска событий:*

1. В окне веб-интерфейса приложения выберите раздел **Поиск угроз**.

   Откроется форма поиска событий.
2. Выполните поиск событий в режиме конструктора или режиме исходного кода.
3. Нажмите на кнопку **Сохранить как правило TAA (IOA)**.

   Откроется окно **Новое правило TAA (IOA)**.
4. В поле **Имя** введите имя правила.
5. Нажмите на кнопку **Сохранить**.

Условие поиска событий будет сохранено. В таблице правил TAA (IOA) раздела **Пользовательские правила**, в подразделе **TAA** веб-интерфейса отобразится новое правило с заданным именем.

Не рекомендуется в условиях поиска событий, сохраняемых как пользовательское правило TAA (IOA), использовать следующие поля:

- IOAId.
- IOATag.
- IOATechnique.

- IOATactics.
- IOAImportance.
- IOAConfidence.

На момент сохранения пользовательского правила TAA (IOA) в приложении может не быть событий, содержащих данные для этих полей. Когда события с этими данными появятся, пользовательское правило TAA (IOA), созданное ранее, не сможет разметить события по этим полям.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция создания правила TAA (IOA) на основе условий поиска событий недоступна.

Импорт правила TAA (IOA)

Вы можете импортировать файл формата IOC и использовать его для проверки событий и создания обнаружений Targeted Attack Analyzer.

Настоятельно рекомендуется проверить работу пользовательских правил в тестовой среде перед импортом. Пользовательские правила TAA (IOA) могут вызвать проблемы производительности, в случае которых стабильная работа Kaspersky Anti Targeted Attack Platform не гарантируется

► *Чтобы импортировать правило TAA (IOA):*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).
2. Нажмите на кнопку **Импортировать**.

   Откроется окно выбора файла на вашем локальном компьютере.
3. Выберите файл, который вы хотите загрузить и нажмите на кнопку **Открыть**.

   Откроется окно **Новое правило TAA (IOA)**.
4. Переместите переключатель **Состояние** в положение **Включено**, если вы хотите включить использование правила при проверке базы событий.
5. На закладке **Сведения** в поле **Имя** введите имя правила.
6. В поле **Описание** введите любую дополнительную информацию о правиле.
7. В раскрывающемся списке **Важность** выберите степень важности, которая будет присвоена обнаружению, выполненному по этому правилу TAA (IOA):
   - **Низкая**.
   - **Средняя**.
   - **Высокая**.
8. В раскрывающемся списке **Надежность** выберите уровень надежности этого правила, по вашей оценке:
   - **Низкая**.
   - **Средняя**.

- **Высокая**.

9. В блоке параметров **Область применения** установите флажки напротив тех серверов, на которых вы хотите применить правило.
10. На закладке **Запрос** проверьте заданные условия поиска. Если требуется, внесите изменения.
11. Нажмите на кнопку **Сохранить**.

Пользовательское правило TAA (IOA) будет импортировано в приложение.

Вы также можете добавить правило TAA (IOA), сохранив условия поиска по базе событий (см. раздел "Создание правила TAA (IOA) на основе условий поиска событий" на стр. 377) в разделе **Поиск угроз**.

Просмотр информации о правиле TAA (IOA)

► *Чтобы просмотреть информацию о правиле TAA (IOA):*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).
2. Выберите правило, информацию о котором вы хотите просмотреть.

Откроется окно с информацией о правиле.

Окно содержит следующую информацию:

- **Обнаружения** – по ссылке в новой вкладке браузера откроется таблица обнаружений, отфильтрованных по технологии Targeted Attack Analyzer (см. раздел "Фильтрация и поиск обнаружений по названию технологии" на стр. 340) и имени правила TAA (IOA) (см. раздел "Фильтрация и поиск обнаружений по полученной информации" на стр. 338), с которым вы работаете.
- **События** – по ссылке в новой вкладке браузера откроется таблица событий (см. раздел "Информация о событиях" на стр. 378), отфильтрованных по имени правила.
- **Запрос** – по ссылке в новой вкладке браузера откроется таблица событий (см. раздел "Информация о событиях" на стр. 378), отфильтрованных по имени правила. В условиях поиска событий указаны данные из правила TAA (IOA), с которым вы работаете. Например, `EventType=Запущен процесс AND FileName CONTAINS <имя правила, с которым вы работаете>`. Вы можете отредактировать запрос на поиск событий (см. раздел "Изменение условий поиска событий" на стр. 374).
- **IOA ID** – по ссылке открывается идентификатор, присваиваемый приложением каждому правилу.

  Изменение идентификатора недоступно. Вы можете скопировать идентификатор по кнопке **Скопировать значение в буфер**.
- **Состояние** – использование правила при проверке базы событий.

На закладке **Сведения** отображается следующая информация:

- **Имя** – имя правила, которое вы указали при добавлении правила.
- **Описание** – любая дополнительная информация о правиле, которую вы указали.

- **Важность** – оценка возможного влияния события на безопасность компьютеров или локальной сети организации, указанная пользователем при добавлении правила.
- **Надежность** – уровень надежности в зависимости от вероятности ложных срабатываний, заданный пользователем при добавлении правила.
- **Тип** – тип правила в зависимости от роли сервера, на котором оно создано:
  - **Глобальный** – созданные на сервере PCN. По этим правилам производится проверка событий на этом сервере PCN и на всех серверах SCN, подключенных к этому серверу PCN. Проверяемые события относятся к тенантам, в рамках которых пользователь работает в веб-интерфейсе программы.
  - **Локальный** – созданные на сервере SCN. По этим правилам производится проверка событий на этом сервере SCN. Проверяемые события относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
- **Область применения** – имена серверов с компонентом Central Node, на которых применяется правило.

На закладке **Запрос** отображается исходный код запроса, по которому осуществляется проверка. По ссылке **Запрос** в верхней части окна вы можете перейти в раздел **Поиск угроз** и выполнить запрос на поиск событий.

Поиск обнаружений и событий, в которых сработали правила TAA (IOA)

► *Чтобы найти и просмотреть обнаружения и события, при создании которых сработало пользовательское правило TAA (IOA):*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).
2. Выберите правило, результат срабатывания которого вы хотите просмотреть.

   Откроется окно с информацией о правиле.
3. Выполните одно из следующих действий:
   - Если вы хотите просмотреть обнаружения, при создании которых сработало правило TAA (IOA), по ссылке **Обнаружения** перейдите в базу обнаружений.

     Откроется новая вкладка браузера с таблицей найденных обнаружений.
   - Если вы хотите просмотреть события, при создании которых сработало правило TAA (IOA), по ссылке **События** перейдите в базу событий.

     Откроется новая вкладка браузера с таблицей найденных событий.

► *Чтобы найти и просмотреть обнаружения и события, при создании которых сработало правило TAA (IOA) "Лаборатории Касперского", выполните следующие действия:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. По ссылке в столбце **Технологии** откройте окно настройки фильтрации.
3. В раскрывающемся списке слева выберите **Содержит**.

4. В раскрывающемся списке справа выберите технологию **(TAA) Targeted Attack Analyzer**.
5. Нажмите на кнопку **Применить**.

   В таблице отобразятся обнаружения, выполненные технологией TAA на основе правил TAA (IOA).
6. Выберите обнаружение, для которого в столбце **Обнаружено** отображается название нужного правила.

   Откроется окно с информацией об обнаружении.
7. В блоке **Результаты проверки** по ссылке с названием правила откройте окно с информацией о правиле.
8. Выполните одно из следующих действий:
   - Если вы хотите просмотреть обнаружения, при создании которых сработало правило TAA (IOA), по ссылке **Обнаружения** перейдите в базу обнаружений.

     Откроется новая вкладка браузера с таблицей найденных обнаружений.
   - Если вы хотите просмотреть события, при создании которых сработало правило TAA (IOA), по ссылке **События** перейдите в базу событий.

     Откроется новая вкладка браузера с таблицей найденных событий.

Фильтрация и поиск правил TAA (IOA)

► *Чтобы отфильтровать или найти правила TAA (IOA) по требуемым критериям:*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).
2. Выполните следующие действия в зависимости от критерия фильтрации:
   - **По степени важности**

a. По значку откройте окно настройки фильтрации IOA-правил.

b. Установите флажки напротив тех степеней важности, которые вы хотите включить в критерии фильтрации:
   - **Низкая**.
   - **Средняя**.
   - **Высокая**.

c. Нажмите на кнопку **Применить**.
   - **По типу правила**

d. По ссылке **Тип** откройте окно настройки фильтрации.

e. Выберите один из следующих элементов:
   - **Все** – все правила.
   - **Глобальный** – правила, созданные на сервере PCN. По этим правилам производится проверка событий на этом сервере PCN и на всех серверах SCN, подключенных к этому серверу PCN. Проверяемые события относятся к тенантам, в рамках которых пользователь работает в веб-интерфейсе программы.

- **Локальный** – правила, созданные на сервере SCN. По этим правилам производится проверка событий на этом сервере SCN. Проверяемые события относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
- **По уровню надежности**

f. По ссылке **Надежность** откройте окно настройки фильтрации.

g. Установите флажки напротив тех уровней надежности, которые вы хотите включить в критерии фильтрации:

- **Низкая**.
- **Средняя**.
- **Высокая**.

h. Нажмите на кнопку **Применить**.

- **По имени правила**

i. По ссылке **Тег IOA** откройте окно настройки фильтрации.

j. Введите один или несколько символов названия IOA-правила.

k. Нажмите на кнопку **Применить**.

- **По имени сервера**

l. По ссылке **Серверы** откройте окно настройки фильтрации.

m. Установите флажки напротив тех тенантов или серверов внутри тенантов, которые вы хотите включить в критерии фильтрации.

n. Нажмите на кнопку **Применить**.

- **По созданию обнаружений на основе правила**

o. По ссылке **Обнаружения** раскройте список настройки фильтрации.

p. Выберите один из следующих вариантов:

- **Все**.
- **Включено**.
- **Выключено**.
- **По состоянию правила**

q. По ссылке **Состояние** раскройте список настройки фильтрации.

r. Выберите один из следующих вариантов:

- **Все**.
- **Включено**.
- **Выключено**.

В таблице отобразятся только правила, соответствующие заданным условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра правил ТАА (IOA)

► *Чтобы сбросить фильтр правил ТАА (IOA) по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **ТАА**.

   Откроется таблица правил ТАА (IOA).

2. Нажмите на кнопку ☒ справа от того заголовка столбца таблицы правил, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице отобразятся только правила, соответствующие заданным условиям.

Включение и отключение использования правил ТАА (IOA)

Пользователи с ролью **Старший сотрудник службы безопасности** могут включить или отключить использование одного или нескольких правил, а также всех правил сразу.

► *Чтобы включить или отключить использование правила ТАА (IOA) при проверке событий:*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **ТАА**.

   Откроется таблица правил ТАА (IOA).

2. В строке с нужным правилом в столбце **Состояние** включите или выключите переключатель.

Использование правила при проверке событий будет включено или отключено.

► *Чтобы включить или отключить использование всех или нескольких правил ТАА (IOA) при проверке событий:*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **ТАА**.

   Откроется таблица правил ТАА (IOA).

2. Установите флажки слева от правил, использование которых вы хотите включить или отключить.

   Вы можете выбрать все правила, установив флажок в строке с заголовками столбцов.

   В нижней части окна отобразится панель управления.

3. Нажмите на кнопку **Включить** или **Отключить**, чтобы включить или отключить использование всех правил.

Использование выбранных правил при проверке событий будет включено или отключено.

В режиме распределенного решения и мультитенантности на сервере PCN доступно управление только глобальными правилами TAA (IOA). Управление локальными правилами TAA (IOA) доступно на серверах SCN тех тенантов, к которым у вас есть доступ.
Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** включение и отключение правил TAA (IOA) недоступно.

Изменение правила TAA (IOA)

Пользователи с ролью **Старший сотрудник службы безопасности** могут изменять пользовательские правила TAA (IOA). Изменение правил "Лаборатории Касперского" недоступно.

При работе в режиме распределенного решения и мультитенантности вы можете изменять только те правила TAA (IOA), которые были созданы на текущем сервере. Это значит, что в веб-интерфейсе PCN доступно изменение только правил, созданных на PCN. В веб-интерфейсе SCN доступно изменение только правил, созданных на SCN.

► *Чтобы изменить правило TAA (IOA):*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).

2. Выберите правило, которое вы хотите изменить.

   Откроется окно с информацией об этом правиле.

3. Внесите необходимые изменения.
4. Нажмите на кнопку **Сохранить**.

Параметры правила будут изменены.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция изменения правила TAA (IOA) на основе условий поиска событий недоступна.

Удаление правил TAA (IOA)

Пользователи с ролью **Старший сотрудник службы безопасности** могут удалить одно или несколько пользовательских правил TAA (IOA), а также все правила сразу.

При работе в режиме распределенного решения и мультитенантности вы можете удалять только те правила TAA (IOA), которые были созданы на текущем сервере. Это значит, что в веб-интерфейсе PCN доступно удаление только правил, созданных на PCN. В веб-интерфейсе SCN доступно удаление только правил, созданных на SCN.

► *Чтобы удалить пользовательское правило ТАА (IOA):*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **ТАА**.

   Откроется таблица правил ТАА (IOA).

2. Выберите правило, которое вы хотите удалить.

   Откроется окно с информацией об этом правиле.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Правило будет удалено.

► *Чтобы удалить все или несколько пользовательских правил ТАА (IOA):*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **ТАА**.

   Откроется таблица правил ТАА (IOA).

2. Установите флажки слева от правил, которые вы хотите удалить.

   Вы можете выбрать все правила, установив флажок в строке с заголовками столбцов.

   В нижней части окна отобразится панель управления.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Выбранные правила будут удалены.

Вы не можете удалять правила ТАА (IOA) "Лаборатории Касперского". Если вы не хотите использовать при проверке правило ТАА (IOA) "Лаборатории Касперского", вам требуется добавить его в исключения (см. раздел "Добавление правила ТАА (IOA) в исключения" на стр. 579).
Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция изменения правила ТАА (IOA) на основе условий поиска событий недоступна.

Работа с пользовательскими правилами IOC

Вы можете использовать IOC-файлы для поиска индикаторов компрометации по базе событий и на компьютерах с компонентом Endpoint Agent. Например, если вы получили из внешних источников информацию о распространении вредоносного приложения, вы можете выполнить следующие действия:

1. Загрузить в веб-интерфейс Kaspersky Anti Targeted Attack Platform IOC-файл с индикаторами компрометации для вредоносного приложения (см. раздел "Загрузка IOC-файла" на стр. 516).
2. Найти события, соответствующие условиям выбранного IOC-файла (см. раздел "Поиск событий по IOC-файлу" на стр. 518).

Вы можете просмотреть эти события и, если вы хотите, чтобы приложение Kaspersky Anti Targeted Attack Platform формировало обнаружения по выбранным событиям, вы можете создать правило TAA (IOA) (см. раздел "Создание правила TAA (IOA) на основе условий поиска событий" на стр. 377).

3. Включить автоматическое использование выбранного IOC-файла для поиска индикаторов компрометации на компьютерах с компонентом Endpoint Agent (см. раздел "Включение и отключение автоматического использования IOC-файла при проверке хостов" на стр. 517).

   Если в результате проверки компьютеров компонент Endpoint Agent обнаружит индикаторы компрометации, приложение Kaspersky Anti Targeted Attack Platform сформирует обнаружение.

4. Настроить расписание поиска индикаторов компрометации с помощью IOC-файлов на компьютерах с компонентом Endpoint Agent (см. раздел "Настройка расписания IOC-проверки" на стр. 519).

В режиме распределенного решения и мультитенантности IOC-файлы могут быть следующих типов:

- **Локальный** – IOC-файлы, загруженные на сервер SCN. По этим IOC-файлам производится поиск индикаторов компрометации на хостах с программой Kaspersky Endpoint Agent, подключенных к этому серверу SCN.
- **Глобальный** – IOC-файлы, загруженные на сервер PCN. По этим IOC-файлам производится поиск индикаторов компрометации на хостах с программой Kaspersky Endpoint Agent, подключенных к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN.

При создании IOC-файла ознакомьтесь со списком IOC-терминов, поддерживаемых приложением, которое вы используете в роли компонента Endpoint Agent.

Kaspersky Endpoint Security 11.4 для Linux не поддерживает работу с IOC-файлами.

Пользователи с ролью **Старший сотрудник службы безопасности** могут импортировать (см. раздел "Загрузка IOC-файла" на стр. 516), удалять (см. раздел "Удаление IOC-файла" на стр. 517), скачивать IOC-файлы на компьютер (см. раздел "Скачивание IOC-файла на компьютер" на стр. 516), включать и отключать поиск индикаторов компрометации по IOC-файлам (см. раздел "Включение и отключение автоматического использования IOC-файла при проверке хостов" на стр. 517), а также настраивать расписание поиска индикаторов компрометации на компьютерах с компонентом Endpoint Agent (см. раздел "Настройка расписания IOC-проверки" на стр. 519).

Пользователи с ролью **Сотрудник службы безопасности** и **Аудитор** могут просматривать список IOC-файлов (см. раздел "Просмотр таблицы IOC-файлов" на стр. 514) и информацию о выбранном файле (см. раздел "Просмотр информации об IOC-файле" на стр. 515), а также экспортировать IOC-файлы на компьютер (см. раздел "Скачивание IOC-файла на компьютер" на стр. 516).

kaspersky

В этом разделе

Просмотр таблицы IOC-файлов 514
Просмотр информации об IOC-файле 515
Загрузка IOC-файла 516
Скачивание IOC-файла на компьютер 516
Включение и отключение автоматического использования IOC-файла при проверке хостов 517
Удаление IOC-файла 517
Поиск обнаружений по результатам IOC-проверки 518
Поиск событий по IOC-файлу 518
Фильтрация и поиск IOC-файлов 518
Сброс фильтра IOC-файлов 519
Настройка расписания IOC-проверки 519

Просмотр таблицы IOC-файлов

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Таблица IOC-файлов содержит информацию об IOC-файлах, используемых для проверки на компьютерах с компонентом Endpoint Agent, и находится в разделе **Пользовательские правила**, подразделе **IOC** окна веб-интерфейса приложения.

В таблице IOC-файлов содержится следующая информация:

1. – степень важности, которая будет присвоена обнаружению, произведенному с использованием этого IOC-файла.

   Степень важности может иметь одно из следующих значений:

   - – низкая важность.
   - – средняя важность.
   - – высокая важность.
2. **Тип** – тип IOC-файла в зависимости от режима работы приложения и сервера, на который загружен IOC-файл:

   - **Локальный** – IOC-файлы, загруженные на сервер SCN. По этим IOC-файлам производится поиск индикаторов компрометации на хостах с компонентом Endpoint Agent, подключенных к этому серверу SCN.

- **Глобальный** – IOC-файлы, загруженные на сервер PCN. По этим IOC-файлам производится поиск индикаторов компрометации на хостах с компонентом Endpoint Agent, подключенных к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN.

3. **Имя** – имя IOC-файла.
4. **Серверы** – имя сервера с ролью PCN или SCN, на который распространяется правило.

   Столбец отображается, если вы используете режим распределенного решения и мультитенантности.
5. **Автоматическая проверка** – использование IOC-файла при автоматической проверке хостов с компонентом Endpoint Agent.

   Проверка хостов с использованием этого IOC-файла может находиться в одном из следующих состояний:

   - **Включено**.
   - **Выключено**.

Просмотр информации об IOC-файле

► *Чтобы просмотреть информацию об IOC-файле:*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **IOC**.

   Откроется таблица IOC-файлов.
2. Выберите IOC-файл, информацию о котором вы хотите просмотреть.

Откроется окно с информацией об IOC-файле.

Окно содержит следующую информацию:

- **Найти обнаружения** – по ссылке открывается раздел **Обнаружения** с условием фильтрации, содержащим имя выбранного вами IOC-файла.
- **Найти события** – по ссылке открывается раздел **Поиск угроз** с условием поиска, содержащим индикаторы компрометации выбранного вами IOC-файла.
- **Скачать** – по ссылке открывается окно скачивания IOC-файла.
- **Автоматическая проверка** – использование IOC-файла при автоматической проверке хостов с компонентом Endpoint Agent.
- **Имя** – имя IOC-файла.
- **Важность** – степень важности, которая будет присвоена обнаружению, произведенному с использованием этого IOC-файла.

  Степень важности может иметь одно из следующих значений:

  - – низкая важность.
  - – средняя важность.
  - – высокая важность.

- **Область применения** – отображает название тенанта и имена серверов, к которым относятся события, проверяемые по этому IOC-файлу (в режиме распределенного решения и мультитенантности).
- **XML** – отображает содержимое IOC-файла в формате XML.

Загрузка IOC-файла

IOC-файлы со свойствами UserItem для доменных пользователей не поддерживаются.

► *Чтобы загрузить IOC-файл:*

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.

   Откроется таблица IOC-файлов.
2. Нажмите на кнопку **Загрузить**.

   Откроется окно выбора файла на вашем локальном компьютере.
3. Выберите файл, который вы хотите загрузить и нажмите на кнопку **Открыть**.
4. Укажите следующие параметры:
   a. **Автоматическая проверка** – использование IOC-файла при автоматической проверке хостов с компонентом Endpoint Agent:
      - **Включено**.
      - **Выключено**.
   b. **Имя** – имя IOC-файла.
   c. **Важность** – степень важности, которая будет присвоена обнаружению, произведенному с использованием этого IOC-файла:
      - **Низкая**.
      - **Средняя**.
      - **Высокая**.
   d. **Область применения** – название тенанта и имена серверов, которые вы хотите проверять с помощью этого IOC-файла (в режиме распределенного решения и мультитенантности).
5. Нажмите на кнопку **Сохранить**.

IOC-файл будет загружен в формате XML.

Скачивание IOC-файла на компьютер

Вы можете скачать ранее загруженный IOC-файл на компьютер.

► *Чтобы скачать IOC-файл на компьютер:*

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.

   Откроется таблица IOC-файлов.

2. Выберите IOC-файл, который вы хотите скачать.

   Откроется окно с информацией об IOC-файле.

3. В зависимости от параметров вашего браузера, по ссылке **Скачать** сохраните файл в папку по умолчанию или укажите папку для сохранения файла.

IOC-файл будет сохранен на компьютер в папку загрузки браузера.

Включение и отключение автоматического использования IOC-файла при проверке хостов

Вы можете включить или отключить автоматическое использование IOC-файла для поиска индикаторов компрометации на хостах с компонентом Endpoint Agent.

► *Чтобы включить или отключить автоматическое использование IOC-файла для поиска индикаторов компрометации на хостах с компонентом Endpoint Agent:*

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.

   Откроется таблица IOC-файлов.

2. В строке с IOC-файлом, использование которого вы хотите включить или отключить, в столбце **Состояние** переведите переключатель в одно из следующих положений:

   - **Включено**.
   - **Выключено**.

Автоматическое использование IOC-файла для поиска индикаторов компрометации на хостах с компонентом Endpoint Agent будет включено или отключено.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция включения или отключения автоматического использования IOC-файла недоступна.

Удаление IOC-файла

► *Чтобы удалить IOC-файл:*

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.

   Откроется таблица IOC-файлов.

2. Выберите IOC-файл, который вы хотите удалить.

   Откроется окно с информацией об IOC-файле.

3. Нажмите на кнопку **Удалить**.

IOC-файл будет удален.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция удаления IOC-файла недоступна.

Поиск обнаружений по результатам IOC-проверки

► *Чтобы найти и просмотреть результаты проверки по выбранному IOC-файлу:*

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.

   Откроется таблица IOC-файлов.
2. Выберите IOC-файл, для которого вы хотите просмотреть результаты проверки.

   Откроется окно с информацией об IOC-файле.
3. Перейдите в базу обнаружений по ссылке **Найти обнаружения**.

   Откроется новая вкладка браузера с таблицей найденных обнаружений.

Вы также можете просмотреть результаты проверки по всем IOC-файлам, отфильтровав обнаружения по названию технологии (см. раздел "Фильтрация и поиск обнаружений по названию технологии" на стр. 340).

Поиск событий по IOC-файлу

► *Чтобы просмотреть события, найденные с помощью IOC-файла:*

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.

   Откроется таблица IOC-файлов.
2. Выберите IOC-файл, который вы хотите использовать для поиска событий по базе событий.

   Откроется окно с информацией об IOC-файле.
3. Перейдите в базу событий по ссылке **Найти события**.

   Откроется новая вкладка браузера с таблицей найденных событий.

Фильтрация и поиск IOC-файлов

► *Чтобы отфильтровать или найти IOC-файлы по требуемым критериям:*

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.
2. Откроется таблица IOC-файлов. Выполните следующие действия в зависимости от критерия фильтрации:
   - **По степени важности**

a. По значку откройте окно настройки фильтрации IOC-файлов.

b. Выберите одну или несколько из следующих степеней важности:
   - **Низкая**.
   - **Средняя**.
   - **Высокая**.

c. Нажмите на кнопку **Применить**.

- **По имени файла**

d. По ссылке **Имя** откройте окно настройки фильтрации IOC-файлов.

e. Введите один или несколько символов имени IOC-файла.

f. Нажмите на кнопку **Применить**.

- **По состоянию автоматической проверки (включена / выключена)**

g. По ссылке **Автоматическая проверка** откройте окно настройки фильтрации IOC-файлов.

h. Выберите один из следующих вариантов:

- **Включено**.
- **Выключено**.

В таблице IOC-файлов отобразятся только IOC-файлы, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра IOC-файлов

► *Чтобы сбросить фильтр IOC-файлов по одному или нескольким условиям фильтрации:*

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.
2. Откроется таблица IOC-файлов.Нажмите на кнопку ☒ справа от того заголовка столбца таблицы IOC-файлов, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице IOC-файлов отобразятся только IOC-файлы, соответствующие заданным вами условиям.

Настройка расписания IOC-проверки

Вы можете настроить расписание поиска индикаторов компрометации с помощью IOC-файлов на хостах с компонентом Endpoint Agent.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** недоступна функция настройки расписания поиска индикаторов компрометации с помощью IOC-файлов.

► *Чтобы настроить расписание поиска индикаторов компрометации с помощью IOC-файлов на хостах с компонентом Endpoint Agent:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Endpoint Agents**, блок параметров **Расписание IOC-проверки**.
2. В раскрывающихся списках **Время запуска** выберите время начала поиска индикаторов компрометации.
3. В раскрывающемся списке **Максимальное время проверки** выберите ограничение по времени выполнения поиска индикаторов компрометации.
4. Нажмите на кнопку **Применить**.

Новое расписание поиска индикаторов компрометации с помощью IOC-файлов на хостах с компонентом Endpoint Agent начнет действовать сразу после сохранения изменений. Результаты поиска индикаторов компрометации отобразятся в таблице обнаружений.

Управление поиском индикаторов компрометации с помощью IOC-файлов ограничено возможностями, доступными в веб-интерфейсе Kaspersky Anti Targeted Attack Platform. Других способов управления поиском индикаторов компрометации не предусмотрено.

Если в роли компонента Endpoint Agent вы используете приложение Kaspersky Endpoint Security для Windows, убедитесь, что IOC-файлы соответствуют требованиям. Также вам нужно учитывать, что при добавлении типа данных RegistryItem в область поиска IOC приложение анализирует только некоторые разделы реестра.

Подробнее о требованиях к IOC-файлам и проверяемых разделах реестра см. в справке Kaspersky Endpoint Security для Windows:

- Область поиска IOC в реестре (RegistryItem).
- Требования к IOC-файлам.

Работа с пользовательскими правилами IDS

В режиме распределенного решения и мультитенантности пользовательские правила IDS могут быть одного из следующих типов:

- **Глобальный** – созданные на сервере PCN. По этим правилам производится проверка событий на этом сервере PCN и на всех серверах SCN, подключенных к этому серверу PCN. Проверяемые события относятся к тенантам, в рамках которых пользователь работает в веб-интерфейсе программы.
- **Локальный** – созданные на сервере SCN. По этим правилам производится проверка событий на этом сервере SCN. Проверяемые события относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

Пользователи с ролью **Старший сотрудник службы безопасности** могут импортировать (см. раздел "Импорт пользовательского правила IDS" на стр. 521), заменять (см. раздел "Замена пользовательского правила IDS" на стр. 523) и удалять (см. раздел "Удаление пользовательского правила IDS" на стр. 524) пользовательские правила IDS, а также добавлять правила IDS "Лаборатории Касперского" в исключения из проверки (см. раздел "Добавление правила IDS в исключения" на стр. 574). Пользователи с ролями **Старший сотрудник службы безопасности** и **Аудитор** могут использовать правила IDS для поиска признаков целевых атак, зараженных и возможно зараженных объектов в базе обнаружений, а также просматривать информацию о правиле IDS (см. раздел "Просмотр информации о пользовательском правиле IDS" на стр. 522).

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к к пользовательским правилам IDS.

В этом разделе

Импорт пользовательского правила IDS 521

Просмотр информации о пользовательском правиле IDS 522

Включение и отключение использования правила IDS при проверке событий 522

Настройка важности обнаружений, выполненных по пользовательскому правилу IDS 522

Замена пользовательского правила IDS 523

Экспорт файла пользовательского правила IDS на компьютер 523

Удаление пользовательского правила IDS 524

Импорт пользовательского правила IDS

Вы можете импортировать файл формата Snort® или Suricata и использовать его для проверки событий и создания обнаружений Intrision Detection System.

Настоятельно рекомендуется проверить работу пользовательских правил в тестовой среде перед импортом. Пользовательские правила IDS могут вызвать проблемы производительности, в случае которых стабильная работа Kaspersky Anti Targeted Attack Platform не гарантируется

Например, загрузка пользовательских правил может привести к следующим ошибкам:

- приложение может создавать слишком много IDS-обнаружений;
- если приложение не будет успевать записывать IDS-обнаружения, некоторые объекты сетевого трафика могут остаться непроверенными;
- регулярные выражения в составе пользовательских правил могут привести к ухудшению производительности или сбоям в работе приложения;
- даже формально корректные пользовательские правила могут привести к ухудшению производительности или сбоям в работе приложения.

При загрузке идентификаторы и атрибуты пользовательских правил могут быть изменены. Действия правил Reject и Drop будут заменены на Alert, правила с действием Pass будут удалены

► *Чтобы импортировать пользовательское правило IDS:*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **IDS**.

   Откроется окно пользовательского правила IDS.

2. Нажмите на кнопку **Импортировать**.

   Откроется окно выбора файла на вашем локальном компьютере.

3. Выберите файл, который вы хотите загрузить и нажмите на кнопку **Открыть**.

Пользовательское правило IDS будет импортировано в приложение.

Просмотр информации о пользовательском правиле IDS

► *Чтобы просмотреть информацию о пользовательском правиле IDS,*

в окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **IDS**.

В веб-интерфейсе отображается следующая информация о правиле IDS:

- **Состояние** – состояние использования правила при проверке событий.
- **Размер файла** – размер файла правила.
- **Последнее обновление** – время импорта правила.
- **Автор** – имя пользователя, под учетной записью которого было импортировано правило.
- **Важность** – степень важности, которая будет присвоена обнаружению, выполненному по этому правилу IDS.

Включение и отключение использования правила IDS при проверке событий

► *Чтобы включить или отключить использование правила IDS при проверке событий:*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **IDS**.
2. Откроется окно пользовательского правила IDS.
3. Переведите переключатель **Состояние** в одно из следующих положений:
   - **Включено**.
   - **Выключено**.

Использование правила IDS при проверке событий будет включено или отключено.

Для пользователей с ролью **Аудитор** функция включения и отключения правил IDS недоступна.
У пользователей с ролью **Сотрудник службы безопасности** нет доступа к пользовательским правилам IDS.

Настройка важности обнаружений, выполненных по пользовательскому правилу IDS

► *Чтобы настроить степень важности, которая будет присвоена обнаружению, выполненному по правилу IDS:*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **IDS**.
2. Откроется окно пользовательского правила IDS.В раскрывающемся списке **Важность** выберите степень важности, которая будет присвоена обнаружению, выполненному по этому правилу IDS:
   - **Низкая**.

- **Средняя**.
- **Высокая**.

3. При необходимости с помощью переключателя **Состояние** включите использование этого правила IDS.

Важность обнаружений, выполненных по этому правилу IDS, будет настроена.

Для пользователей с ролью **Аудитор** функция настройки правил IDS недоступна.
У пользователей с ролью **Сотрудник службы безопасности** нет доступа к к пользовательским правилам IDS.

Замена пользовательского правила IDS

Вы можете заменить ранее импортированный файл формата Snort или Suricata и использовать его для проверки событий и создания обнаружений Intrusion Detection System.

Настоятельно рекомендуется проверить работу пользовательских правил в тестовой среде перед импортом. Пользовательские правила IDS могут вызвать проблемы производительности, в случае которых стабильная работа Kaspersky Anti Targeted Attack Platform не гарантируется

При загрузке идентификаторы и атрибуты пользовательских правил могут быть изменены. Действия правил Reject и Drop будут заменены на Alert, правила с действием Pass будут удалены

► *Чтобы заменить пользовательское правило IDS:*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **IDS**.
2. Откроется окно пользовательского правила IDS.Под информацией о правиле нажмите на кнопку **Заменить**.

   Откроется окно выбора файла на вашем локальном компьютере.
3. Выберите файл, который вы хотите загрузить и нажмите на кнопку **Открыть**.

Пользовательское правило IDS будет импортировано в приложение и заменит ранее импортированное правило.

Для пользователей с ролью **Аудитор** функция замены пользовательского правила IDS недоступна.
У пользователей с ролью **Сотрудник службы безопасности** нет доступа к к пользовательским правилам IDS.

Экспорт файла пользовательского правила IDS на компьютер

Вы можете экспортировать ранее импортированный файл правила IDS.

► *Чтобы экспортировать файл пользовательского правила IDS:*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **IDS**.

Откроется окно пользовательского правила IDS.

2. Под информацией о правиле нажмите на кнопку **Скачать**.

Файл будет сохранен на ваш локальный компьютер в папку загрузки браузера.

Удаление пользовательского правила IDS

При работе в режиме распределенного решения пользователи с ролью **Старший сотрудник службы безопасности** могут удалять только то пользовательское правило IDS, которое было импортировано на текущий сервер. Это значит, что в веб-интерфейсе PCN доступно удаление только правила, созданного на PCN. В веб-интерфейсе SCN доступно удаление только правила, созданного на SCN.

► *Чтобы удалить пользовательское правило IDS:*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **IDS**.
2. Откроется окно пользовательского правила IDS.Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.
3. Нажмите на кнопку **Да**.

Правило будет удалено.

Вы не можете удалять правила IDS "Лаборатории Касперского". Если вы не хотите использовать при проверке правило IDS "Лаборатории Касперского", вам требуется добавить его в исключения.
Для пользователей с ролью **Аудитор** функция удаления пользовательского правила IDS недоступна.
У пользователей с ролью **Сотрудник службы безопасности** нет доступа к пользовательским правилам IDS.

Работа с пользовательскими правилами YARA

Вы можете использовать правила YARA в качестве баз модуля YARA для проверки файлов и объектов, поступающих на Central Node, и для проверки хостов (см. раздел "Создание задачи проверки хостов с помощью правил YARA" на стр. 470) с компонентом Endpoint Agent.

В режиме распределенного решения и мультитенантности пользовательские правила YARA могут быть одного из следующих типов:

- **Глобальный** – созданные на сервере PCN. По этим правилам производится проверка файлов и объектов, поступивших на сервер PCN и все серверы SCN, подключенные к этому серверу PCN. Проверяемые файлы и объекты относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе приложения.
- **Локальный** – созданные на сервере SCN. По этим правилам производится проверка файлов и объектов, поступивших на сервер SCN. Проверяемые файлы и объекты относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе приложения.

При работе в веб-интерфейсе приложения пользователи с ролью **Старший сотрудник службы безопасности** могут импортировать файл правил YARA в Kaspersky Anti Targeted Attack Platform через веб-интерфейс приложения.

Пользователи с ролями **Аудитор** и **Сотрудник службы безопасности** могут только просматривать правила YARA.

В этом разделе

Просмотр таблицы правил YARA 525

Настройка отображения таблицы правил YARA 526

Импорт правил YARA 526

Просмотр информации о правиле YARA 527

Фильтрация и поиск правил YARA 528

Сброс фильтра правил YARA 529

Включение и отключение использования правил YARA 530

Удаление правил YARA 531

Просмотр таблицы правил YARA

Таблица пользовательских правил YARA содержит информацию о правилах YARA, используемых для проверки событий и создания обнаружений, и отображается в разделе **Пользовательские правила**, подразделе **YARA** окна веб-интерфейса приложения.

В таблице содержится следующая информация:

- **Создано** – время создания правила.
- – важность обнаружения для пользователя Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние это обнаружение может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".

  По умолчанию обнаружениям, выполненным по загруженным правилам YARA, присваивается высокая степень важности.
- **Тип** – тип правила в зависимости от режима работы приложения и роли сервера, на котором оно было создано:
  - **Глобальный** – созданные на сервере PCN. По этим правилам производится проверка файлов и объектов, поступивших на сервер PCN и все серверы SCN, подключенные к этому серверу PCN. Проверяемые файлы и объекты относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе приложения.
  - **Локальный** – созданные на сервере SCN. По этим правилам производится проверка файлов и объектов, поступивших на сервер SCN. Проверяемые файлы и объекты относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе приложения.
- **Имя** – название правила.
- **Файл** – название файла, из которого было импортировано правило.
- **Автор** – имя пользователя, под учетной записью которого было импортировано правило.

- **Серверы** – имя сервера с ролью PCN или SCN, на который распространяется правило.

  Столбец отображается, если вы используете режим распределенного решения и мультитенантности.

- **Проверка трафика** – состояние использования правила при потоковой проверке файлов и объектов, поступающих на Central Node:
  - **Включено** – правило используется.
  - **Выключено** – правило не используется.

Настройка отображения таблицы правил YARA

Вы можете настроить отображение столбцов, а также порядок их следования в таблице.

► *Чтобы настроить отображение таблицы:*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **YARA**.

   Откроется таблица правил YARA.

2. В заголовочной части таблицы нажмите на кнопку ⚙.

   Отобразится окно **Настройка таблицы**.

3. Если вы хотите включить отображение столбца в таблице, установите флажок рядом с названием того параметра, который должен отображаться в таблице.

   Если вы не хотите, чтобы параметр отображался в таблице, снимите флажок.

   > Должен быть установлен хотя бы один флажок.

4. Если вы хотите изменить порядок отображения столбцов в таблице, наведите курсор мыши на строку с нужным параметром, нажмите на кнопку ⠿ и переместите строку с параметром в нужное место.
5. Если вы хотите восстановить параметры отображения таблицы по умолчанию, нажмите на ссылку **По умолчанию**.
6. Нажмите на кнопку **Применить**.

Отображение таблицы будет настроено.

Импорт правил YARA

► *Чтобы импортировать правила YARA:*

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **YARA**.
2. Нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.

3. Выберите файл правил YARA, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

Окно выбора файлов закроется, откроется окно **Импорт правил YARA**.

> Максимальный допустимый размер загружаемого файла – 20 МБ.

В нижней части окна отображается отчет. В отчете содержится следующая информация:

- Количество правил, которые могут быть успешно импортированы.
- Количество правил, которые не будут импортированы (если такие есть).

  Для каждого правила, которое не может быть импортировано, указывается его название.

4. Установите флажок **Проверка трафика**, если вы хотите использовать импортированные правила при потоковой проверке объектов и данных, поступающих на Central Node.
5. При необходимости в поле **Описание** введите любую дополнительную информацию.

> Поле **Важность** недоступно для редактирования. По умолчанию обнаружениям, выполненным по загруженным правилам YARA, будет присвоена высокая степень важности.

6. В блоке параметров **Область применения** установите флажки напротив тех серверов, на которых вы хотите применить правила.

   Поле отображается только когда вы используете режим распределенного решения и мультитенантности.
7. Нажмите на кнопку **Сохранить**.

Импортированные правила отобразятся в таблице YARA-правил.

Просмотр информации о правиле YARA

► *Чтобы просмотреть информацию о правиле YARA:*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **YARA**.

   Откроется таблица правил YARA.
2. Выберите правило, информацию о котором вы хотите просмотреть.

Откроется окно с информацией о правиле.

Окно содержит следующую информацию:

- **Обнаружения** – по ссылке в новой вкладке браузера откроется таблица обнаружений, отфильтрованных по технологии Targeted Attack Analyzer (см. раздел "Фильтрация и поиск обнаружений по названию технологии" на стр. 340) и имени правила TAA (IOA) (см. раздел "Фильтрация и поиск обнаружений по полученной информации" на стр. 338), с которым вы работаете.
- **Запустить YARA-проверку** – по ссылке открывается окно создания задачи (см. раздел "Создание задачи проверки хостов с помощью правил YARA" на стр. 470).
- **Скачать** – по ссылке скачивается файл с правилами YARA.
- **Правило** – имя правила, указанное в файле.

- **Проверка трафика** – использование правила при потоковой проверке файлов и объектов, поступающих на Central Node.
- **Тип** – тип правила в зависимости от роли сервера, на котором оно создано:
  - **Глобальный** – созданные на сервере PCN. По этим правилам производится проверка файлов и объектов, поступивших на сервер PCN и все серверы SCN, подключенные к этому серверу PCN. Проверяемые файлы и объекты относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе приложения.
  - **Локальный** – созданные на сервере SCN. По этим правилам производится проверка файлов и объектов, поступивших на сервер SCN. Проверяемые файлы и объекты относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе приложения.
- **Важность** – степень важности, которая присваивается обнаружению, выполненному по этому правилу.

  По умолчанию обнаружениям, выполненным по загруженным правилам YARA, присваивается высокая степень важности.
- **Описание** – любая дополнительная информация о правиле, которую вы указали.
- **Область применения** – имена серверов с компонентом Central Node, на которых применяется правило.

Фильтрация и поиск правил YARA

► *Чтобы отфильтровать или найти правила YARA по требуемым критериям:*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **YARA**.

   Откроется таблица правил YARA.
2. Выполните следующие действия в зависимости от критерия фильтрации:
   - **По времени создания**

a. По ссылке **Создано** откройте окно настройки фильтрации.

b. Выберите один из следующих вариантов:
   - **За все время**, если вы хотите, чтобы приложение отображало в таблице правила, созданные за все время.
   - **Прошедший час**, если вы хотите, чтобы приложение отображало в таблице правила, созданные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы приложение отображало в таблице правила, созданные за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы приложение отображало в таблице правила, созданные за указанный вами период.

c. Если вы выбрали **Пользовательский диапазон**, выберите даты начала и конца периода и нажмите на кнопку **Применить**.
   - **По имени правила**

d. По ссылке **Правило** откройте меню фильтрации.

e. В раскрывающемся списке выберите один из следующих операторов фильтрации:

- **Содержит**.
- **Не содержит**.

f. В поле ввода введите название правила или несколько символов из названия правила.

g. Нажмите на кнопку **Применить**.

- **По имени файла**

h. По ссылке **Файл** откройте меню фильтрации.

i. В раскрывающемся списке выберите один из следующих операторов фильтрации:

- **Содержит**.
- **Не содержит**.

j. В поле ввода введите название файла или несколько символов из названия файла.

k. Нажмите на кнопку **Применить**.

- **По имени пользователя, загрузившего файл с правилами**

l. По ссылке **Автор** откройте меню фильтрации.

m. В раскрывающемся списке выберите один из следующих операторов фильтрации:

- **Содержит**.
- **Не содержит**.

n. В поле ввода введите имя пользователя или несколько символов из имени пользователя.

o. Нажмите на кнопку **Применить**.

- **По состоянию правила**

p. По ссылке **Проверка трафика** раскройте список настройки фильтрации.

q. Выберите один из следующих вариантов:

- **Все**.
- **Включено**.
- **Выключено**.

В таблице отобразятся только правила, соответствующие заданным условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра правил YARA

► *Чтобы сбросить фильтрацию правил YARA по одному или нескольким условиям:*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **YARA**.

   Откроется таблица правил YARA.

2. Нажмите на кнопку ☒ справа от того заголовка столбца таблицы правил, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу для каждого из условий.

Выбранные фильтры будут сброшены.

В таблице отобразятся только правила, соответствующие заданным условиям.

Включение и отключение использования правил YARA

Пользователи с ролью **Старший сотрудник службы безопасности** могут включить или отключить использование одного или нескольких правил, а также всех правил сразу.

При работе в режиме распределенного решения и мультитенантности вы можете включить или отключить использование правил YARA, которые были созданы на текущем сервере. Это значит, что в веб-интерфейсе PCN доступно включение и отключение использования только правил, созданных на сервере PCN. В веб-интерфейсе SCN доступно включение и отключение использования только правил, созданных на сервере SCN.
Если на серверах PCN и SCN включено использование правил YARA с одинаковыми именами, при проверке файлов и объектов, поступающих на SCN, применяется правило, созданное на PCN.

► *Чтобы включить или отключить использование правила YARA при потоковой проверке файлов и объектов, поступающих на Central Node:*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **YARA**.

   Откроется таблица правил YARA.

2. В строке с нужным правилом в столбце **Проверка трафика** включите или отключите переключатель.

Использование правила при потоковой проверке файлов и объектов, поступающих на Central Node, будет включено или отключено.

► *Чтобы включить или отключить использование всех или нескольких правил YARA при потоковой проверке файлов и объектов, поступающих на Central Node:*

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **YARA**.
2. Установите флажки слева от правил, использование которых вы хотите включить или отключить.

   Вы можете выбрать все правила, установив флажок в строке с заголовками столбцов.

   В нижней части окна отобразится панель управления.

3. Нажмите на кнопку **Включить** или **Отключить**, чтобы включить или отключить использование всех правил.

Использование выбранных правил при потоковой проверке файлов и объектов, поступающих на Central Node, будет включено или отключено.

Удаление правил YARA

► *Чтобы удалить правило YARA:*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **YARA**.

   Откроется таблица правил YARA.

2. Выберите правило, которое вы хотите удалить.

   Откроется окно с информацией об этом правиле.

3. Нажмите на кнопку **Удалить**.
4. В открывшемся окне подтверждения действия нажмите на кнопку **Да**.

Правило будет удалено.

► *Чтобы удалить все или несколько правил YARA:*

1. В окне веб-интерфейса приложения выберите раздел **Пользовательские правила**, подраздел **YARA**.

   Откроется таблица правил YARA.

2. Установите флажки слева от правил, которые вы хотите удалить.

   Вы можете выбрать все правила, установив флажок в строке с заголовками столбцов.

   В нижней части окна отобразится панель управления.

3. Нажмите на кнопку **Удалить**.
4. В открывшемся окне подтверждения действия нажмите на кнопку **Да**.

Выбранные правила будут удалены.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция удаления правила YARA недоступна.

Работа с объектами в Хранилище и на карантине

В Хранилище помещаются файлы, которые нужно отправить на проверку (см. раздел "Отправка объектов из Хранилища на проверку" на стр. 540), а также файлы, полученные в результате выполнения задач (см. раздел "Работа с задачами" на стр. 456) **Получить файл**, **Восстановить файл из карантина**, **Собрать форензику**, **Получить метафайлы NTFS**, **Получить ключ реестра**, **Получить дамп памяти процесса**.

Хранилище расположено на сервере Central Node.

Вы можете управлять объектами в Хранилище: удалять, скачивать, загружать, отправлять на проверку, а также фильтровать списки объектов.

Kaspersky Anti Targeted Attack Platform отображает объекты в Хранилище в виде таблицы объектов.

Если вы используете режим распределенного решения и мультитенантности, Хранилище расположено на серверах PCN и SCN. В веб-интерфейсе сервера PCN отображается информация о Хранилище всех

подключенных SCN в рамках тех тенантов, к данным которых у пользователя есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса приложения" на стр. 200).

Пользователь с ролью **Старший сотрудник службы безопасности** может поместить копии объектов в Хранилище с помощью задач или загрузив объект в Хранилище через веб-интерфейс Kaspersky Anti Targeted Attack Platform (см. раздел "Загрузка объектов в Хранилище" на стр. 539) на том сервере PCN или SCN, с которым он работает в рамках тех тенантов, к данным которых у него есть доступ.

Пользователь с ролью **Сотрудник службы безопасности** может работать только с файлами, полученными в результате выполнения задач, которые он сам создал на том сервере PCN или SCN, с которым он работает в рамках тех тенантов, к данным которых у него есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса приложения" на стр. 200).

Если вы считаете файл опасным, вы можете поместить его на карантин на компьютере с компонентом Endpoint Agent. Метаданные файла, помещенного на карантин, отобразятся в разделе **Хранилище**, подразделе **Карантин** веб-интерфейса Kaspersky Anti Targeted Attack Platform.

Карантин на сервере Kaspersky Anti Targeted Attack Platform – это область Хранилища серверной части решения Kaspersky Anti Targeted Attack Platform, предназначенная для хранения метаданных объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent, в разделе **Хранилище**, подразделе **Карантин** веб-интерфейса Kaspersky Anti Targeted Attack Platform.

Вы можете управлять объектами на карантине: восстанавливать объекты из карантина (см. раздел "Восстановление объекта из карантина" на стр. 547), а также загружать копии объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent, в Хранилище Kaspersky Anti Targeted Attack Platform (см. раздел "Получение копии объекта на карантине на сервер Kaspersky Anti Targeted Attack Platform" на стр. 548).

Kaspersky Anti Targeted Attack Platform отображает информацию об объектах, помещенных на карантин, в виде таблицы.

Максимальный объем Хранилища определяется при настройке параметров масштабирования приложения. Как только объем Хранилища превышает заданное по умолчанию пороговое значение, приложение начинает удалять из Хранилища самые старые копии объектов. Когда объем Хранилища снова становится меньше порогового значения, приложение прекращает удалять копии объектов из Хранилища.

Реальный размер объекта может быть больше видимого размера объекта из-за метаданных, необходимых для восстановления объекта из карантина. При помещении на карантин учитывается реальный размер объекта. Зашифрованные файлы могут передаваться в расшифрованном виде (в зависимости от параметров шифрования), сжатые файлы передаются в исходном виде.

kaspersky

В этом разделе

Просмотр таблицы объектов, помещенных в Хранилище 533
Просмотр информации об объекте, загруженном в Хранилище через веб-интерфейс 535
Просмотр информации об объекте, помещенном в Хранилище по задаче получения файла 536
Просмотр информации об объекте, помещенном в Хранилище по задаче получения данных 538
Скачивание объектов из Хранилища 539
Загрузка объектов в Хранилище 539
Отправка объектов из Хранилища на проверку 540
Удаление объектов из Хранилища 541
Фильтрация объектов в Хранилище по типу объекта 541
Фильтрация объектов в Хранилище по описанию объекта 542
Фильтрация объектов в Хранилище по результатам проверки 543
Фильтрация объектов в Хранилище по имени сервера Central Node, PCN или SCN 543
Фильтрация объектов в Хранилище по источнику объекта 544
Фильтрация объектов по времени помещения в Хранилище 544
Сброс фильтра объектов в Хранилище 545
Просмотр таблицы объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent 545
Просмотр информации об объекте на карантине 546
Восстановление объекта из карантина 547
Получение копии объекта на карантине на сервер Kaspersky Anti Targeted Attack Platform 548
Удаление информации об объекте, помещенном на карантин, из таблицы 549
Фильтрация информации об объектах, помещенных на карантин, по типу объекта 549
Фильтрация информации об объектах, помещенных на карантин, по описанию объекта 550
Фильтрация информации об объектах, помещенных на карантин, по имени хоста 550
Фильтрация информации об объектах, помещенных на карантин, по времени 551
Сброс фильтра информации об объектах на карантине 552

Просмотр таблицы объектов, помещенных в Хранилище

Таблица объектов, помещенных в Хранилище, находится в разделе **Хранилище**, подразделе **Файлы** веб-интерфейса приложения.

В таблице объектов, помещенных в Хранилище, содержится следующая информация:

1. **Тип** – способ, которым объект был помещен в Хранилище.

   Возможны следующие способы:

- – объект помещен в хранилище одним из следующих способов:
  - выполнена задача **Получить файл**;
  - получена копия объекта, помещенного на карантин на хостах с компонентом Endpoint Agent (в разделе **Хранилище**, подразделе **Карантин** в меню, раскрывшемся по ссылке с директорией объекта, выбрано действие **Получить файл из карантина**).
- – объект помещен в хранилище одним из следующих способов:
  - выполнена задача **Собрать форензику**;
  - выполнена задача **Получить дамп памяти процесса**;
  - выполнена задача **Получить ключ реестра**;
  - выполнена задача **Получить метафайлы NTFS**.
- – объект загружен пользователем вручную в разделе **Хранилище**, подразделе **Файлы**.

2. **Объект** – информация об объекте. Например, имя файла или путь к файлу.
3. **Результаты проверки** – результат проверки объекта.

   Результат проверки отображается в виде одного из следующих значений:

   - **Не обнаружено** – в результате проверки приложение не обнаружила признаков целевой атаки, возможно зараженных объектов или подозрительной активности.
   - **Ошибка выполнения** – проверка объекта завершилась с ошибкой.
   - **Выполняется** – проверка объекта еще не завершилась.
   - **Не выполнялась** – объект не был отправлен на проверку.
   - **Обнаружено** – в результате проверки приложение обнаружило признаки целевой атаки, возможно зараженный объект или подозрительную активность.
4. **Серверы** – имя сервера с ролью PCN или SCN. К этому серверу подключен хост, с которого получен объект

   Столбец отображается, если вы используете режим распределенного решения и мультитенантности.
5. **Адрес источника** – IP-адрес или имя хоста, с которого получен объект, или имя учетной записи пользователя, загрузившего объект.
6. **Время** – дата и время помещения объекта в Хранилище.
7. **Действия** – действия, которые можно выполнить с объектом. Доступны следующие действия:
   - – удалить объект из Хранилища.
   - – отправить объект из Хранилища на проверку технологиями Anti-Malware Engine, YARA и Sandbox.
   - – скачать объект из Хранилища на компьютер.

По ссылке с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.

- **Скачать**.
- **Отправить файл на проверку**.
- **Найти события**:
  - **Путь к файлу**.
  - **MD5**.
  - **SHA256**.
- **Найти обнаружения**:
  - **Путь к файлу**.
  - **MD5**.
  - **SHA256**.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Найти события**.
- **Найти обнаружения**.
- **Скопировать значение в буфер**.

Просмотр информации об объекте, загруженном в Хранилище через веб-интерфейс

► *Чтобы просмотреть информацию об объекте, загруженном в Хранилище вручную, выполните следующие действия:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. В таблице выберите объект со значком , информацию о котором вы хотите посмотреть.

   Откроется окно сведений об объекте.

В окне содержится следующая информация:

- **Файл** – имя файла.
- **Размер** – размер файла.
- **MD5** – MD5-хеш файла.
- **SHA256** – SHA256-хеш файла.
- **Время загрузки** – время загрузки для объектов, загруженных пользователем вручную.

- **Имя пользователя** – имя учетной записи пользователя, загрузившего объект в Хранилище вручную.
- **Результаты проверки** – результат проверки объекта приложением.

Кнопка **Найти на TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.

Кнопка **Создать правило запрета** (см. раздел "**Создание правила запрета**" на стр. 491) позволяет запретить запуск файла.

Кнопка **Скачать** (см. раздел "**Скачивание объектов из Хранилища**" на стр. 539) позволяет загрузить файл на жесткий диск вашего компьютера.

По ссылке с именем файла раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- **Скопировать значение в буфер**.

По ссылке с **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на TIP**.
- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке с **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- **Создать правило запрета** (см. раздел "**Создание правила запрета**" на стр. 491).
- **Скопировать значение в буфер**.

Просмотр информации об объекте, помещенном в Хранилище по задаче получения файла

► *Чтобы просмотреть информацию об объекте, помещенном в Хранилище по задаче **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 460) или **Получить файл из карантина** (см. раздел "**Создание задачи восстановления файла из карантина**" на стр. 479):*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. В таблице выберите объект со значком , информацию о котором вы хотите посмотреть.

   Откроется окно сведений об объекте.

В окне содержится следующая информация:

- Блок рекомендаций. Могут отображаться следующие рекомендации:
  - **Задача** (см. раздел "**Работа с задачами**" на стр. 456) – ссылка, по которой открывается раздел **Задачи**, задача, с помощью которой объект был помещен в Хранилище.
  - **Обнаружение** (см. раздел "**Просмотр обнаружений**" на стр. 350) – ссылка, по которой открывается раздел **Обнаружения**, обнаружение, содержащее объект, помещенный в Хранилище.
  - **Объект на карантине** – ссылка, по которой открывается раздел **Хранилище**, подраздел **Карантин**, метаданные объекта на карантине.
- **Объект** – имя файла или путь к файлу.
- **Размер** – размер файла.
- **MD5** – MD5-хеш файла.
- **SHA256** – SHA256-хеш файла.
- **Время** – время помещения объекта в Хранилище.
- **Тенант** – название тенанта, к которому относится сервер Central Node, PCN или SCN.
- **Сервер** – имя сервера Central Node, PCN или SCN. К этому серверу подключен хост, с которого получен объект.
- **Хост** – имя хоста, с которого получен объект.
- **Результаты проверки** – результат проверки объекта приложением.

Нажатием на кнопку **Sandbox-обнаружение** (см. раздел "**Результаты проверки в Sandbox**" на стр. 357) вы можете открыть окно с подробной информацией о результатах исследования поведения файла.

Кнопка **Найти на TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.

Кнопка **Создать правило запрета** (см. раздел "**Создание правила запрета**" на стр. 491) позволяет запретить запуск файла.

Кнопка **Скачать** (см. раздел "**Скачивание объектов из Хранилища**" на стр. 539) позволяет загрузить файл на жесткий диск вашего компьютера.

По ссылке с именем файла раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- **Скопировать значение в буфер**.

По ссылке с **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на TIP**.
- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).

- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке с **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- **Создать правило запрета** (см. раздел "**Создание правила запрета**" на стр. 491).
- **Скопировать значение в буфер**.

Просмотр информации об объекте, помещенном в Хранилище по задаче получения данных

► *Чтобы просмотреть информацию об объекте, помещенном в Хранилище по задачам **Собрать форензику** (см. раздел "**Создание задачи сбора форензики**" на стр. 461), **Получить дамп памяти процесса** (см. раздел "**Создание задачи получения дампа памяти процесса**" на стр. 465), **Получить ключ реестра** (см. раздел "**Создание задачи получения ключа реестра**" на стр. 463), **Получить метафайлы NTFS** (см. раздел "**Создание задачи получения метафайлов NTFS**" на стр. 464):*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. В таблице выберите объект со значком , информацию о котором вы хотите посмотреть.

   Откроется окно сведений об объекте.

В окне содержится следующая информация:

- **Объект** – имя файла или путь к файлу.
- **Размер** – размер файла.
- **MD5** – MD5-хеш файла.
- **SHA256** – SHA256-хеш файла.
- **Время** – время помещения объекта в Хранилище.
- **Хост** – имя хоста, с которого получен объект.

Кнопка **Скачать** (см. раздел "**Скачивание объектов из Хранилища**" на стр. 539) позволяет загрузить файл на жесткий диск вашего компьютера.

По ссылке с именем файла раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).

- **Скопировать значение в буфер**.

По ссылке с **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на TIP**.
- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке с **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- **Создать правило запрета** (см. раздел "**Создание правила запрета**" на стр. 491).
- **Скопировать значение в буфер**.

Скачивание объектов из Хранилища

Если вы считаете объект в Хранилище безопасным, вы можете скачать его на локальный компьютер.

Скачивание зараженных объектов может угрожать безопасности вашего локального компьютера.

► *Чтобы скачать объект из Хранилища:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. В правой части строки с именем объекта, который вы хотите скачать, нажмите на кнопку .

Объект будет сохранен на ваш локальный компьютер в папку загрузки браузера. Файл загружается в формате ZIP-архива, защищенного паролем infected.

Загрузка объектов в Хранилище

Если вам требуется запустить проверку определенного объекта, вы можете загрузить этот объект в Хранилище и отправить его на проверку (см. раздел "Отправка объектов из Хранилища на проверку" на стр. 540).

► *Чтобы загрузить объект в Хранилище:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. В правом верхнем углу окна нажмите на кнопу **Загрузить**.

   Откроется окно выбора файла.
3. Выберите объект, который вы хотите загрузить в Хранилище.
4. Если вы хотите загрузить в Хранилище файл с расширением .Lnk, выполните следующие действия:
   a. В поле **File name** введите *.Lnk и нажмите на клавишу **Enter**.
   b. Выберите объект.
5. Нажмите на кнопку **Open**.

Объект будет загружен в Хранилище и отобразится в таблице объектов.

Для пользователей с ролью **Аудитор** функция загрузки объектов в Хранилище недоступна.

Отправка объектов из Хранилища на проверку

Вы можете проверить объекты, помещенные в Хранилище, компонентом Central Node с помощью технологий Anti-Malware Engine и YARA, а также компонентом Sandbox.

Рекомендуется отправлять объекты из Хранилища на проверку в следующих случаях:

- проверка при помещении в Хранилище была отключена;
- базы приложения были обновлены;
- объект был загружен в Хранилище вручную.

► *Чтобы отправить объект из Хранилища на проверку:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.
2. Нажмите на объект, который вы хотите проверить.

   Откроется окно сведений об объекте.
3. Нажмите на кнопку **Проверить**.

   Запустится проверка объекта.

   После завершения проверки объекта его статус отобразится в таблице объектов.

Вы также можете отправить объект из Хранилища на проверку нажатием на кнопку в правой части строки с информацией об объекте в таблице объектов, помещенных в Хранилище.

Для пользователей с ролью **Аудитор** функция проверки объектов, помещенных в хранилище, недоступна.

Удаление объектов из Хранилища

► *Чтобы удалить объект из Хранилища:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.
2. Нажмите на объект, который вы хотите удалить.

   Откроется окно сведений об объекте.
3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.
4. Нажмите на кнопку **Да**.

Объект будет удален из Хранилища.

Вы также можете удалить объект из Хранилища нажатием на кнопку в правой части строки с информацией об объекте в таблице объектов, помещенных в Хранилище.

► *Чтобы удалить все или несколько объектов из Хранилища:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.
2. Установите флажки напротив объектов, которые вы хотите удалить из Хранилища.

   Вы можете выбрать все объекты, установив флажок в строке с заголовками столбцов.
3. В панели управления в нижней части окна нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.
4. Нажмите на кнопку **Да**.

Выбранные объекты будут удалены из Хранилища.

Для пользователей с ролью **Аудитор** функция удаления объектов, помещенных в хранилище, недоступна.

Фильтрация объектов в Хранилище по типу объекта

► *Чтобы отфильтровать объекты в Хранилище по их типу:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.
2. По ссылке **Тип** откройте меню фильтрации объектов.
3. Установите один или несколько флажков:

- **Загружен по задаче Получить файл**, если вы хотите, чтобы приложение отображало в таблице объекты, помещенные в Хранилище по задачам **Получить файл** и **Восстановить файл из карантина**.
- **Загружен через веб-интерфейс**, если вы хотите, чтобы приложение отображало в таблице объекты, загруженные пользователем через веб-интерфейс Kaspersky Anti Targeted Attack Platform.
- **Загружен по задаче получения данных**, если вы хотите, чтобы приложение отображало в таблице объекты, помещенные в Хранилище по задачам **Собрать форензику**, **Получить метафайлы NTFS**, **Получить ключ реестра**, **Получить дамп памяти процесса**.

4. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация объектов в Хранилище по описанию объекта

► *Чтобы отфильтровать объекты в Хранилище по описанию объекта:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.
2. По ссылке **Объект** откройте меню фильтрации объектов.
3. В раскрывающемся списке выберите один из следующих вариантов:
   - **Путь к файлу**.
   - **MD5**.
   - **SHA256**.
4. В раскрывающемся списке выберите один из следующих операторов фильтрации объектов:
   - **Содержит**.
   - **Не содержит**.
   - **Равняется**.
   - **Не равняется**.
   - **Соответствует шаблону**.
   - **Не соответствует шаблону**.
5. В поле ввода укажите один или несколько символов описания объекта.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
7. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация объектов в Хранилище по результатам проверки

► *Чтобы отфильтровать объекты в Хранилище по результатам проверки этих объектов:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.
2. По ссылке **Результаты проверки** откройте меню фильтрации объектов.
3. Установите один или несколько флажков:
   - **Не обнаружено**.
   - **Ошибка выполнения**.
   - **Выполняется**.
   - **Не выполнялась**.
   - **Обнаружено**.
4. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация объектов в Хранилище по имени сервера Central Node, PCN или SCN

► *Чтобы отфильтровать объекты в Хранилище по имени сервера Central Node, PCN или SCN:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.
2. По ссылке **Серверы** откройте меню фильтрации объектов.
3. Установите один или несколько флажков напротив тех серверов, по которым вы хотите отфильтровать объекты в Хранилище.
4. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация объектов в Хранилище по источнику объекта

► *Чтобы отфильтровать объекты в Хранилище по источнику, с которого они были получены:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.
2. По ссылке **Адрес источника** откройте меню фильтрации объектов.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации объектов:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов IP-адреса, имени хоста или имени учетной записи пользователя, загрузившего объект вручную.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация объектов по времени помещения в Хранилище

► *Чтобы отфильтровать объекты по времени помещения в Хранилище:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.
2. По ссылке **Время** откройте меню фильтрации объектов.
3. Выберите один из следующих периодов отображения объектов:
   - **Все**, если вы хотите, чтобы приложение отображало в таблице все помещенные в Хранилище объекты.
   - **Прошедший час**, если вы хотите, чтобы приложение отображало в таблице объекты, помещенные в Хранилище за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы приложение отображало в таблице объекты, помещенные в Хранилище за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы приложение отображало в таблице объекты, помещенные в Хранилище за указанный вами период.

4. Если вы выбрали период отображения объектов **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения объектов.
   b. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра объектов в Хранилище

► *Чтобы сбросить фильтр объектов в Хранилище по одному или нескольким условиям фильтрации:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.
2. Нажмите на кнопку ☒ справа от того заголовка столбца таблицы объектов в Хранилище, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Просмотр таблицы объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent

Таблица объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent, находится в разделе **Хранилище**, подразделе **Карантин** веб-интерфейса приложения.

На сервере Kaspersky Anti Targeted Attack Platform хранятся метаданные объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent. Сами объекты хранятся в специальном хранилище на каждом компьютере, на котором был обнаружен опасный объект.

В таблице объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent, содержится следующая информация:

1. **Объект** – информация об объекте. Например, имя файла или путь к файлу.
2. **Адрес источника** – IP-адрес или имя хоста компьютера с компонентом Endpoint Agent, на карантине которого находится объект.
3. **Время** – дата и время помещения объекта на карантин.
4. **Состояние** – состояние объекта.

В правой части строки с информацией об объекте расположены кнопки:

- Кнопка позволяет удалить метаданные объекта на сервере Kaspersky Anti Targeted Attack Platform.
- Кнопка позволяет восстановить объект из карантина на компьютере с компонентом Endpoint Agent.
- Кнопка позволяет получить копию объекта из карантина на компьютере с компонентом Endpoint Agent на сервер Kaspersky Anti Targeted Attack Platform.

По ссылке с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скачать**.
- **Отправить файл на проверку**.
- **Найти события**:
  - **Путь к файлу**.
  - **MD5**.
  - **SHA256**.
- **Найти обнаружения**:
  - **Путь к файлу**.
  - **MD5**.
  - **SHA256**.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Найти события**.
- **Найти обнаружения**.
- **Скопировать значение в буфер**.

Просмотр информации об объекте на карантине

► *Чтобы просмотреть информацию об объекте, помещенном на карантин на компьютере с компонентом Endpoint Agent:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Карантин**.

   Откроется таблица объектов.

2. В таблице выберите объект, информацию о котором вы хотите посмотреть.

   Откроется окно сведений об объекте.

В окне содержится следующая информация:

- Блок рекомендаций. Может отображаться рекомендация **Задача** (см. раздел "**Работа с задачами**" на стр. 456) – ссылка, по которой открывается раздел **Задачи**, задача, с помощью которой объект был помещен на карантин.
- **Тип** – тип объекта, помещенного на карантин.

  Возможны следующие типы объектов:

  - – файл.
  - – дамп памяти процесса.
- **Объект** – имя файла или путь к файлу.
- **Состояние** – состояние файла (можно ли восстановить файл из карантина).
- **Адрес источника** – имя компьютера с компонентом Endpoint Agent, на карантине которого находится объект.
- **Время** – время помещения объекта на карантин.
- **Действия** – состояние файла (можно ли восстановить файл из карантина).

  Доступны следующие действия:

  - – удалить файл из карантина.
  - – получить копию файла на сервер Kaspersky Anti Targeted Attack Platform.

По ссылке с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 366).
- **Найти обнаружения** (см. раздел "**Просмотр таблицы обнаружений**" на стр. 331).
- **Скопировать значение в буфер**.

Восстановление объекта из карантина

► *Чтобы восстановить объект из карантина на компьютере с компонентом Endpoint Agent:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Карантин**.

   Откроется таблица объектов.
2. В таблице выберите объект, который вы хотите восстановить из карантина на компьютере с компонентом Endpoint Agent.

   Откроется окно сведений об объекте.
3. Нажмите на кнопку **Восстановить** в нижней части окна.

   Откроется раздел **Задачи**, задача **Восстановить файл из карантина**.
4. В поле **Описание** введите описание задачи.

5. Нажмите на кнопку **Добавить**.

Файл будет восстановлен из карантина.

Вы также можете запустить задачу восстановления файла из карантина нажатием на кнопку в правой части строки с информацией об объекте таблицы объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent (см. раздел "Просмотр таблицы объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent" на стр. 545).

В режиме распределенного решения и мультитенантности файл, помещенный на карантин (см. раздел "Создание задачи помещения файла на карантин" на стр. 478) сервера SCN, нельзя восстановить на сервере PCN. Вы можете восстановить файл на том сервере SCN, где была создана задача для помещения файла на карантин.
Для пользователей с ролью **Аудитор** функция восстановления объекта из карантина недоступна.

Получение копии объекта на карантине на сервер Kaspersky Anti Targeted Attack Platform

Размер объекта, копию которого требуется получить, не должен превышать 100 МБ. Если размер объекта превышает 100 МБ, задача завершается ошибкой.

► *Чтобы получить копию объекта, помещенного на карантин на компьютере с компонентом Endpoint Agent, на сервер Kaspersky Anti Targeted Attack Platform:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Карантин**.

   Откроется таблица объектов.

2. В таблице выберите объект, который вы хотите восстановить из карантина на компьютере с компонентом Endpoint Agent.

   Откроется окно сведений об объекте.

3. Нажмите на кнопку **Получить файл** в нижней части окна.

Будет создана задача получения копии объекта, помещенного на карантин на компьютере с компонентом Endpoint Agent. При успешном завершении задачи копия объекта загрузится на сервер Kaspersky Anti Targeted Attack Platform. Объект отобразится в разделе **Хранилище**, подразделе **Файлы** веб-интерфейса приложения в таблице объектов, помещенных в Хранилище (см. раздел "Просмотр таблицы объектов, помещенных в Хранилище" на стр. 533).

Информация о задаче отобразится в разделе **Задачи** веб-интерфейса (см. раздел "Работа с задачами" на стр. 456).

Вы также можете получить копию объекта из карантина на компьютере с компонентом Endpoint Agent на сервер Kaspersky Anti Targeted Attack Platform нажатием на кнопку в правой части строки с информацией об объекте таблицы объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent (см. раздел "Просмотр таблицы объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent" на стр. 545).

Для пользователей с ролью **Аудитор** получение копии объекта из карантина недоступно.

Удаление информации об объекте, помещенном на карантин, из таблицы

► *Чтобы удалить информацию об объекте, помещенном на карантин на компьютере с компонентом Endpoint Agent, из таблицы Kaspersky Anti Targeted Attack Platform:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Карантин**.

   Откроется таблица объектов.

2. Нажмите на объект, информацию о котором вы хотите удалить из таблицы.

   Откроется окно сведений об объекте.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Информация об объекте, помещенном на карантин на компьютере с компонентом Endpoint Agent, будет удалена из таблицы.

Вы также можете удалить информацию об объекте, помещенном на карантин на компьютере с компонентом Endpoint Agent, из таблицы нажатием на кнопку в правой части строки с информацией об объекте в таблице объектов, помещенных на карантин (см. раздел "Просмотр таблицы объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent" на стр. 545).

Для пользователей с ролью **Аудитор** удаление информации об объекте, помещенном на карантин, из таблицы недоступно.

Фильтрация информации об объектах, помещенных на карантин, по типу объекта

► *Чтобы отфильтровать информацию об объектах, помещенных на карантин, по их типу:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Карантин**.

   Откроется таблица объектов.

2. По ссылке **Тип** откройте меню фильтрации объектов.
3. Установите один или несколько флажков:
   - **Файл**, если вы хотите, чтобы приложение отображало в таблице метаданные объектов, помещенных на карантин.
   - **Дамп памяти процесса**, если вы хотите, чтобы приложение отображало в таблице метаданные дампов, помещенных на карантин.

4. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация информации об объектах, помещенных на карантин, по описанию объекта

► *Чтобы отфильтровать информацию об объектах, помещенных на карантин, по описанию объекта:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Карантин**.

   Откроется таблица объектов.
2. По ссылке **Объект** откройте меню фильтрации объектов.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации объектов:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов описания объекта.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация информации об объектах, помещенных на карантин, по имени хоста

► *Чтобы отфильтровать информацию об объектах, помещенных на карантин, по имени хоста, на котором они были помещены на карантин:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Карантин**.

   Откроется таблица объектов.
2. По ссылке **Адрес источника** откройте меню фильтрации объектов.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации объектов:
   - **Содержит**.

- **Не содержит**.

4. В поле ввода укажите один или несколько символов имени хоста.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация информации об объектах, помещенных на карантин, по времени

► *Чтобы отфильтровать информацию об объектах, помещенных на карантин, по времени помещения на карантин:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Карантин**.

   Откроется таблица объектов.
2. По ссылке **Время** откройте меню фильтрации объектов.
3. Выберите один из следующих периодов отображения объектов:
   - **Все**, если вы хотите, чтобы приложение отображало в таблице все объекты.
   - **Прошедший час**, если вы хотите, чтобы приложение отображало в таблице объекты, помещенные на карантин за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы приложение отображало в таблице объекты, помещенные на карантин за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы приложение отображало в таблице объекты, помещенные на карантин за указанный вами период.
4. Если вы выбрали период отображения объектов **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения объектов.
   b. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра информации об объектах на карантине

► *Чтобы сбросить фильтр по одному или нескольким условиям фильтрации:*

1. В окне веб-интерфейса приложения выберите раздел **Хранилище**, подраздел **Карантин**.

   Откроется таблица объектов.

2. Нажмите на кнопку ☒ справа от того заголовка столбца таблицы объектов на карантине, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Работа с отчетами

При работе в веб-интерфейсе приложения пользователи с ролью **Старший сотрудник службы безопасности** могут управлять отчетами об обнаружениях приложения: создавать шаблоны отчетов (см. раздел "Создание шаблона" на стр. 554), создавать отчеты по шаблону (см. раздел "Создание отчета по шаблону" на стр. 556), просматривать (см. раздел "Просмотр отчета" на стр. 556) и удалять отчеты (см. раздел "Удаление отчета" на стр. 562) и шаблоны отчетов (см. раздел "Удаление шаблона" на стр. 560).

Пользователи с ролью **Аудитор** могут просматривать отчеты и шаблоны отчетов и создавать отчеты по шаблону.

Отчет формируется на основе выборки обнаружений за указанный период. Если вы используете режим распределенного решения и мультитенантности, выборка данных осуществляется также по тенанту и серверам этого тенанта.

Управление шаблонами отчетов и отчетами доступно во всех режимах работы приложения в соответствии с лицензией.

Выполняйте действия по созданию отчета в следующем порядке:

a. **Создайте шаблон отчета (см. раздел "Создание шаблона" на стр. 554)**

b. **Создайте отчет на основе шаблона (см. раздел "Создание отчета по шаблону" на стр. 556)**

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к отчетам.

kaspersky

В этом разделе

Просмотр таблицы шаблонов и отчетов 553
Создание шаблона 554
Создание отчета по шаблону 556
Просмотр отчета 556
Скачивание отчета на локальный компьютер 557
Изменение шаблона 557
Фильтрация шаблонов по имени 558
Фильтрация шаблонов по имени пользователя, создавшего шаблон 559
Фильтрация шаблонов по времени создания 559
Сброс фильтра шаблонов 560
Удаление шаблона 560
Фильтрация отчетов по времени создания 560
Фильтрация отчетов по имени 561
Фильтрация отчетов по имени сервера с компонентом Central Node 561
Фильтрация отчетов по имени пользователя, создавшего отчет 562
Сброс фильтра отчетов 562
Удаление отчета 562

Просмотр таблицы шаблонов и отчетов

Шаблоны и отчеты отображаются в разделе **Отчеты** окна веб-интерфейса приложения.

В подразделе **Созданные отчеты** отображается таблица отчетов. Таблица содержит следующую информацию:

- **Время создания** – дата и время создания отчета.
- **Имя отчета** – имя отчета, созданного по шаблону.
- **Период** – период, за который создан отчет.
- **Серверы** – имя сервера с ролью PCN или SCN, на который распространяется правило.

  Столбец отображается, если вы используете режим распределенного решения и мультитенантности.
- **Автор** – имя пользователя, создавшего отчет.
- **Состояние** – состояние отчета (можно ли скачать файл).

В подразделе **Шаблоны** отображается таблица шаблонов. Таблица содержит следующую информацию:

- **Время создания** – дата и время создания шаблона.
- **Время обновления** – дата и время последнего изменения шаблона.

- **Имя отчета** – имя шаблона.
- **Автор** – имя пользователя, создавшего шаблон.

Создание шаблона

При создании шаблона отчета вам нужно указать всю информацию, которую вы хотите отображать в отчете: имя отчета, его описание, наличие таблицы, графика или изображения. Также вы можете выбрать данные, которые вы хотите отображать в отчете и задать расположение элементов отчета. Создание отчета (см. раздел "Создание отчета по шаблону" на стр. 556) в разделе **Отчеты**, подразделе **Созданные отчеты** интерфейса позволяет только выбрать шаблон для создания отчета и период отображения данных.
Новый шаблон отчета создается для каждой выборки данных.

► *Чтобы создать шаблон:*

1. В окне веб-интерфейса приложения выберите раздел **Отчеты**, подраздел **Шаблоны**.

   Откроется таблица шаблонов.

2. Нажмите на кнопку **Добавить**.

   Откроется окно создания шаблона. Окно содержит тело отчета и конструктор отчета в плавающем окне. Вы можете перемещать конструктор отчета по рабочей области окна веб-интерфейса.

3. В поле **Имя шаблона** в правом верхнем углу окна введите имя, которое вы хотите присвоить отчетам, создаваемым по этому шаблону. Например, **Обнаружения по технологии**.

   Это имя отобразится в таблице в разделе **Отчеты**, подразделе **Созданные отчеты** при создании всех отчетов на этом шаблоне.

4. Вместо текста **Заголовок отчета** введите имя отчета, которое отобразится в отчете после создания отчета. Если вы не хотите добавлять имя отчета, вы можете удалить текст **Заголовок отчета** и оставить этот раздел отчета пустым.

   Вы можете форматировать текст с помощью кнопок в блоке **Text** в конструкторе шаблона.

5. Вместо текста **Описание отчета** введите описание отчета, которое отобразится в отчете после создания отчета. Если вы не хотите добавлять описание отчета, вы можете удалить текст **Описание отчета** и оставить этот раздел отчета пустым.

   Вы можете форматировать текст с помощью кнопок в блоке **Text** в конструкторе шаблона.

6. Используя конструктор отчета, добавьте один или несколько элементов отчета:
   - **Таблица**.
   - **Диаграмма**.
   - **Изображение**.

7. Если вы выбрали добавление изображения, откроется окно **Изображение**. Выполните следующие действия:
   a. Нажмите на кнопку **Загрузить**.
   b. Загрузите изображение. Например, вы можете загрузить логотип вашей организации.

c. В списке справа от кнопки загрузки выберите выравнивание изображения на странице отчета: **По левому краю**, **По правому краю** или **По центру**.

d. Нажмите на кнопку **Применить**.

8. Если вы выбрали добавление диаграммы, откроется окно **Диаграмма по свойствам обнаружений**. Выполните следующие действия:

   a. В поле **Имя** введите имя диаграммы. Например, **Топ 5 обнаружений по технологии**. Вы также можете оставить поле пустым.

   b. В списке **Источник данных** выберите свойство обнаружения, по которому вы хотите создать диаграмму. Например, **Технологии**.

   c. В поле **Количество секторов** укажите максимальное количество секторов диаграммы. При создании отчета приложение выберет наиболее часто встречающиеся данные. Например, если вы указали 5 секторов и хотите создать диаграмму по технологии, приложение покажет диаграмму по 5 технологиям, выполнившим наибольшее количество обнаружений. Технологии, выполнившие наименьшее количество обнаружений, не отобразятся на диаграмме.

   Нажмите на кнопку **Применить**.

9. Если вы выбрали добавление таблицы, откроется окно **Таблица обнаружений**. Выполните следующие действия:

   a. В поле **Доступные столбцы** двойным щелчком мыши выберите свойства обнаружений, которые вы хотите добавить в таблицу отчета.

   Выбранные свойства переместятся в поле **Выбранные столбцы**. Вы можете перетаскивать имена столбцов между полями **Доступные столбцы** и **Выбранные столбцы**, а также менять порядок столбцов таблицы отчета.

   Например, если в поле **Выбранные столбцы** вы переместили свойства **Технологии, Обнаружено** и **Время создания**, в таблице созданного отчета отобразятся технологии, выполнившие обнаружения, список обнаруженных объектов и время создания обнаружений.

   b. Если вы хотите отфильтровать обнаружения по свойству **Состояние**, установите флажки рядом с теми состояниями обработки обнаружений пользователем, данные по которым вы хотите отображать в отчете.

   c. Если вы хотите отфильтровать обнаружения по свойству **Технологии**, установите флажки рядом с теми названиями модулей и компонентов приложения, данные по которым вы хотите отображать в отчете.

   d. Если вы хотите отфильтровать обнаружения по свойству **Важность**, установите флажки рядом с теми степенями важности обнаружений, данные по которым вы хотите отображать в отчете.

   e. Если вы хотите отфильтровать обнаружения по статусу **Статус VIP**, в списке выберите **VIP**. В отчете отобразятся только обнаружения со статусом VIP.

   f. Нажмите на кнопку **Применить**.

10. Нажмите на кнопку **Сохранить** в правом верхнем углу окна.

Будет создан новый шаблон.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция создания шаблона отчета недоступна.

Создание отчета по шаблону

► *Чтобы создать отчет по шаблону:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.

2. Нажмите на кнопку **Добавить**.

   Откроется окно **Новый отчет**.

3. Выполните следующие действия:

   a. В раскрывающемся списке **Шаблон** выберите один из шаблонов для создания отчета.

   b. В блоке параметров **Период** выберите один из следующих вариантов:

   - **Прошедший час**, если вы хотите, чтобы отчет содержал информацию о работе приложения за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы отчет содержал информацию о работе приложения за предыдущий день.
   - **Прошедшие 7 дней**, если вы хотите, чтобы отчет содержал информацию о работе приложения за предыдущую неделю.
   - **Прошедшие 30 дней**, если вы хотите, чтобы отчет содержал информацию о работе системы за предыдущий месяц.
   - **Пользовательские**, если вы хотите, чтобы отчет содержал информацию о работе системы за указанный вами период.

4. Если вы выбрали период отображения информации о работе приложения **Пользовательские**, выполните следующие действия:

   a. В открывшемся календаре укажите даты начала и конца периода, за который будет создан отчет.

   b. Нажмите на кнопку **Применить**.

5. Если вы используете режим распределенного решения и мультитенантности, в блоке параметров **Серверы** установите флажки напротив тех тенантов и серверов, данные по которым вы хотите отображать в отчете.

6. Нажмите на кнопку **Создать**.

Созданный отчет отобразится в таблице отчетов. Вы можете загрузить отчет для просмотра на вашем компьютере.

Для пользователей с ролью **Сотрудник службы безопасности** функция создания шаблона отчета недоступна.

Просмотр отчета

► *Чтобы просмотреть отчет:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

Откроется таблица отчетов.

2. Выберите отчет, который вы хотите просмотреть.

Отчет откроется в новой вкладке вашего браузера.

Скачивание отчета на локальный компьютер

► *Чтобы скачать отчет на ваш компьютер:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.

2. В строке с отчетом, который вы хотите просмотреть, нажмите на значок .

   Отчет будет сохранен в формате HTML на ваш локальный компьютер в папку загрузки браузера.

   Для просмотра отчета вы можете использовать любое приложение для просмотра HTML-файлов (например, браузер).

Изменение шаблона

► *Чтобы изменить шаблон:*

1. В окне веб-интерфейса приложения выберите раздел **Отчеты**, подраздел **Шаблоны**.
2. Откроется таблица шаблонов. Выберите шаблон, который вы хотите изменить.

   Откроется окно изменения шаблона.

3. Вы можете изменить следующие параметры:
   - **Имя шаблона** – имя отчета, которое отобразится в таблице в разделе **Отчеты**, подразделе **Созданные отчеты** при создании всех отчетов по этому шаблону.
   - **Заголовок отчета** – имя отчета, которое отобразится в отчете после создания отчета.

     Вы можете форматировать текст с помощью кнопок в блоке **Text** в конструкторе шаблона.
   - **Описание отчета** – описание отчета, которое отобразится в отчете после создания отчета.

     Вы можете форматировать текст с помощью кнопок в блоке **Text** в конструкторе шаблона.
   - **Изображение**. Вы можете загрузить или удалить изображение.
   - **Диаграмма**. Вы можете изменить следующие параметры диаграммы:
     - **Имя**.
     - **Источник данных**.
     - **Количество секторов**.

     Нажмите на кнопку **Применить**.
   - **Таблица**. Вы можете изменить следующие параметры таблицы:
     - **Выбранные столбцы**. Вы можете перетаскивать имена столбцов между полями **Доступные столбцы** и **Выбранные столбцы**, а также менять порядок столбцов таблицы отчета.

- **Состояние**.
- **Технологии**.
- **Важность**.
- **Статус VIP**.

4. Выберите один из следующих способов сохранения шаблона:
   - Если вы хотите применить изменения к текущему шаблону, нажмите на кнопку **Сохранить**.

     Шаблон будет изменен.
   - Если вы хотите создать новый шаблон, введите имя шаблона и нажмите на кнопку **Сохранить как**.

     Имя нового шаблона не должно совпадать с именем уже существующего шаблона.

     Новый шаблон будет сохранен.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция изменения шаблона недоступна.

Фильтрация шаблонов по имени

► *Чтобы отфильтровать шаблоны по имени:*

1. В окне веб-интерфейса приложения выберите раздел **Отчеты**, подраздел **Шаблоны**.
2. Откроется таблица шаблонов. По ссылке **Имя отчета** откройте меню фильтрации шаблонов.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации шаблонов:
   - **Содержит**.
   - **Не содержит**.
4. Введите один или несколько символов имени шаблона.
5. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку + под списком операторов фильтрации и повторите действия по вводу условий фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице шаблонов отобразятся только шаблоны, соответствующие заданным вами условиям.

Фильтрация шаблонов по имени пользователя, создавшего шаблон

► *Чтобы отфильтровать шаблоны по имени пользователя, создавшего шаблон:*

1. В окне веб-интерфейса приложения выберите раздел **Отчеты**, подраздел **Шаблоны**.
2. Откроется таблица шаблонов. По ссылке **Автор** откройте меню фильтрации шаблонов.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации шаблонов:
   - **Содержит**.
   - **Не содержит**.
4. Введите один или несколько символов имени пользователя.
5. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку + под списком операторов фильтрации и повторите действия по вводу условий фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице шаблонов отобразятся только шаблоны, соответствующие заданным вами условиям.

Фильтрация шаблонов по времени создания

► *Чтобы отфильтровать шаблоны отчетов по времени создания:*

1. В окне веб-интерфейса приложения выберите раздел **Отчеты**, подраздел **Шаблоны**.
2. Откроется таблица шаблонов. По ссылке **Время создания** откройте меню фильтрации шаблонов.
3. Выберите один из следующих периодов отображения шаблонов:
   - **Все**, если вы хотите, чтобы приложение отображало в таблице все созданные шаблоны.
   - **Прошедший час**, если вы хотите, чтобы приложение отображало в таблице шаблоны, созданные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы приложение отображало в таблице шаблоны, созданные за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы приложение отображало в таблице шаблоны, созданные за указанный вами период.
4. Если вы выбрали период отображения шаблонов **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения шаблонов.
   b. Нажмите на кнопку **Применить**.

В таблице шаблонов отобразятся только шаблоны, соответствующие заданным вами условиям.

Сброс фильтра шаблонов

► *Чтобы сбросить фильтр шаблонов по одному или нескольким условиям фильтрации:*

1. В окне веб-интерфейса приложения выберите раздел **Отчеты**, подраздел **Шаблоны**.
2. Откроется таблица шаблонов. Нажмите на кнопку ✕ справа от того заголовка столбца таблицы шаблонов, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице шаблонов отобразятся только шаблоны, соответствующие заданным вами условиям.

Удаление шаблона

► *Чтобы удалить шаблон:*

1. В окне веб-интерфейса приложения выберите раздел **Отчеты**, подраздел **Шаблоны**.
2. Откроется таблица шаблонов. Установите флажок в строке с шаблоном, который вы хотите удалить.
3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.
4. Нажмите на кнопку **Да**.

Выбранный вами шаблон будет удален.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция удаления шаблона недоступна.

Фильтрация отчетов по времени создания

► *Чтобы отфильтровать отчеты по времени их создания:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.
2. По ссылке **Время создания** откройте меню фильтрации отчетов.
3. Выберите один из следующих периодов отображения отчетов:
   - **Все**, если вы хотите, чтобы приложение отображало в таблице все созданные отчеты.
   - **Прошедший час**, если вы хотите, чтобы приложение отображало в таблице отчеты, созданные за предыдущий час.

- **Прошедшие сутки**, если вы хотите, чтобы приложение отображало в таблице отчеты, созданные за предыдущий день.
- **Пользовательский диапазон**, если вы хотите, чтобы приложение отображало в таблице отчеты, созданные за указанный вами период.

4. Если вы выбрали период отображения отчетов **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения отчетов.
   b. Нажмите на кнопку **Применить**.

В таблице отчетов отобразятся только отчеты, соответствующие заданным вами условиям.

Фильтрация отчетов по имени

► *Чтобы отфильтровать отчеты по имени:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.
2. По ссылке **Имя отчета** откройте меню фильтрации отчетов.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации отчетов:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов имени отчета.
5. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку + под списком операторов фильтрации и повторите действия по вводу условий фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице отчетов отобразятся только отчеты, соответствующие заданным вами условиям.

Фильтрация отчетов по имени сервера с компонентом Central Node

► *Чтобы отфильтровать отчеты по имени сервера с компонентом Central Node:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.
2. По ссылке **Серверы** откройте меню фильтрации отчетов.
3. Установите флажки напротив тех серверов, по которым вы хотите отфильтровать отчеты.
4. Нажмите на кнопку **Применить**.

В таблице отчетов отобразятся только отчеты, соответствующие заданным вами условиям.

Фильтрация отчетов по имени пользователя, создавшего отчет

► *Чтобы отфильтровать отчеты по имени пользователя, создавшего отчет:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.
2. По ссылке **Автор** откройте меню фильтрации отчетов.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации отчетов:
   - **Содержит**.
   - **Не содержит**.
4. Введите один или несколько символов имени пользователя.
5. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку + под списком операторов фильтрации и повторите действия по вводу условий фильтрации.

В таблице отчетов отобразятся только отчеты, соответствующие заданным вами условиям.

Сброс фильтра отчетов

► *Чтобы сбросить фильтр отчетов по одному или нескольким условиям фильтрации:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.
2. Нажмите на кнопку ✕ справа от того заголовка столбца таблицы отчетов, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице отчетов отобразятся только отчеты, соответствующие заданным вами условиям.

Удаление отчета

► *Чтобы удалить отчет о работе приложения:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.
2. Установите флажок в строке с отчетом, который вы хотите удалить.
3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.
4. Нажмите на кнопку **Да**.

Выбранный отчет будет удален.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция удаления отчета недоступна.

Работа с правилами присвоения обнаружениям статуса VIP

Пользователи с ролью **Старший сотрудник службы безопасности** могут создавать, удалять, изменять, импортировать и экспортировать список правил присвоения обнаружениям статуса VIP.

Вы можете создавать правила одного из следующих типов:

- **IP**. Новым обнаружениям, связанным с этим IP-адресом компьютера, будет присвоен статус VIP.
- **Имя хоста**. Новым обнаружениям, связанным с этим именем хоста, будет присвоен статус VIP.
- **Email**. Новым обнаружениям, связанным с этим адресом электронной почты, будет присвоен статус VIP.

Пользователи с ролью **Аудитор** могут просматривать, импортировать и экспортировать список правил присвоения обнаружениям статуса VIP.

Пользователям с ролью **Сотрудник службы безопасности** просмотр списка правил присвоения обнаружениям статуса VIP недоступен.

В этом разделе

Просмотр таблицы правил присвоения статуса VIP 563
Создание правила присвоения статуса VIP 564
Удаление правила присвоения статуса VIP 564
Изменение правила присвоения статуса VIP 565
Импорт списка правил присвоения статуса VIP 565
Экспорт списка данных, исключенных из проверки 566
Фильтрация и поиск по типу правила присвоения статуса VIP 566
Фильтрация и поиск по значению правила присвоения статуса VIP 566
Фильтрация и поиск по описанию правила присвоения статуса VIP 567
Сброс фильтра правил присвоения статуса VIP 567

Просмотр таблицы правил присвоения статуса VIP

Таблица правил присвоения статуса VIP находится в разделе **Параметры**, подразделе **Статус VIP** веб-интерфейса приложения.

В таблице содержится следующая информация:

- **Критерий** – критерий добавления записи в список правил.
- **Значение** – значение критерия.
- **Описание** – дополнительная информация, указанная при создании правила.

Создание правила присвоения статуса VIP

► *Чтобы добавить правило присвоения обнаружениям статуса VIP:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Статус VIP**.
2. В правом верхнем углу окна веб-интерфейса приложения нажмите на кнопку **Добавить**.

   Откроется окно добавления правила.
3. В раскрывающемся списке **Критерий** выберите один из следующих типов правила:
   - **IP**, если вы хотите добавить правило для IP-адреса компьютера.
   - **Хост**, если вы хотите добавить правило для имени хоста.
   - **Email**, если вы хотите добавить правило для адреса электронной почты.
4. В поле **Значение** введите нужное значение.

   Например, если в списке **Критерий** вы выбрали **Email**, в поле **Значение** введите адрес электронной почты, для которого вы хотите добавить правило.
5. В поле **Описание** введите дополнительную информацию, если необходимо.
6. Нажмите на кнопку **Добавить**.

Правило будет добавлено. Новым обнаружениям, связанным с добавленным IP-адресом, именем хоста или адресом электронной почты, будет присвоен статус VIP.

Для пользователей с ролью **Аудитор** функция создания правил для присвоения обнаружениям статуса VIP недоступна.
Пользователям с ролью **Сотрудник службы безопасности** просмотр списка правил присвоения обнаружениям статуса VIP недоступен.

Удаление правила присвоения статуса VIP

► *Чтобы удалить правило присвоения обнаружениям статуса VIP:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Статус VIP**.
2. Установите флажок слева от каждого правила, которое вы хотите удалить из списка.
3. Если вы хотите удалить все правила, установите флажок над списком.
4. В правом верхнем углу окна веб-интерфейса приложения нажмите на кнопку **Удалить**.

   Отобразится окно подтверждения действия.

5. Нажмите на кнопку **Да**.

Выбранные правила будут удалены.

Для пользователей с ролью **Аудитор** функция удаления правил для присвоения обнаружениям статуса VIP недоступна.
Пользователям с ролью **Сотрудник службы безопасности** просмотр списка правил присвоения обнаружениям статуса VIP недоступен.

Изменение правила присвоения статуса VIP

► *Чтобы изменить правило присвоения обнаружениям статуса VIP:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Статус VIP**.
2. Выберите правило, которое вы хотите изменить.

   Откроется окно изменения правила.
3. Внесите необходимые изменения в поля **Критерий**, **Значение**, **Описание**.
4. Нажмите на кнопку **Сохранить**.

Правило будет изменено.

Для пользователей с ролью **Аудитор** функция изменения правил для присвоения обнаружениям статуса VIP недоступна.
Пользователям с ролью **Сотрудник службы безопасности** просмотр списка правил присвоения обнаружениям статуса VIP недоступен.

Импорт списка правил присвоения статуса VIP

► *Чтобы импортировать список правил присвоения обнаружениям статуса VIP:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Статус VIP**.
2. Нажмите на кнопку **Импортировать**.

   Отобразится подтверждение импорта списка.

   Импортированный список правил присвоения обнаружениям статуса VIP заменит текущий список правил присвоения обнаружениям статуса VIP.
3. Нажмите на кнопку **Да**.

   Откроется окно выбора файлов.
4. Выберите файл формата JSON со списком правил, которые вы хотите импортировать, и нажмите на кнопку **Открыть**.

Окно выбора файлов закроется.

Список будет импортирован.

Экспорт списка данных, исключенных из проверки

► *Чтобы экспортировать список исключений из проверки:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **Проверка**.
3. В правом верхнем углу окна веб-интерфейса приложения нажмите на кнопку **Экспортировать**.

Файл в формате JSON с экспортированным списком исключений из проверки будет сохранен в папку загрузки браузера на вашем компьютере.

Фильтрация и поиск по типу правила присвоения статуса VIP

► *Чтобы отфильтровать или найти правила присвоения обнаружениям статуса VIP по типу правила:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Статус VIP**.
2. По ссылке **Критерий** откройте окно настройки фильтрации.
3. Установите один или несколько флажков рядом с типами правил:
   - **IP**.
   - **Хост**.
   - **Email**.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск по значению правила присвоения статуса VIP

► *Чтобы отфильтровать или найти правила присвоения обнаружениям статуса VIP по значению правила:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Статус VIP**.
2. По ссылке **Значение** откройте окно настройки фильтрации.
3. Введите один или несколько символов значения правила.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск по описанию правила присвоения статуса VIP

► *Чтобы отфильтровать или найти правила присвоения обнаружениям статуса VIP по описанию:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Статус VIP**.
2. По ссылке **Описание** откройте окно настройки фильтрации.
3. Введите один или несколько символов описания.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра правил присвоения статуса VIP

► *Чтобы сбросить фильтр правил присвоения обнаружениям статуса VIP по одному или нескольким условиям фильтрации:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Статус VIP**.
2. Нажмите на кнопку ☒ справа от того заголовка столбца таблицы, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице отобразятся только правила, соответствующие заданным вами условиям.

Работа со списком исключений из проверки

Пользователи с ролью **Старший сотрудник службы безопасности** могут создавать, импортировать и экспортировать список *исключений из проверки* – список данных, которые Kaspersky Anti Targeted Attack Platform будет считать безопасными и не будет отображать в таблице обнаружений (см. раздел "Просмотр таблицы обнаружений" на стр. 331). Вы можете создать правила исключений из проверки для следующих данных:

- **MD5**.
- **Формат**.
- **Маска URL**.
- **Адрес получателя**.
- **Адрес отправителя**.
- **IP или подсеть источника**.
- **IP или подсеть назначения**.
- **Агент пользователя**.

Пользователи с ролью **Аудитор** и **Сотрудник службы безопасности** могут просматривать список правил исключений из проверки (см. раздел "Просмотр таблицы данных, исключенных из проверки" на стр. 568), а также экспортировать его.

В этом разделе

Просмотр таблицы данных, исключенных из проверки 568

Добавление правила исключения из проверки 569

Удаление правила исключения из проверки 570

Изменение правила, добавленного в исключения из проверки 571

Экспорт списка данных, исключенных из проверки 571

Фильтрация правил в списке исключений из проверки по критерию 572

Поиск правил в списке исключений из проверки по значению 572

Сброс фильтра правил в списке исключений из проверки 573

Просмотр таблицы данных, исключенных из проверки

► *Чтобы просмотреть таблицу с данными, исключенными из проверки:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Перейдите на закладку **Проверка**.

Отобразится таблица со списком данных, которые Kaspersky Anti Targeted Attack Platform будет считать безопасными и не будет создавать для них обнаружения. Вы можете фильтровать правила по ссылкам в названии столбцов.

В таблице содержится следующая информация:

- **Критерий** – критерий добавления записи в список разрешенных объектов.
- **Значение** – значение критерия.

Добавление правила исключения из проверки

► *Чтобы добавить правило исключения из проверки:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **Проверка**.
3. В правом верхнем углу окна веб-интерфейса приложения нажмите на кнопку **Добавить**.

   Откроется окно **Новое правило**.
4. В раскрывающемся списке **Критерий** выберите один из следующих критериев добавления правила в список исключений из проверки:
   - **MD5**.
   - **Формат**.
   - **Маска URL**.
   - **Адрес получателя**.
   - **Адрес отправителя**.
   - **IP или подсеть источника**.
   - **IP или подсеть назначения**.
   - **Агент пользователя**.
5. Если вы выбрали **Формат**, в раскрывающемся списке **Значение** выберите формат файла, который вы хотите добавить.

   Например, вы можете выбрать формат **MSOfficeDoc**.
6. Если вы выбрали **MD5**, **Маска URL**, **Адрес получателя**, **Адрес отправителя**, **IP или подсеть источника**, **IP или подсеть назначения** или **Агент пользователя**, в поле **Значение** введите значение соответствующего критерия, которое вы хотите добавить в список исключений из проверки:
   - Если вы выбрали **MD5**, в поле **Значение** введите MD5-хеш файла.
   - Если вы выбрали **Маска URL**, в поле **Значение** введите маску URL-адреса.

     При формировании маски вы можете использовать следующие специальные символы:

     * – любая последовательность символов.

Пример:

Если вы введете маску `*abc*`, приложение будет считать безопасным любой URL-адрес, содержащий последовательность `abc`. Например, `www.example.com/download_virusabc`

     ? – любой один символ.

Пример:

Если вы введете маску `example_123?.com`, приложение будет считать безопасным любой URL-адрес, содержащий заданную последовательность символов и любой символ, следующий за `3`. Например, `example_1234.com`

В случае, если символы `*` и `?` входят в состав полного URL-адреса, добавляемого в исключения из проверки, при вводе этих символов нужно использовать `\` – отмена одного из следующих за ним символов `*` или `?`, \.

Пример:

В качестве доверенного адреса требуется добавить следующий URL-адрес:
`www.example.com/download_virus/virus.dll?virus_name=`

Чтобы приложение не восприняло `?` как специальный символ формирования маски, нужно поставить перед `?` знак `\`.

URL-адрес, добавляемый в список исключений из проверки, будет выглядеть следующим образом:
`www.example.com/download_virus/virus.dll\?virus_name=`

- Если вы выбрали **Адрес получателя** или **Адрес отправителя**, в поле **Значение** введите адрес электронной почты.
- Если вы выбрали **Агент пользователя**, в поле **Значение** введите заголовок **User agent HTTP-запросов**, содержащий информацию о браузере.
- Если вы выбрали **IP или подсеть источника** или **IP или подсеть назначения**, в поле **Значение** введите адрес или подсеть (например, 255.255.255.0).

В полях **Маска URL**, **Адрес получателя**, **Адрес отправителя** вы можете указывать доменные имена, содержащие символы кириллицы. В этом случае указанный адрес будет преобразован в Punycode и обработан в соответствии с параметрами приложения.

7. Нажмите на кнопку **Добавить**.

Правило будет добавлено в список исключений из проверки.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция добавления правила исключения из проверки недоступна.

Удаление правила исключения из проверки

► *Чтобы удалить одно или несколько правил из списка исключений из проверки:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **Проверка**.
3. Установите флажок слева от каждого правила, которое вы хотите удалить из списка исключений из проверки.

Если вы хотите удалить все правила, установите флажок над списком.

4. В нижней части окна нажмите на кнопку **Удалить**.

   Отобразится окно подтверждения действия.

5. Нажмите на кнопку **Да**.

Выбранные правила будут удалены из списка исключений из проверки.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция удаления записи в списке исключений из проверки недоступна.

Изменение правила, добавленного в исключения из проверки

► *Чтобы изменить правило в списке исключений из проверки:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **Проверка**.
3. Выберите правило, которое вы хотите изменить.

   Откроется окно **Изменить правило**.

4. Внесите необходимые изменения в поля **Критерий** и **Значение**.
5. Нажмите на кнопку **Сохранить**.

Правило будет изменено.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция изменения правила в списке исключений из проверки недоступна.

Экспорт списка данных, исключенных из проверки

► *Чтобы экспортировать список исключений из проверки:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **Проверка**.
3. В правом верхнем углу окна веб-интерфейса приложения нажмите на кнопку **Экспортировать**.

Файл в формате JSON с экспортированным списком исключений из проверки будет сохранен в папку загрузки браузера на вашем компьютере.

Фильтрация правил в списке исключений из проверки по критерию

► *Чтобы отфильтровать записи в списке исключений из проверки по типу правила:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **Проверка**.
3. По ссылке **Критерий** откройте окно настройки фильтрации.
4. Установите один или несколько флажков рядом с критериями, по которым вы хотите отфильтровать правила:
   - **MD5**.
   - **Формат**.
   - **Маска URL**.
   - **Адрес получателя**.
   - **Адрес отправителя**.
   - **IP или подсеть источника**.
   - **IP или подсеть назначения**.
   - **Агент пользователя**.
5. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В списке исключений из проверки отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Поиск правил в списке исключений из проверки по значению

► *Чтобы найти правила в списке исключений из проверки по значению:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **Проверка**.
3. По ссылке **Значение** откройте окно настройки фильтрации.
4. Введите символы значения.
5. Нажмите на кнопку **Применить**.

В списке исключений из проверки отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра правил в списке исключений из проверки

► *Чтобы сбросить фильтр записей в списке исключений по одному или нескольким условиям фильтрации:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **Проверка**.
3. Нажмите на кнопку ☒ справа от того заголовка столбца таблицы записей в списке исключений из проверки, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В списке исключений из проверки отобразятся только правила, соответствующие заданным вами условиям.

Работа с IDS-исключениями

Пользователи с ролью **Старший сотрудник службы безопасности** могут добавлять правила IDS "Лаборатории Касперского" в исключения из проверки. Kaspersky Anti Targeted Attack Platform не будет создавать обнаружения по правилам IDS, добавленным в исключения.

Вы можете добавить в исключения только правила IDS "Лаборатории Касперского". Если вы не хотите применять при проверке пользовательское правило IDS, вы можете отключить это правило (см. раздел "Включение и отключение использования правила IDS при проверке событий" на стр. 522) или удалить (см. раздел "Удаление пользовательского правила IDS" на стр. 524) его.

Если вы хотите настроить точечное исключение, например, для выбранного адреса источника, вы можете выполнить следующие действия:

1. Добавить правила IDS "Лаборатории Касперского" в исключения из проверки (см. раздел "Добавление правила IDS в исключения" на стр. 574).
2. Добавить в список пользовательских правил IDS новое правило, созданное на основе исключенного правила "Лаборатории Касперского", одним из следующих способов:
   - Если в системе уже есть пользовательские правила IDS, вам нужно экспортировать (см. раздел "Экспорт файла пользовательского правила IDS на компьютер" на стр. 523) файл с правилами и дописать в этот файл новое правило с уточняющими условиями, используя синтаксис Suricata.

- Если в системе пока нет пользовательских правил IDS, вам нужно создать текстовый файл и добавить в него правило с уточняющими условиями, используя синтаксис Suricata.

3. Импортировать (см. раздел "Импорт пользовательского правила IDS" на стр. 521) файл с добавленным правилом.

Пользователи с ролью **Аудитор** могут просматривать список правил IDS, добавленных в исключения, и свойства выбранного правила.

Пользователям с ролью **Сотрудник службы безопасности** список правил IDS, добавленных в исключения, недоступен.

В этом разделе

Просмотр таблицы правил IDS, добавленных в исключения 574
Добавление правила IDS в исключения 574
Редактирование описания правила IDS, добавленного в исключения 575
Удаление правил IDS из исключений 576

Просмотр таблицы правил IDS, добавленных в исключения

► *Чтобы просмотреть таблицу правил IDS, добавленных в исключения:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Перейдите на закладку **IDS**.

Отобразится таблица правил IDS, добавленных в исключения. Вы можете фильтровать правила по ссылкам в названии столбцов.

В таблице содержится следующая информация:

- **Время создания** – дата и время добавления правила IDS в исключения.
- **Правило** – имя правила IDS.
- **ID правила** – идентификатор правила IDS. sid (signature ID) в формате Suricata.
- **Описание** – описание правила IDS.
- **Автор** – имя пользователя, под учетной записью которого правило IDS было добавлено в исключения.

Добавление правила IDS в исключения

Вы можете добавлять правила IDS "Лаборатории Касперского", по которым выполнены обнаружения средней и высокой степени важности, в исключения из проверки событий.

Вы можете добавить в исключения только правила IDS "Лаборатории Касперского". Если вы не хотите применять при проверке событий пользовательское правило IDS , вы можете отключить это правило (см. раздел "Включение и отключение использования правила IDS при проверке событий" на стр. 522) или удалить (см. раздел "Удаление пользовательского правила IDS" на стр. 524) его.

► *Чтобы добавить правило IDS в исключения:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. По ссылке в столбце **Технологии** откройте окно настройки фильтрации.
3. В раскрывающемся списке слева выберите **Содержит**.
4. В раскрывающемся списке справа выберите технологию **(IDS) Intrusion Detection System**.
5. Нажмите на кнопку **Применить**.
6. Если вы хотите отфильтровать обнаружения, по значку раскройте список параметров фильтрации и выберите нужный фильтр.
7. Выберите обнаружение, для которого в столбце **Обнаружено** отображается название нужного правила IDS.

   Откроется окно с информацией об обнаружении.
8. В правой части окна в блоке **Рекомендации** в разделе **Оценка** выберите **Добавить в исключения**.

   Откроется окно **Добавить правило IDS в исключения**.
9. В поле **Описание** введите описание правила IDS.
10. Нажмите на кнопку **Добавить**.

Правило IDS будет добавлено в исключения и отобразится в списке исключений в разделе **Параметры** веб-интерфейса приложения, подразделе **Исключения** на закладке **IDS**. Это правило не будет применяться при создании обнаружений.

Для пользователей с ролью **Аудитор** функция изменения записи в списке разрешенных объектов недоступна.
Пользователи с ролью **Сотрудник службы безопасности** не имеют доступа к списку правил IDS, добавленных в исключения.

Редактирование описания правила IDS, добавленного в исключения

► *Чтобы отредактировать описание правила IDS, добавленного в исключения, из раздела **Обнаружения**:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. По ссылке в столбце **Технологии** откройте окно настройки фильтрации.
3. В раскрывающемся списке слева выберите **Содержит**.
4. В раскрывающемся списке справа выберите технологию **(IDS) Intrusion Detection System**.
5. Нажмите на кнопку **Применить**.
6. Если вы хотите отфильтровать обнаружения, по значку раскройте список параметров фильтрации и выберите нужный фильтр.
7. Выберите обнаружение, для которого в столбце **Обнаружено** отображается название нужного правила IDS.

   Откроется окно с информацией об обнаружении.
8. В правой части окна в блоке **Рекомендации** в разделе **Оценка** выберите **Изменить исключение IDS**.

   Откроется окно **Изменить исключение IDS**.

   В поле **Описание** измените описание правила.

   Нажмите на кнопку **Сохранить**.

Описание правила IDS, добавленного в исключения, будет изменено. Это правило не будет применяться при создании обнаружений.

Для пользователей с ролью **Аудитор** функция редактирования описания правила IDS недоступна. Пользователи с ролью **Сотрудник службы безопасности** не имеют доступа к списку правил IDS, добавленных в исключения.

Удаление правил IDS из исключений

Вы можете удалить из исключений одно или несколько правил IDS, а также все правила сразу.

► *Чтобы удалить правило IDS из исключений:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Исключения** и перейдите на закладку **IDS**.
2. Отобразится список правил IDS, добавленных в исключения.
3. Выберите правило, которое вы хотите удалить из исключений.

   Откроется окно с информацией о правиле.
4. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.
5. Нажмите на кнопку **Да**.

Правило будет удалено из исключений. Правило будет применяться при создании обнаружений.

► *Чтобы удалить все или несколько правил IDS из исключений:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Исключения** и перейдите на закладку **IDS**.
2. Отобразится список правил IDS, добавленных в исключения.
3. Установите флажки напротив правил, которые вы хотите удалить из исключений.

   Вы можете выбрать все правила, установив флажок в строке с заголовками столбцов.
4. В панели управления в нижней части окна нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.
5. Нажмите на кнопку **Да**.

Выбранные правила будут удалены из исключений. Правила будут применяться при создании обнаружений.

Для пользователей с ролью **Аудитор** функция удаления правила IDS из исключений недоступна. Пользователи с ролью **Сотрудник службы безопасности** не имеют доступа к списку IDS-исключений.

Работа с ТАА-исключениями

Правила ТАА (IOA) (см. раздел "Об использовании индикаторов компрометации (IOC) и атаки (IOA) для поиска угроз" на стр. 499), сформированные специалистами "Лаборатории Касперского", содержат признаки подозрительного поведения объекта в IT-инфраструктуре организации. Kaspersky Anti Targeted Attack Platform проверяет базу событий приложения и создает обнаружения для событий, которые совпадают с поведением, описанным в правилах ТАА (IOA). Если вы хотите, чтобы приложение не создавало обнаружения для событий, сформированных в результате нормальной для вашей организации активности хоста, вы можете добавить правило ТАА (IOA) в исключения.

В приложении предусмотрены следующие режимы работы правил ТАА (IOA), добавленных в исключения:

- Правило исключается всегда.

  В этом случае Kaspersky Anti Targeted Attack Platform не отмечает события как соответствующие правилу ТАА (IOA) и не создает обнаружения по этому правилу.
- Правило дополняется условием.

  В этом случае правило ТАА (IOA) дополняется условиями в виде поискового запроса. Kaspersky Anti Targeted Attack Platform не отмечает события, подходящие под заданные условия, как соответствующие правилу ТАА (IOA). Для событий, которые соответствуют правилу ТАА (IOA), но не соответствуют условиям примененного исключения, приложение отмечает события и создает обнаружения.

Если вы используете режим распределенного решения и мультитенантности, исключения ТАА могут быть следующих типов:

- **Локальный** – созданные на сервере SCN. Действие исключений распространяется только на хосты, подключенные к этому серверу SCN. Исключения относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе приложения.

- **Глобальный** – созданные на сервере PCN. Действие исключений распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Исключения относятся к тенанту, в рамках которой пользователь работает в веб-интерфейсе приложения.

Пользователи с ролью **Старший сотрудник службы безопасности** могут создавать, редактировать, удалять исключения в рамках тех тенантов, к данным которых у них есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса приложения" на стр. 200).

Пользователи с ролью **Аудитор** и **Сотрудник службы безопасности** могут только просматривать список исключений TAA и свойства выбранного исключения.

Для каждого правила TAA (IOA) можно создать только одно локальное или глобальное исключение. Если для одного правила TAA (IOA) созданы исключения на сервере SCN и PCN, Kaspersky Anti Targeted Attack Platform обрабатывает события в соответствии с параметрами, заданными для исключения на сервере PCN.

В этом разделе

Просмотр таблицы правил TAA (IOA), добавленных в исключения 578
Добавление правила TAA (IOA) в исключения 579
Просмотр правила TAA (IOA), добавленного в исключения 582
Удаление правил TAA (IOA) из исключений 583

Просмотр таблицы правил TAA (IOA), добавленных в исключения

► *Чтобы просмотреть таблицу правил TAA (IOA), добавленных в исключения:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Перейдите закладку **TAA (IOA)**.

Отобразится таблица правил TAA (IOA), добавленных в исключения. Вы можете фильтровать правила по ссылкам в названии столбцов.

В таблице содержится следующая информация:

- – степень важности, присвоенная обнаружению, выполненному по этому правилу TAA (IOA).

  Степень важности может иметь одно из следующих значений:

  - – **Низкая**.
  - – **Средняя**.
  - – **Высокая**.
- **Тип** – тип правила в зависимости от роли сервера, на котором оно создано:

- **Локальный** – созданные на сервере SCN. Действие исключений распространяется только на хосты, подключенные к этому серверу SCN. Исключения относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе приложения (см. раздел "Начало работы в веб-интерфейсе приложения под учетной записью локального администратора" на стр. 186).
- **Глобальный** – созданные на сервере PCN. Действие исключений распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Исключения относятся к тенанту, в рамках которой пользователь работает в веб-интерфейсе приложения.

- **Надежность** – уровень надежности в зависимости от вероятности ложных срабатываний правила:
  - **Высокая**.
  - **Средняя**.
  - **Низкая**.

  Чем выше уровень надежности, тем меньше вероятность ложных срабатываний.
- **Исключать правило** – режим работы правила, добавленного в исключения.
  - **Всегда** – правило исключается всегда. В этом случае Kaspersky Anti Targeted Attack Platform не отмечает события как соответствующие правилу TAA (IOA) и не создает обнаружения по этому правилу.
  - **При условии** – правило исключается при добавлении условия. В этом случае правило TAA (IOA) дополняется условиями в виде поискового запроса. Kaspersky Anti Targeted Attack Platform не отмечает события, подходящие под заданные условия, как соответствующие правилу TAA (IOA). Для событий, которые соответствуют правилу TAA (IOA), но не соответствуют условиям примененного исключения, программа отмечает события и создает обнаружения.
- **Имя** – имя правила.

Добавление правила TAA (IOA) в исключения

Вы можете добавить в исключения только правила TAA (IOA) "Лаборатории Касперского". Если вы не хотите применять при проверке событий пользовательское правило TAA (IOA), вы можете отключить это правило (см. раздел "Включение и отключение использования правил TAA (IOA)" на стр. 510) или удалить (см. раздел "Удаление правил TAA (IOA)" на стр. 511) его.

► *Чтобы добавить правило TAA (IOA) в исключения из раздела **Обнаружения**:*

1. В окне веб-интерфейса приложения выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. По ссылке в столбце **Технологии** откройте окно настройки фильтрации.
3. В раскрывающемся списке слева выберите **Содержит**.
4. В раскрывающемся списке справа выберите технологию **(TAA) Targeted Attack Analyzer**.
5. Нажмите на кнопку **Применить**.

   В таблице отобразятся обнаружения, выполненные технологией TAA на основе правил TAA (IOA).

6. Выберите обнаружение, для которого в столбце **Обнаружено** отображается название нужного правила.

   Откроется окно с информацией об обнаружении.

7. В блоке **Результаты проверки** по ссылке с названием правила откройте окно с информацией о правиле.

8. Справа от названия параметра **Исключение ТАА (IOA)** нажмите на кнопку **Добавить в исключения**.

   Откроется окно добавления правила ТАА (IOA) в исключения.

9. В поле **Исключать правило** выберите режим работы исключения:

   - **Всегда**, если вы хотите, чтобы приложение не создавало обнаружения для событий, соответствующих выбранному правилу ТАА (IOA).
   - **При условии**, если вы хотите, чтобы приложение не создавало обнаружения только для событий, подходящих под заданные условия. Для событий, которые соответствуют правилу ТАА (IOA) при заданных условиях исключения, приложение создаст обнаружения.

     Если вы выбрали **При условии**, выполните следующие действия:

     a. По ссылке **Настройка дополнительных условий** откройте форму поиска событий.

     b. Если вы используете режим распределенного решения и мультитенантности и хотите включить отображение событий по всем тенантам, включите переключатель **Искать по всем тенантам**.

     c. Выполните поиск событий в режиме конструктора.

        Отобразится таблица событий, соответствующих правилу ТАА (IOA) при заданных условиях исключения.

        Если вы используете режим распределенного решения и мультитенантности, отобразятся уровни группировки найденных событий: Сервер – Названия тенантов – Имена серверов.

     d. Нажмите на имя того сервера, события которого вы хотите просмотреть.

        Отобразится таблица хостов выбранного сервера. Уровни группировки событий отобразятся над таблицей.

        При необходимости вы можете изменить условия поиска событий.

     e. Нажмите на кнопку **Добавить исключение**.

10. Если вы используете режим распределенного решения и мультитенантности, в поле **Применить к серверам*** установите флажки напротив тенантов и серверов, к которым будет применяться правило.

11. Нажмите на кнопку **Добавить**.

Правило ТАА (IOA) будет добавлено в исключения и отобразится в списке исключений в разделе **Параметры** веб-интерфейса приложения, подразделе **Исключения** на закладке **ТАА (IOA)**. Это правило не будет применяться при создании обнаружений.

► *Чтобы добавить правило ТАА (IOA) в исключения из раздела **Поиск угроз**:*

1. В окне веб-интерфейса приложения выберите раздел **Поиск угроз**.

   Откроется форма поиска событий.

2. Задайте условия поиска и нажмите на кнопку **Найти**. Например, вы можете выбрать критерии для поиска событий в группе **Свойства ТАА** в режиме конструктора.

   Отобразится таблица событий, удовлетворяющих условиям поиска.

3. Выберите событие.
4. Справа от названия параметра **Теги IOA** нажмите на имя правила.

   Откроется окно с информацией о правиле.

5. Справа от названия параметра **Исключение ТАА (IOA)** нажмите на кнопку **Добавить в исключения**.

   Откроется окно добавления правила ТАА (IOA) в исключения.

6. В поле **Исключать правило** выберите режим работы исключения:
   - **Всегда**, если вы хотите, чтобы приложение не создавало обнаружения для событий, соответствующих выбранному правилу ТАА (IOA).
   - **При условии**, если вы хотите, чтобы приложение не создавало обнаружения только для событий, подходящих под заданные условия. Для событий, которые соответствуют правилу ТАА (IOA) при заданных условиях исключения, приложение создаст обнаружения.

     Если вы выбрали **При условии**, выполните следующие действия:

     a. По ссылке **Настройка дополнительных условий** откройте форму поиска событий.

     b. Если вы используете режим распределенного решения и мультитенантности и хотите включить отображение событий по всем тенантам, включите переключатель **Искать по всем тенантам**.

     c. Выполните поиск событий в режиме конструктора.

        Отобразится таблица событий, соответствующих правилу ТАА (IOA) при заданных условиях исключения.

        Если вы используете режим распределенного решения и мультитенантности, отобразятся уровни группировки найденных событий: Сервер – Названия тенантов – Имена серверов.

     d. Нажмите на имя того сервера, события которого вы хотите просмотреть.

        Отобразится таблица хостов выбранного сервера. Уровни группировки событий отобразятся над таблицей.

        При необходимости вы можете изменить условия поиска событий.

     e. Нажмите на кнопку **Добавить исключение**.

7. Нажмите на кнопку **Добавить**.

Правило ТАА (IOA) будет добавлено в исключения и отобразится в списке исключений в разделе **Параметры** веб-интерфейса приложения, подразделе **Исключения** на закладке **ТАА (IOA)**. Это правило не будет применяться при проверке событий.

При создании поискового запроса, сохраняемого как условия исключения, не рекомендуется использовать следующие поля:

- IOAId.
- IOATag.
- IOATechnique.

- IOATactics.
- IOAImportance.
- IOAConfidence.

Перечисленные поля отображаются только после того, как Kaspersky Anti Targeted Attack Platform отмечает события как подходящие под правила TAA (IOA).

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция добавления правила TAA (IOA) в исключения недоступна.

Просмотр правила TAA (IOA), добавленного в исключения

► *Чтобы просмотреть правило TAA (IOA), добавленное в исключения:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения** и перейдите на закладку **TAA (IOA)**.

   Отобразится таблица правил TAA (IOA), добавленных в исключения.

2. Выберите правило, которое вы хотите просмотреть.

Откроется окно с информацией о правиле.

Окно содержит следующую информацию:

- **Правило TAA (IOA)** – по ссылке открывается окно с описанием техники MITRE, соответствующей этому правилу, рекомендациями по реагированию на событие и данными о вероятности ложных срабатываний.
- **ID** – идентификатор, присваиваемый приложением каждому правилу.
- **Имя** – имя правила, которое вы указали при добавлении правила.
- **Важность** – оценка возможного влияния события на безопасность компьютеров или локальной сети организации, по оценке специалистов "Лаборатории Касперского".
- **Надежность** – уровень надежности в зависимости от вероятности ложных срабатываний, по оценке специалистов "Лаборатории Касперского".
- **Исключать правило** – режим работы правила, добавленного в исключения.
  - **Всегда** – правило исключается всегда. В этом случае Kaspersky Anti Targeted Attack Platform не отмечает события как соответствующие правилу TAA (IOA) и не создает обнаружения по этому правилу.
  - **При условии** – правило исключается при добавлении условия. В этом случае правило TAA (IOA) дополняется условиями в виде поискового запроса. Kaspersky Anti Targeted Attack Platform не отмечает события, подходящие под заданные условия, как соответствующие правилу TAA (IOA). Для событий, которые соответствуют правилу TAA (IOA), но не соответствуют условиям примененного исключения, программа отмечает события и создает обнаружения.
- **Настройка дополнительных условий** – по ссылке открывается форма поиска событий с условиями поискового запроса.

Поле отображается, если при добавлении правила ТАА (IOA) в исключения вы выбрали режим работы правила **При условии** и задали условия поискового запроса.

- Условия поискового запроса в формате `<IOA ID> AND NOT <условия поискового запроса>`.

  Условия поискового запроса отображаются, если при добавлении правила ТАА (IOA) в исключения вы выбрали режим работы правила **При условии** и задали условия поискового запроса.

- **Применить к серверам*** – хосты, к которым применяется исключение.

  Поле отображается в режиме распределенного решения и мультитенантности.

Удаление правил ТАА (IOA) из исключений

Вы можете удалить из исключений одно или несколько правил ТАА (IOA), а также все правила сразу.

► *Чтобы удалить правило ТАА (IOA) из исключений, выполните следующие действия:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения** и перейдите на закладку **ТАА (IOA)**.

   Отобразится таблица правил ТАА (IOA), добавленных в исключения.

2. Выберите правило, которое вы хотите удалить из исключений.

   Откроется окно с информацией о правиле.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Правило будет удалено из исключений. Правило будет применяться при создании обнаружений и при проверке событий.

► *Чтобы удалить все или несколько правил ТАА (IOA) из исключений, выполните следующие действия:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения** и перейдите на закладку **ТАА (IOA)**.
2. Отобразится таблица правил ТАА (IOA), добавленных в исключения.
3. Установите флажки напротив правил, которые вы хотите удалить из исключений.

   Вы можете выбрать все правила, установив флажок в строке с заголовками столбцов.

4. В панели управления в нижней части окна нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

5. Нажмите на кнопку **Да**.

Выбранные правила будут удалены из исключений. Правила будут применяться при создании обнаружений и при проверке событий.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция удаления из исключений правил TAA (IOA) недоступна.

Работа с ICAP-исключениями

Пользователи с ролью **Старший сотрудник службы безопасности** могут создавать список ICAP-исключений – список данных, которые Kaspersky Anti Targeted Attack Platform не будет проверять. Вы можете создать правила ICAP-исключений для следующих данных:

- **Формат**.
- **Агент пользователя**.
- **MD5**.
- **Маска URL**.
- **IP или подсеть источника**.

Пользователи с ролью **Аудитор** и **Сотрудник службы безопасности** могут просматривать список правил ICAP-исключений.

В режиме распределенного решения ICAP-исключения, созданные на SCN, распространяются на все компоненты Sensor, подключенные к этой SCN. ICAP-исключения, созданные на PCN, распространяются на SCN, установленную на одном устройстве с PCN, и все подключенные к этой SCN компоненты Sensor.

В этом разделе

Просмотр таблицы ICAP-исключений 585
Добавление правила в ICAP-исключения 585
Удаление правил из ICAP-исключений 587
Изменение и выключение правила в списке ICAP-исключений 587
Фильтрация правил в списке ICAP-исключений по критерию 588
Фильтрация правил в списке ICAP-исключений по значению 588
Фильтрация правил в списке ICAP-исключений по состоянию 589
Сброс условий фильтрации правил в списке ICAP-исключений 589

Просмотр таблицы ICAP-исключений

► *Чтобы просмотреть таблицу ICAP-исключений:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **ICAP**.

   Отобразится таблица данных, которые Kaspersky Anti Targeted Attack Platform не будет проверять. Вы можете фильтровать правила по ссылкам в названии столбцов.

В столбцах таблицы содержится следующая информация:

- **Значение** – значение критерия.
- **Критерий** – критерий добавления записи в список разрешенных объектов.
- **Состояние** – состояние правила.

Добавление правила в ICAP-исключения

Правила ICAP-исключения обрабатываются в том случае, если правило с данными не было ранее добавлено в правила исключений из проверки (см. раздел "Добавление правила исключения из проверки" на стр. 569).

► *Чтобы добавить правило в ICAP-исключения:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **ICAP**.
3. В правом верхнем углу окна веб-интерфейса приложения нажмите на кнопку **Добавить**.

   Откроется окно **Новое правило**.
4. Установите переключатель **Состояние** в нужное положение.

   По умолчанию переключатель находится в положении **Включено**.
5. В раскрывающемся списке **Критерий** выберите один из следующих критериев добавления правила в список ICAP-исключений:
   - **Формат**.
   - **Агент пользователя**.
   - **MD5**.
   - **Маска URL**.
   - **IP или подсеть источника**.
6. В зависимости от выбранного критерия укажите в поле **Значение** следующую информацию:
   - Если вы выбрали **Формат**, в раскрывающемся списке выберите формат файла, который вы хотите добавить.

При добавлении правила ICAP-исключения по формату содержимое веб-страниц соответствующего формата будет загружаться без проверки, а также не нарушится отображение веб-страниц.

- Если вы выбрали **Агент пользователя**, введите заголовок `User agent HTTP-запросов`, содержащий информацию о браузере.
- Если вы выбрали **MD5**, введите MD5-хеш файла.
- Если вы выбрали **Маска URL**, введите маску URL-адреса.

  При формировании маски вы можете использовать следующие специальные символы:

  * – любая последовательность символов.

Пример:

Если вы введете маску `*abc*`, приложение не будет проверять любой URL-адрес, содержащий последовательность `abc`. Например, `www.example.com/download_virusabc`

  ? – любой один символ.

Пример:

Если вы введете маску `example_123?.com`, приложение не будет проверять любой URL-адрес, содержащий заданную последовательность символов и любой символ, следующий за `3`. Например, `example_1234.com`

  Если символы `*` и `?` входят в состав полного URL-адреса, добавляемого в исключения из проверки, при вводе этих символов нужно использовать `\` – отмена одного из следующих за ним символов `*` или `?`, \.

Пример:

В качестве доверенного адреса требуется добавить следующий URL-адрес:
`www.example.com/download_virus/virus.dll?virus_name=`

Чтобы приложение не восприняло `?` как специальный символ формирования маски, нужно поставить перед `?` знак `\`.

URL-адрес, добавляемый в список исключений из проверки, будет выглядеть следующим образом:
`www.example.com/download_virus/virus.dll\?virus_name=`

В поле **Маска URL** вы можете указывать доменные имена, содержащие символы кириллицы. В этом случае указанный адрес будет преобразован в Punycode и обработан в соответствии с параметрами приложения.

- Если вы выбрали **IP или подсеть источника**, введите адрес или подсеть (например, 255.255.255.0).

7. Нажмите на кнопку **Добавить**.

Правило будет добавлено в список ICAP-исключений.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция добавления правила ICAP-исключений недоступна.

Удаление правил из ICAP-исключений

► *Чтобы удалить одно или несколько правил из списка ICAP-исключений:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **ICAP**.
3. Установите флажок слева от каждого правила, которое вы хотите удалить из списка ICAP-исключений.

   Если вы хотите удалить все правила, установите флажок над списком.
4. В нижней части окна нажмите на кнопку **Удалить**.
5. В открывшемся окне подтвердите удаление правил, нажав на кнопку **Да**.

Выбранные правила будут удалены из списка ICAP-исключений. Данные, которые находились в правилах ICAP-исключений, будут проверяться Kaspersky Anti Targeted Attack Platform.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция удаления записи в списке ICAP-исключений недоступна.

Изменение и выключение правила в списке ICAP-исключений

► *Чтобы изменить правило в списке ICAP-исключений:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **ICAP**.
3. Выберите правило, которое вы хотите изменить.

   Откроется окно **Изменить правило**.
4. Внесите необходимые изменения в поля **Состояние**, **Критерий** и **Значение**.
5. Нажмите на кнопку **Сохранить**.

Правило будет изменено.

► *Чтобы выключить правило в списке ICAP-исключений:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Перейдите на закладку **ICAP**.

3. Справа от правила, которое вы хотите выключить в списке ICAP-исключений, в столбце **Состояние** переведите переключатель в положение **Выключено**.
4. В открывшемся окне подтвердите выключение правила, нажав на кнопку **Да**.

Правило будет выключено.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция изменения и выключения правила в списке ICAP-исключений недоступна.

Фильтрация правил в списке ICAP-исключений по критерию

► *Чтобы фильтровать записи в списке ICAP-исключений по критерию:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **ICAP**.
3. По ссылке **Критерий** откройте окно настройки фильтрации.
4. Установите один или несколько флажков рядом с критериями, по которым вы хотите отфильтровать правила:
   - **Формат**.
   - **Агент пользователя**.
   - **MD5**.
   - **Маска URL**.
   - **IP или подсеть источника**.
5. Нажмите на кнопку **Применить**.

   Окно настройки фильтрации закроется.

В списке ICAP-исключений отобразятся только правила, соответствующие заданным условиям фильтрации. Вы можете одновременно выполнять фильтрацию по столбцам **Значение** и **Состояние**.

Фильтрация правил в списке ICAP-исключений по значению

► *Чтобы фильтровать правила в списке ICAP-исключений по значению:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **ICAP**.
3. По ссылке **Значение** откройте окно настройки фильтрации.
4. Введите значение.
5. Нажмите на кнопку **Применить**.

В списке ICAP-исключений отобразятся только правила, соответствующие заданным условиям поиска. Вы можете одновременно выполнять фильтрацию по столбцам **Критерий** и **Состояние**.

Фильтрация правил в списке ICAP-исключений по состоянию

► *Чтобы фильтровать правила в списке ICAP-исключений по состоянию:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **ICAP**.
3. По ссылке **Состояние** откройте окно настройки фильтрации.
4. Установите флажок напротив одного из значений:
   - **Включено**.
   - **Выключено**.
5. Нажмите на кнопку **Применить**.

В списке ICAP-исключений отобразятся только правила, соответствующие заданным условиям поиска. Вы можете одновременно выполнять фильтрацию по столбцам **Критерий** и **Значение**.

Сброс условий фильтрации правил в списке ICAP-исключений

► *Чтобы сбросить условия фильтрации правил в списке ICAP-исключений:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Исключения**.
2. Откройте вкладку **ICAP**.
3. Нажмите на кнопку ☒ справа от того заголовка столбца таблицы **Значение**, **Критерий** или **Состояние**, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные условия фильтрации будут сброшены. В списке ICAP-исключений отобразятся только правила, соответствующие заданным условиям.

Создание списка паролей для архивов

Приложение не проверяет архивы, защищенные паролем. Вы можете создать список наиболее часто встречающихся паролей для архивов, которые используются при обмене файлами в вашей организации. В этом случае при проверке архива приложение будет проверять пароли из списка. Если какой-либо из паролей подойдет, архив будет разблокирован и проверен.

Список паролей, заданный в параметрах приложения, также передается на сервер с компонентом Sandbox.

► *Чтобы создать список паролей для архивов:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Пароли к архивам**.
2. В поле **Пароли к архивам** введите пароли, которые приложение будет использовать для архивов, защищенных паролем.

   Вводите каждый пароль с новой строки. Вы можете ввести до 50 паролей.
3. Нажмите на кнопку **Применить**.

Список паролей для архивов будет создан. При проверке файлов формата PDF, а также файлов приложений Microsoft Word, Excel®, PowerPoint®, защищенных паролем, приложение будет подбирать пароли из заданного списка.

Пользователи с ролью **Аудитор** могут просматривать список паролей для архивов без возможности редактирования.

Просмотр параметров сервера

Пользователям с ролью **Аудитор** доступен просмотр настроек сервера Central Node и PCN в режиме распределенного решения и мультитенантности.

Настройки сервера располагаются в разделе **Параметры** окна веб-интерфейса. В этом разделе вы можете просмотреть следующую информацию:

- **Пользователи** – список учетных записей пользователей (см. раздел "Просмотр таблицы учетных записей пользователей" на стр. 198) веб-интерфейса приложения.
- **Общие параметры** – общие параметры сервера.
  - **Обновление баз** – обновление баз данных (см. раздел "Обновление баз приложения" на стр. 317).
  - **Мониторинг** – максимальное допустимое значение заполнения жесткого диска серверов Central Node и Sensor.
  - **SNMP** – параметры соединения с протоколом SNMP (см. раздел "Настройка соединения с протоколом SNMP" на стр. 282).
  - **Управление сервером** – управление сервером.
- **Сертификаты** – состояние сертификатов сервера и компьютеров с компонентом Endpoint Agent.
- **Дата и время** – настройки даты и времени сервера (см. раздел "Настройка даты и времени сервера" на стр. 254).
- **Endpoint Agents** – функции приложения, доступные при интеграции с компонентом Endpoint Agent.
  - **Расписание IOC-проверки** – настройки расписания IOC-проверки (см. раздел "Настройка расписания IOC-проверки" на стр. 519).
  - **Автоматическая отправка файлов в Sandbox** – автоматическая отправка файлов на проверку компоненту Sandbox (см. раздел "Автоматическая отправка файлов с хостов с компонентом Endpoint Agent на проверку в Sandbox по правилам TAA (IOA) "Лаборатории Касперского"" на стр. 451).

- **Индикаторы активности** – показатели активности компонента Endpoint Agent (см. раздел "Настройка показателей активности компонента Endpoint Agent" на стр. 293).
- **Автоматическое удаление неактивных хостов** – автоматическое удаление неактивных хостов из таблицы Endpoint Agents (см. раздел "Автоматическое удаление неактивных хостов" на стр. 294).

- **KSN/KPSN и MDR** – настройки участия в Kaspersky Security Network и Kaspersky Privat Security Network.
- **Репутационная база KPSN** – настройки использования репутационной базы KPSN (см. раздел "Настройка подключения к локальной репутационной базе KPSN" на стр. 211).
- **SIEM-система** – настройки интеграции с SIEM-системой (см. раздел "Настройка интеграции с SIEM-системой" на стр. 304).
- **Уведомления** – настройки отправки уведомлений (см. раздел "Отправка уведомлений" на стр. 597)
- **Статус VIP** – список правил присвоения обнаружениям статуса VIP (см. раздел "Работа с правилами присвоения обнаружениям статуса VIP" на стр. 563).
- **Исключения** – список разрешенных объектов (см. раздел "Работа со списком исключений из проверки" на стр. 568) и списки исключений из правил TAA (см. раздел "Работа с TAA-исключениями" на стр. 577) и IDS (см. раздел "Работа с IDS-исключениями" на стр. 573).
- **Сетевые параметры** – настройки параметров сетевого интерфейса (см. раздел "Настройка параметров сетевого интерфейса" на стр. 257).
- **Пароли к архивам** – список паролей для архивов (см. раздел "Создание списка паролей для архивов" на стр. 319).
- **Лицензия** – состояние ключа лицензии (см. раздел "Просмотр информации о лицензии и добавленных ключах в веб-интерфейсе Central Node" на стр. 158).
- **Журнал активности** – настройки журнала активности (см. раздел "Управление журналом активности" на стр. 312).

Просмотр таблицы серверов с компонентом Sandbox

Пользователи с ролью **Аудитор** могут просматривать таблицу серверов с компонентом Sandbox (см. раздел "Расчеты для компонента Sandbox" на стр. 103).

Таблица серверов с компонентом Sandbox находится в разделе **Серверы Sandbox**, на закладке **Серверы** окна веб-интерфейса приложения.

В поле **Отпечаток сертификата** отображается отпечаток TLS-сертификата сервера Central Node.

Таблица **Список серверов** содержит следующую информацию:

- **IP и имя** – IP-адрес или полное доменное имя сервера с компонентом Sandbox.
- **Отпечаток сертификата** – отпечаток сертификата сервера с компонентом Sandbox.
- **Авторизация** – статус запроса на подключение к компоненту Sandbox.
- **Состояние** – состояние подключения к компоненту Sandbox.

Для пользователей с ролью **Сотрудник службы безопасности** просмотр таблицы серверов с компонентом Sandbox недоступен.

Просмотр параметров набора операционных систем для проверки объектов в Sandbox

Пользователи с ролью **Аудитор** могут просматривать параметры набора операционных систем, на основе которого будут формироваться задачи на проверку объектов для компонента Sandbox. На сервере Sandbox должны быть установлены виртуальные машины (см. раздел "Установка и настройка образов операционных систем и приложений для работы компонента Sandbox" на стр. 221), которые соответствуют выбранному набору.

Информация о параметрах набора операционных систем для проверки объектов в Sandbox находится в разделе **Серверы Sandbox**, на закладке **Параметры** окна веб-интерфейса приложения.

В блоке параметров **Набор ОС** отображаются наборы операционных систем, в которых компонент Sandbox может проверять объекты.

В блоке параметров **Состав набора** отображаются операционные системы, которые входят в состав выбранного набора.

Просмотр таблицы серверов с компонентом Sensor

Таблица серверов с компонентом Sensor находится в разделе **Серверы Sensor** окна веб-интерфейса приложения.

В поле **Отпечаток сертификата** отображается отпечаток TLS-сертификата сервера Central Node.

В таблице **Список серверов** содержится следующая информация:

- **IP/имя** – IP-адрес или доменное имя сервера с компонентом Sensor.
- **Тип** – тип компонента Sensor. Может принимать следующие значения:
  - **Central Node** – компонент Sensor установлен на том же сервере, что и компонент Central Node.
  - **Удаленный** – компонент Sensor установлен на другом сервере или в качестве компонента Sensor используется почтовый сенсор.
- **Отпечаток сертификата** – отпечаток TLS-сертификата, с помощью которого устанавливается шифрованное соединение между серверами с компонентами Sensor и Central Node.
- **KSN/KPSN** – состояние подключения к репутационным базам KSN/KPSN.
- **SPAN** – состояние обработки SPAN-трафика.
- **SMTP** – состояние интеграции с почтовым сервером по протоколу SMTP.
- **ICAP** – состояние интеграции с прокси-сервером по протоколу ICAP.
- **POP3** – состояние интеграции с почтовым сервером по протоколу POP3.
- **Состояние** – состояние запроса на подключение.

Работа с сырым сетевым трафиком

При работе в веб-интерфейсе приложения пользователи с ролью **Старший сотрудник службы безопасности** могут выгружать дампы сырого сетевого трафика в формате PCAP с серверов с компонентом Sensor и проводить расследование для обнаружения подозрительной активности.

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия на том сервере PCN или SCN, к которому подключен сервер с компонентом Sensor.

► *Чтобы выгрузить сырой сетевой трафик, захваченный с сетевых интерфейсов:*

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.

   Отобразится таблица **Список серверов**.

2. Выберите компонент Sensor, с которого вы хотите выгрузить сырой сетевой трафик.

   Отобразится страница с параметрами компонента Sensor.

3. Выберите сетевые интерфейсы, с которых вы хотите выгрузить сырой сетевой трафик, установив флажок слева от названия сетевого интерфейса.

   По умолчанию, выбраны все сетевые интерфейсы.

   Если в столбце **Проверка SPAN-трафика** переключатель справа от названия сетевого интерфейса установлен в положении **Выключено**, вы не сможете выгрузить с этого сетевого интерфейса дампы сырого сетевого трафика.

4. Нажмите на кнопку **Выгрузить трафик**.

   Отобразится окно настройки параметров выгрузки сырого сетевого трафика.

   В открывшемся окне в поле **Первый сохраняемый дамп** отображается дата и время первого сохраненного дампа сырого сетевого трафика, в поле **Последний сохраняемый дамп** отображается дата и время последнего сохраненного дампа сырого сетевого трафика. В поле **Доступно в хранилище дампов** первое число обозначает свободное пространство в хранилище дампов, а второе число обозначает общий размер хранилища дампов.

5. Выберите поле **Период** и выполните следующие действия:

   a. В открывшемся календаре укажите даты начала и конца периода, за который вы хотите выгрузить сырой сетевой трафик.

   b. Нажмите на кнопку **Применить**.

6. В поле **Максимальный размер дампа** укажите максимальный размер скачиваемого дампа сырого сетевого трафика.

   Значение по умолчанию: 100 МБ. Минимальное возможное значение – 1 МБ, максимальное – 1000000 ТБ.

7. Если вы хотите ограничить выгрузку данных в сыром сетевом трафике, в поле **Фильтрация трафика BPF** переведите переключатель в положение **Включено**.

   По умолчанию переключатель находится в положении **Выключено**.

8. Если вы перевели переключатель в поле **Фильтрация трафика BPF** в положение **Включено**, введите в поле **Правило фильтрации** правило фильтрации**.** Для написания правила фильтрации BPF используется формат libpcap. Подробнее об описании синтаксиса см. в Руководстве pcap-filter https://www.tcpdump.org/manpages/pcap-filter.7.html.

   Пример выражения для фильтрации:

   ```
   tcp port 102 or tcp port 502
   ```

9. Если вы хотите ограничить выгрузку данных в сыром сетевом трафике, в поле **Фильтрация трафика Regexp** переведите переключатель в положение **Включено**.

   По умолчанию переключатель находится в положении **Выключено**.

10. Если вы перевели переключатель в поле **Фильтрация трафика Regexp]** в положение **Включено**, введите в поле **Правило фильтрации** правило фильтрации**.**

    Пример выражения для фильтрации:

    ```
    ^test.+xABxCD
    ```

11. Нажмите на кнопку **Выгрузить**.

Дампы сырого сетевого трафика будут выгружены.

В этом разделе

Выгрузка сырого сетевого трафика, захваченного с сетевых интерфейсов 594

Выгрузка сырого сетевого трафика, захваченного с сетевых интерфейсов

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия на том сервере PCN или SCN, к которому подключен сервер с компонентом Sensor.

► *Чтобы выгрузить сырой сетевой трафик, захваченный с сетевых интерфейсов:*

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.

   Отобразится таблица **Список серверов**.

2. Выберите компонент Sensor, с которого вы хотите выгрузить сырой сетевой трафик.

   Отобразится страница с параметрами компонента Sensor.

3. Выберите сетевые интерфейсы, с которых вы хотите выгрузить сырой сетевой трафик, установив флажок слева от названия сетевого интерфейса.

   По умолчанию, выбраны все сетевые интерфейсы.

   Если в столбце **Проверка SPAN-трафика** переключатель справа от названия сетевого интерфейса установлен в положении **Выключено**, вы не сможете выгрузить с этого сетевого интерфейса дампы сырого сетевого трафика.

4. Нажмите на кнопку **Выгрузить трафик**.

   Отобразится окно настройки параметров выгрузки сырого сетевого трафика.

   В открывшемся окне в поле **Первый сохраняемый дамп** отображается дата и время первого сохраненного дампа сырого сетевого трафика, в поле **Последний сохраняемый дамп** отображается дата и время последнего сохраненного дампа сырого сетевого трафика. В поле **Доступно в хранилище дампов** первое число обозначает свободное пространство в хранилище дампов, а второе число обозначает общий размер хранилища дампов.

5. Выберите поле **Период** и выполните следующие действия:

   a. В открывшемся календаре укажите даты начала и конца периода, за который вы хотите выгрузить сырой сетевой трафик.

   b. Нажмите на кнопку **Применить**.

6. В поле **Максимальный размер дампа** укажите максимальный размер скачиваемого дампа сырого сетевого трафика.

   Значение по умолчанию: 100 МБ. Минимальное возможное значение – 1 МБ, максимальное – 1000000 ТБ.

7. Если вы хотите ограничить выгрузку данных в сыром сетевом трафике, в поле **Фильтрация трафика BPF** переведите переключатель в положение **Включено**.

   По умолчанию переключатель находится в положении **Выключено**.

8. Если вы перевели переключатель в поле **Фильтрация трафика BPF** в положение **Включено**, введите в поле **Правило фильтрации** правило фильтрации**.** Для написания правила фильтрации BPF используется формат libpcap. Подробнее об описании синтаксиса см. в Руководстве pcap-filter https://www.tcpdump.org/manpages/pcap-filter.7.html.

   Пример выражения для фильтрации:

   ```
   tcp port 102 or tcp port 502
   ```

9. Если вы хотите ограничить выгрузку данных в сыром сетевом трафике, в поле **Фильтрация трафика Regexp** переведите переключатель в положение **Включено**.

   По умолчанию переключатель находится в положении **Выключено**.

10. Если вы перевели переключатель в поле **Фильтрация трафика Regexp]** в положение **Включено**, введите в поле **Правило фильтрации** правило фильтрации**.**

    Пример выражения для фильтрации:

    ```
    ^test.+xABxCD
    ```

11. Нажмите на кнопку **Выгрузить**.

Дампы сырого сетевого трафика будут выгружены.

Просмотр таблицы внешних систем

Пользователи с ролью **Аудитор** могут просматривать таблицу внешних систем.

Таблица внешних систем находится в разделе **Внешние системы** окна веб-интерфейса приложения.

В поле **Отпечаток сертификата** отображается отпечаток TLS-сертификата сервера Central Node.

В таблице **Список серверов** содержится следующая информация:

- **Sensor** – IP-адрес или доменное имя сервера внешней системы.
- **Тип** – тип внешней системы (почтовый сенсор или другая система).
- **Имя** – название интегрированной внешней системы, не являющейся почтовым сенсором.

  Для почтового сенсора в этой столбце отображается прочерк.
- **ID** – идентификатор внешней системы.
- **Отпечаток сертификата** – отпечаток TLS-сертификата сервера с внешней системой, с помощью которого устанавливается шифрованное соединение с сервером Central Node.

  Отпечаток сертификата сервера с компонентом Central Node отображается в верхней части окна в поле **Отпечаток сертификата**.
- **Состояние** – состояние запроса на интеграцию.

Для пользователей с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** просмотр таблицы внешних систем недоступен.

Отправка уведомлений

Пользователи с ролью **Администратор**, **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности** могут настроить отправку уведомлений на один или несколько адресов электронной почты.

Вы можете создать уведомления об обнаружениях и о работоспособности системы.

Пользователи с ролью **Аудитор** могут просматривать список правил для отправки уведомлений, свойства выбранного правила и параметры соединения с почтовым сервером без возможности редактирования.

Для корректной отправки уведомлений на адрес электронной почты необходимо предварительно настроить параметры соединения с почтовым сервером. Настройку соединения выполняет **Администратор**.

В этом разделе

Просмотр таблицы правил для отправки уведомлений 597

Создание правила для отправки уведомлений об обнаружениях 598

Создание правила для отправки уведомлений о работе компонентов приложения 599

Включение и отключение правила для отправки уведомлений 600

Изменение правила для отправки уведомлений 600

Удаление правила для отправки уведомлений 600

Фильтрация и поиск правил отправки уведомлений по типу правила 601

Фильтрация и поиск правил отправки уведомлений по теме уведомлений 601

Фильтрация и поиск правил отправки уведомлений по адресу электронной почты 602

Фильтрация и поиск правил отправки уведомлений по их состоянию 602

Сброс фильтра правил отправки уведомлений 603

Просмотр таблицы правил для отправки уведомлений

Правила для отправки уведомлений отображаются в разделе **Параметры**, подразделе **Уведомления** окна веб-интерфейса приложения.

Таблица правил для отправки уведомлений содержит следующую информацию:

- **Тип** – тип правила для отправки уведомлений.

  Возможны следующие типы правил:

  - **Обнаружения** – правило для отправки уведомления об обнаружениях;
  - **Работа приложения** – правило для отправки уведомления о работе компонентов приложения.
- **Тема** – тема сообщения с уведомлением.

- **Кому** – адреса электронной почты, на которые отправляются уведомления.
- **Состояние** – состояние правила для отправки уведомления.

Создание правила для отправки уведомлений об обнаружениях

► *Чтобы создать правило для отправки уведомлений об обнаружениях:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. Нажмите на кнопку **Добавить**.

   Откроется окно **Новое правило**.
4. В поле **Кому** введите один или несколько адресов электронной почты, на которые вы хотите настроить отправку уведомлений.

   Вы можете ввести несколько адресов электронной почты через запятую.
5. В поле **Тема** введите тему сообщения с уведомлением.
6. Если вы хотите, чтобы приложение подставляло важность обнаружения в тему сообщения, добавьте в поле **Тема** макрос `%importance%`.
7. В поле **Тип уведомления** выберите **Обнаружения**.
8. В раскрывающемся списке **Важность обнаружения** выберите минимальное значение важности обнаружений, о которых вы хотите настроить отправку уведомлений.

   Например, вы можете настроить отправку уведомлений об обнаружениях только высокой степени важности или только средней и высокой степени важности.
9. В поле **Адрес источника или назначения** введите IP-адрес и маску сети, если вы хотите настроить отправку уведомлений об обнаружениях, связанных с определенным IP-адресом или адресом подсети источника или назначения.
10. В поле **Email** введите адрес электронной почты, если вы хотите настроить отправку уведомлений об обнаружениях, связанных с определенным адресом отправителя или получателя сообщений электронной почты.
11. В блоке параметров **Компоненты** установите флажки рядом с названиями одной или нескольких технологий, если вы хотите настроить отправку уведомлений об обнаружениях, выполненных определенными технологиями.
12. Нажмите на кнопку **Добавить**.

Правило для отправки уведомлений об обнаружениях будет добавлено в список правил. Чтобы уведомления приходили на указанный адрес электронной почты, требуется включить правило отправки уведомлений (см. раздел "Включение и отключение правила для отправки уведомлений" на стр. 600). Уведомления отправляются однократно по всем указанным в правиле адресам электронной почты.

Для пользователей с ролью **Администратор** и **Аудитор** функция создания правил для отправки уведомлений об обнаружениях недоступна.

В режиме распределенного решения (см. раздел "Распределенное решение и мультитенантность" на стр. 75) уведомления требуется создать отдельно для каждого подчиненного сервера (*Secondary Central Node*, *SCN*).

Создание правила для отправки уведомлений о работе компонентов приложения

► *Чтобы создать правило для отправки уведомлений о работе компонентов приложения:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. Нажмите на кнопку **Добавить**.

   Откроется окно **Новое правило**.
4. В поле **Кому** введите один или несколько адресов электронной почты, на которые вы хотите настроить отправку уведомлений.

   Вы можете ввести несколько адресов электронной почты через запятую.
5. В поле **Тема** введите тему сообщения с уведомлением.
6. Если вы хотите, чтобы приложение указывало важность обнаружения в теме сообщения, добавьте в поле **Тема** макрос `%importance%`.
7. В поле **Тип уведомления** выберите **Работа приложения**.
8. В блоке параметров **Компоненты** установите флажки рядом с названиями тех функциональных областей приложения, о которых вы хотите получать уведомления.
9. Нажмите на кнопку **Добавить**.

Правило для отправки уведомлений о работе компонентов приложения будет добавлено в список правил. Чтобы уведомления приходили на указанный адрес электронной почты, требуется включить правило отправки уведомлений (см. раздел "Включение и отключение правила для отправки уведомлений" на стр. 600). Уведомления отправляются однократно по всем указанным в правиле адресам электронной почты.

Для пользователей с ролью **Аудитор** функция создания правил для отправки уведомлений о работе приложения недоступна.
В режиме распределенного решения (см. раздел "Распределенное решение и мультитенантность" на стр. 75) уведомления настраиваются отдельно для каждого подчиненного сервера (*Secondary Central Node*, *SCN*).

Включение и отключение правила для отправки уведомлений

► *Чтобы включить или отключить правило для отправки уведомлений об обнаружениях:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. В столбце **Состояние** включите или отключите правило для отправки уведомлений с помощью переключателя рядом с этим правилом.

Состояние правила для отправки уведомлений об обнаружениях будет изменено.

Для пользователей с ролью **Аудитор** функция включения и отключения правил для отправки уведомлений недоступна.

Изменение правила для отправки уведомлений

► *Чтобы изменить правило для отправки уведомлений:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. В списке правил для отправки уведомлений выберите правило, которое вы хотите изменить.

   Откроется окно **Изменить правило**.
4. Внесите необходимые изменения.
5. Нажмите на кнопку **Сохранить**.

Правило для отправки уведомлений будет изменено.

Для пользователей с ролью **Аудитор** функция изменения правил для отправки уведомлений недоступна.

Удаление правила для отправки уведомлений

► *Чтобы удалить правило для отправки уведомлений:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. Установите флажок слева от названия каждого правила, которое вы хотите удалить.

   Если вы хотите удалить все правила, установите флажок над списком.

4. Нажмите на кнопку **Удалить** в нижней части окна.
5. В окне подтверждения нажмите на кнопку **Да**.

Выбранные правила будут удалены.

Для пользователей с ролью **Аудитор** функция удаления правил для отправки уведомлений недоступна.

Фильтрация и поиск правил отправки уведомлений по типу правила

► *Чтобы отфильтровать или найти правила отправки уведомлений по типу правила:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. В таблице правил для отправки уведомлений нажмите на значок .

   Откроется окно настройки фильтрации.
4. Выберите один из следующих вариантов:
   - **Все**.
   - **Обнаружения**.
   - **Работа приложения**.

В таблице правил отправки уведомлений отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск правил отправки уведомлений по теме уведомлений

► *Чтобы отфильтровать или найти правила отправки уведомлений по теме уведомлений:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. По ссылке **Тема** откройте окно настройки фильтрации.
4. Введите один или несколько символов темы уведомлений.
5. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице правил отправки уведомлений отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск правил отправки уведомлений по адресу электронной почты

► *Чтобы отфильтровать или найти правила отправки уведомлений по адресу электронной почты, на который они отправляются:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. По ссылке **Кому** откройте окно настройки фильтрации.
4. Введите один или несколько символов адреса электронной почты.
5. Нажмите на кнопку **Применить**.

В таблице правил отправки уведомлений отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск правил отправки уведомлений по их состоянию

► *Чтобы отфильтровать или найти правила отправки уведомлений по их состоянию:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. По ссылке **Состояние** откройте окно настройки фильтрации.
4. Установите один или несколько флажков рядом со значениями состояний:
   - **Включено**.
   - **Выключено**.
5. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице правил отправки уведомлений отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра правил отправки уведомлений

► *Чтобы сбросить фильтр правил отправки уведомлений по одному или нескольким условиям фильтрации:*

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. Нажмите на кнопку ☒ справа от того заголовка столбца таблицы правил отправки уведомлений, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице правил отправки уведомлений отобразятся только правила, соответствующие заданным вами условиям.

Управление приложением Kaspersky Endpoint Agent для Windows

Kaspersky Endpoint Agent – приложение, которое устанавливается на отдельные устройства, входящие в IT-инфраструктуру организации. Приложение осуществляет постоянное наблюдение за процессами, запущенными на этих устройствах, открытыми сетевыми соединениями и изменяемыми файлами.

Kaspersky Endpoint Agent обеспечивает взаимодействие защищаемого устройства с другими решениями "Лаборатории Касперского" для обнаружения комплексных угроз, таких как таргетированные атаки.

При настроенной интеграции Kaspersky Endpoint Agent с Kaspersky Anti Targeted Attack Platform приложение выполняет задачи и применяет параметры, поступающие от Kaspersky Anti Targeted Attack Platform, а также отправляет на сервер с компонентом Central Node данные телеметрии с защищаемого устройства. Подробнее о действиях, которые может выполнять Kaspersky Endpoint Agent при интеграции с Kaspersky Anti Targeted Attack Platform, см. в разделе *Принцип работы приложения* (на стр. 69).

Подробнее об управлении Kaspersky Endpoint Agent см. в справке приложения:

- Активация приложения.
- Установка и удаление приложения.

  Перед установкой приложения требуется выключить использование TLS 1.0 и TLS 1.1 в операционной системе. О том, как это сделать, читайте в статье https://learn.microsoft.com/ru-ru/windows-server/security/tls/tls-registry-settings?tabs=diffie-hellman#tls-dtls-and-ssl-protocol-version-settings.

- Управление параметрами Kaspersky Endpoint Agent в Консоли администрирования Kaspersky Security Center и с помощью Kaspersky Security Center Web Console:
  - Управление политиками.
  - Управление задачами.
  - Открытие окна параметров.
  - Настройка параметров безопасности.
  - Настройка параметров соединения Kaspersky Endpoint Agent с прокси-сервером.
  - Настройка Kaspersky Security Center в качестве прокси-сервера для активации Kaspersky Endpoint Agent.
  - Настройка использования KSN в Kaspersky Endpoint Agent.
  - Настройка параметров хранилищ в Kaspersky Endpoint Agent.
  - Настройка диагностики сбоев.
- Управление Kaspersky Endpoint Agent через интерфейс командной строки:
  - Управление активацией.
  - Управление аутентификацией.

- Настройка трассировки.
- Настройка создания дампа процессов Kaspersky Endpoint Agent.
- Просмотр информации о параметрах карантина и объектах на карантине.
- Действия над объектами на карантине.
- Запуск обновления баз или модулей Kaspersky Endpoint Agent.
- Запуск, остановка и просмотр текущего состояния приложения.
- Защита приложения паролем.
- Защита служб приложения технологией PPL.
- Управление параметрами самозащиты.
- Управление стандартными задачами поиска IOC.
- Управление сканированием файлов и процессов по YARA-правилам.
- Создание дампа памяти.
- Создание дампа диска.

Управление приложением Kaspersky Endpoint Security для Windows

Kaspersky Endpoint Security – приложение, которое устанавливается на отдельные устройства, входящие в IT-инфраструктуру организации. Приложение осуществляет постоянное наблюдение за процессами, запущенными на этих устройствах, открытыми сетевыми соединениями и изменяемыми файлами. Данные о событиях на компьютере (телеметрия) отправляются на сервер Kaspersky Anti Targeted Attack Platform. Приложение Kaspersky Endpoint Security также передает на сервер Kaspersky Anti Targeted Attack Platform данные об угрозах, обнаруженных приложением, и данные о результатах обработки этих угроз.

При настроенной интеграции Kaspersky Endpoint Security с Kaspersky Anti Targeted Attack Platform приложение выполняет задачи и применяет параметры, поступающие от Kaspersky Anti Targeted Attack Platform, а также отправляет на сервер с компонентом Central Node данные телеметрии с защищаемого устройства. Подробнее о действиях, которые может выполнять Kaspersky Endpoint Security при интеграции с Kaspersky Anti Targeted Attack Platform, см. в разделе *Принцип работы приложения* (на стр. 69).

Подробнее об управлении Kaspersky Endpoint Security см. в справке приложения следующие разделы:

- Установка и удаление приложения.
- Лицензирование приложения.

  Для интеграции с Kaspersky Anti Targeted Attack Platform, кроме ключа активации Kaspersky Endpoint Security, вам нужно также нужно добавить ключ Kaspersky Endpoint Detection and Response (KATA) Add-on. Подробнее о лицензировании приложения см. в справке Kaspersky Endpoint Security → Интеграция с EDR (KATA).
- Интеграция с EDR (KATA).
- Настройка отправки телеметрии.
- Работа с карантином.
- Команды управления Detection and Response KATAEDR: Интеграция с EDR (KATA).

Управление приложением Kaspersky Endpoint Security для Linux

Kaspersky Endpoint Security для Linux – приложение, которое устанавливается на отдельные устройства под управлением операционных систем Linux, входящие в IT-инфраструктуру организации. Приложение осуществляет постоянное наблюдение за процессами, запущенными на этих устройствах, открытыми сетевыми соединениями и изменяемыми файлами. Данные о событиях на компьютере (телеметрия) отправляются на сервер Kaspersky Anti Targeted Attack Platform. Приложение Kaspersky Endpoint Security для Linux также передает на сервер Kaspersky Anti Targeted Attack Platform данные об угрозах, обнаруженных приложением, и данные о результатах обработки этих угроз.

При настроенной интеграции Kaspersky Endpoint Security с Kaspersky Anti Targeted Attack Platform приложение выполняет задачи и применяет параметры, поступающие от Kaspersky Anti Targeted Attack Platform, а также отправляет на сервер с компонентом Central Node данные телеметрии с защищаемого устройства. Подробнее о действиях, которые может выполнять Kaspersky Endpoint Security при интеграции с Kaspersky Anti Targeted Attack Platform, см. в разделе *Принцип работы приложения* (на стр. 69).

Подробнее об управлении Kaspersky Endpoint Security для Linux см. в справке приложения.

Для интеграции с Kaspersky Anti Targeted Attack Platform вам не требуется добавлять дополнительный лицензионный ключ в Kaspersky Endpoint Security для Linux.

Управление приложением Kaspersky Endpoint Security для Mac

Kaspersky Endpoint Security для Mac – приложение, которое устанавливается на отдельные устройства под управлением операционных систем macOS, входящие в IT-инфраструктуру организации. Приложение осуществляет постоянное наблюдение за процессами, запущенными на этих устройствах, открытыми сетевыми соединениями и изменяемыми файлами. Данные о событиях на компьютере (телеметрия) отправляются на сервер Kaspersky Anti Targeted Attack Platform. Приложение Kaspersky Endpoint Security для Mac также передает на сервер Kaspersky Anti Targeted Attack Platform данные об угрозах, обнаруженных приложением, и данные о результатах обработки этих угроз.

При настроенной интеграции Kaspersky Endpoint Security для Mac с Kaspersky Anti Targeted Attack Platform приложение выполняет задачи и применяет параметры, поступающие от Kaspersky Anti Targeted Attack Platform, а также отправляет на сервер с компонентом Central Node данные телеметрии с защищаемого устройства. Подробнее о действиях, которые может выполнять Kaspersky Endpoint Security для Mac при интеграции с Kaspersky Anti Targeted Attack Platform, см. в разделе *Принцип работы приложения* (на стр. 69).

Подробнее об управлении Kaspersky Endpoint Security для Mac см. в справке приложения.

Создание резервной копии и восстановление приложения

Вы можете создать резервную копию приложения, а затем восстановить его из резервной копии.

Для отдельного сервера Central Node вы можете создать резервную копию данных этого сервера Central Node.

Если вы используете режим распределенного решения и мультитенантности, вы можете:

- Создать резервную копию данных PCN.
- Создать резервную копию данных SCN.

  При восстановлении данных из резервной копии SCN роль сервера изменится с SCN на отдельный сервер Central Node.

Выполняйте действия по созданию резервной копии приложения на том сервере, резервную копию данных которого вы хотите создать.

В Kaspersky Anti Targeted Attack Platform могут содержаться данные пользователей и другая конфиденциальная информация. Администратору Kaspersky Anti Targeted Attack Platform нужно обеспечить безопасность этих данных самостоятельно при создании резервной копии приложения, замене оборудования, на которое установлено приложение, и в прочих случаях, когда может потребоваться удаление данных без возможности восстановления. Администратор Kaspersky Anti Targeted Attack Platform несет ответственность за доступ к данным, хранящимся на серверах приложения.

Вы можете создать резервную копию следующих данных:

- Базы данных приложения.
- Объектов в Хранилище.
- Файлов из обнаружений, выполненных при повторной проверке (rescan).
- Артефактов Sandbox.
- Конфигурационных файлов.
- Параметров Central Node или PCN:
  - Если вы используете отдельный сервер Central Node, создается резервная копия параметров Central Node.
  - Если вы используете режим распределенного решения и мультитенантности и работаете на сервере PCN, создается резервная копия параметров PCN.
  - Если вы используете режим распределенного решения и мультитенантности и работаете на сервере SCN, вы можете создать резервную копию SCN, но при восстановлении данных из резервной копии роль сервера изменится с SCN на отдельный сервер Central Node.

Вы можете очистить директорию перед созданием резервной копии приложения.

Перед восстановлением приложения из резервной копии на сервере Central Node или PCN, на котором вы выполняете восстановление приложения, происходит очистка:

- Базы данных приложения.
- Объектов в Хранилище.
- Файлов из обнаружений, выполненных при повторной проверке (rescan).
- Артефактов Sandbox.
- Конфигурационных файлов.
- Параметров Central Node или PCN.

Таблица 43. Состав и объем данных, экспортируемых для создания резервной копии приложения

Тип данных	Экспортируемые данные	Режим работы с приложением	Способ развертывания

• Параметры Central Node.
• Базы данных приложения на Central Node:
  • обнаружения и наличие у обнаружений статуса VIP;
  • задачи и результаты их выполнения;
  • политики;
  • пользовательские правила TAA (IOA) и исключения;
  • пользовательские правила IDS и исключения;
  • IOC-файлы;
  • правила исключений из проверки;
  • информация о файлах в Хранилище;
  • информация об объектах на карантине;
  • список компьютеров с Endpoint Agent;
  • отчеты и шаблоны отчетов;
  • данные учетных записей пользователей;
  • уведомления.
	Параметры Central Node – по выбору.
	Базы данных приложения – по умолчанию.
		Отдельный сервер Central Node.	Все способы развертывания.

Параметры PCN.	По выбору.	Режим распределенного решения и мультитенантности.	Все способы развертывания.
Параметры SCN.	По выбору. Как для отдельного сервера Central Node.	Режим распределенного решения и мультитенантности.	Все способы развертывания.

Тип данных	Экспортируемые данные	Режим работы с приложением	Способ развертывания
Базы данных приложения на PCN: • обнаружения и наличие у обнаружений статуса VIP; • результаты выполнения задач; • политики; • пользовательские правила TAA (IOA) и исключения; • пользовательские правила IDS и исключения; • IOC-файлы; • список данных, исключенных из проверки; • информация о файлах в Хранилище; • информация об объектах на карантине; • список хостов Kaspersky Endpoint Agent; • отчеты и шаблоны отчетов; • данные учетных записей пользователей; • уведомления.	По умолчанию.	Режим распределенного решения и мультитенантности.	Все способы развертывания.
Конфигурационные файлы.	Да	Все режимы.	Все способы развертывания.
Хранилище.	По выбору.	Все режимы.	Все способы развертывания.
Артефакты Sandbox.	По выбору.	Все режимы.	Неотказоустойчивая версия.
Файлы из обнаружений, выполненных при повторной проверке (rescan).	По выбору.	Все режимы.	Неотказоустойчивая версия.
База событий.	Нет.	Все режимы.	Неотказоустойчивая версия.

Файлы, которые в момент создания резервной копии приложения находились в очереди на проверку, не экспортируются.

Версии восстанавливаемой и установленной на сервер приложений должны совпадать. Если версии приложений не совпадают, при запуске восстановления приложения отобразится сообщение об ошибке и процесс восстановления будет прерван.

В этом разделе

Создание резервной копии параметров сервера Central Node из меню администратора приложения612

Загрузка файла с резервной копией параметров сервера с сервера Central Node или PCN на жесткий диск компьютера.....612

Загрузка файла с резервной копией параметров сервера с вашего компьютера на сервер Central Node 613

Восстановление параметров сервера из резервной копии через меню администратора приложения613

Создание резервной копии приложения в режиме Technical Support Mode 615

Восстановление приложения из резервной копии в режиме Technical Support Mode 616

Создание резервной копии параметров сервера Central Node из меню администратора приложения

► *Чтобы создать резервную копию параметров Central Node (PCN или SCN в режиме распределенного решения и мультитенантности), выполните следующие действия в меню администратора (см. раздел "Начало работы в меню администратора приложения" на стр. 188) сервера:*

1. В списке разделов меню администратора приложения выберите раздел **System administration**.
2. Нажмите на клавишу **ENTER**.

   Откроется окно выбора действий.
3. В списке действий выберите **Backup/Restore settings**.
4. Нажмите на клавишу **ENTER**.

   Откроется окно **Backup/Restore settings**.
5. В списке действий выберите **New**.
6. Нажмите на клавишу **ENTER**.

   Откроется окно **Backup settings**.
7. Нажмите на кнопку **Back up**.

Резервная копия параметров сервера будет создана.

Резервная копия Kaspersky Anti Targeted Attack Platform будет содержать только базы данных (базу обнаружений, сведения о статусе VIP, список данных, исключенных из проверки, уведомления) и параметры Central Node или PCN.

Загрузка файла с резервной копией параметров сервера с сервера Central Node или PCN на жесткий диск компьютера

Рекомендуется сохранять файлы с резервной копией параметров сервера Central Node на жесткий диск вашего компьютера.

► *Чтобы загрузить файл с резервной копией параметров сервера Central Node на жесткий диск вашего компьютера, выполните команду в интерфейсе командной строки операционной системы Linux на вашем компьютере:*

```
scp <имя учетной записи для работы в меню администратора и в консоли
управления сервером>@<IP-адрес сервера>:<имя файла с резервной копией
приложения вида settings-<дата и время создания резервной копии>.tar.gz>
```

Пример:

Команда для загрузки на жесткий диск вашего компьютера архива с резервной копией параметров сервера, созданной на сервере Central Node с IP-адресом 10.0.0.10 под учетной записью admin 10 апреля 2020 года в 10 часов 00 минут 00 секунд:

```
scp admin@10.0.0.10:settings-20200410-100000.tar.gz
```

Файл с резервной копией параметров сервера будет сохранен на жесткий диск вашего компьютера в текущую директорию.

Загрузка файла с резервной копией параметров сервера с вашего компьютера на сервер Central Node

► *Чтобы загрузить файл с резервной копией параметров сервера Central Node с жесткого диска вашего компьютера на сервер, выполните следующую команду в режиме Technical Support Mode:*

```
scp <имя файла с резервной копией параметров сервера вида settings-<дата и
время создания резервной копии>.tar.gz> <имя учетной записи для работы в
меню администратора и в консоли управления сервером>@<IP-адрес сервера>:
```

Пример:

Команда для загрузки архива с резервной копией параметров сервера, созданной 10 апреля 2020 года в 10 часов 00 минут 00 секунд, на сервер Central Node с IP-адресом 10.0.0.10 под учетной записью admin:

```
scp settings-20200410-100000.tar.gz admin@10.0.0.10:
```

Файл с резервной копией параметров сервера будет загружен на сервер Central Node в текущую директорию.

Восстановление параметров сервера из резервной копии через меню администратора приложения

Для восстановления параметров сервера Central Node из резервной копии нужно предварительно создать резервную копию текущих параметров сервера (см. раздел "Создание резервной копии параметров сервера Central Node из меню администратора приложения" на стр. 612). В случае сбоя при восстановлении параметров сервера вы сможете воспользоваться сохраненной копией параметров сервера.

► *Чтобы восстановить параметры сервера из уже созданной ранее резервной копии, выполните следующие действия в меню администратора (см. раздел "Начало работы в меню администратора приложения" на стр. 188) сервера:*

1. В списке разделов меню администратора приложения выберите раздел **System administration**.
2. Нажмите на клавишу **ENTER**.

   Откроется окно выбора действий.
3. В списке действий выберите **Backup/Restore settings**.
4. Нажмите на клавишу **ENTER**.

   Откроется окно **Backup/Restore settings**.
5. В списке файлов с резервными копиями приложения выберите файл, из которого вы хотите восстановить параметры сервера.

   Если нужного файла нет в списке, вам нужно загрузить файл с резервной копией параметров на сервер.
6. Нажмите на клавишу **ENTER**.

   Откроется окно выбора действий.
7. В списке действий выберите **Restore <имя файла с резервной копией параметров сервера>**.
8. Нажмите на клавишу **ENTER**.

   Откроется окно подтверждения действия.
9. Нажмите на кнопку **Restore**.

   Начнется процесс восстановления параметров сервера из резервной копии.
10. При отображении запроса на ввод пароля, введите пароль администратора сервера, на котором была создана резервная копия параметров сервера.
11. Нажмите на клавишу **ENTER**.
12. Введите пароль администратора сервера, на котором выполняется восстановление параметров сервера из резервной копии.
13. Нажмите на клавишу **ENTER**.

Параметры сервера будут восстановлены из выбранного файла.

Резервная копия параметров сервера не содержит настроек получения зеркалированного трафика со SPAN-портов. Если вы раннее произвели настройку и хотите получать зеркалированный трафик со SPAN-портов вам необходимо перед восстановлением параметров сервера настроить получение зеркалированного трафика (см. раздел "Настройка получения зеркалированного трафика со SPAN-портов" на стр. 263) и во время обновления приложения на шаге Настройка получения зеркалированного трафика со SPAN-портов (см. раздел "Шаг 10. Настройка получения зеркалированного трафика со SPAN-портов" на стр. 141) включить получение зеркалированного трафика со SPAN-портов.
Kaspersky Anti Targeted Attack Platform не содержит в резервной копии параметров ICAP-исключений. Если вам необходимо сохранить и восстановить параметры ICAP-исключений, до восстановления параметров сервера обратитесь в Службу технической поддержки (см. раздел "Обращение в Службу технической поддержки" на стр. 670).

Если аппаратная конфигурация сервера Central Node, на котором была создана резервная копия, отличается от аппаратной конфигурации сервера, на котором вы планируете восстановить параметры сервера, после восстановления вам нужно заново настроить параметры масштабирования приложения.

Создание резервной копии приложения в режиме Technical Support Mode

► *Чтобы создать резервную копию Kaspersky Anti Targeted Attack Platform, выполните следующую команду в режиме Technical Support Mode (см. раздел "Начало работы с приложением в режиме Technical Support Mode" на стр. 189) сервера:*

```
kata-run.sh kata-backup-restore backup
```

Вы также можете указать один или несколько параметров к этой команде (см. таблицу ниже).

Подсказка по использованию параметров доступна по команде `-h`.

Таблица 44. Параметры команды для создания резервной копии Kaspersky Anti Targeted Attack Platform

Обязательный параметр	Параметр	Описание
Да	`-b <path>`	Создать файл с резервной копией приложения по указанному пути, где <path> – абсолютный или относительный путь к директории, в которой создается файл с резервной копией приложения.
Нет	`-c`	Очистить директорию перед сохранением файла с резервной копией приложения.
Нет	`-d <number of stored files>`	Указать максимальное количество файлов с резервной копией приложения, хранимых в директории, где <number> – количество файлов.
Нет	`-e`	Сохранить файлы в Хранилище.
Нет	`-q`	Сохранить файлы на карантине.
Нет	`-a`	Сохранить файлы, ожидающие повторной проверки (rescan).
Нет	`-s`	Сохранить артефакты Sandbox.
Нет	`-n`	Сохранить параметры Central Node или PCN.
Нет	`-l <filepath>`	Сохранить результат выполнения команды в файл, где <filepath> – имя файла журнала событий, включая абсолютный или относительный путь к файлу.

Если дополнительные параметры не указаны, резервная копия Kaspersky Anti Targeted Attack Platform будет содержать только базы данных (базу обнаружений, сведения о статусе VIP, список данных, исключенных из проверки, уведомления). Если вы создаете резервную копию приложения, установленного в виде отказоустойчивого кластера, вы не можете использовать параметры -q, -a, -s, -e.

Если вы используете приложение, установленное в виде отказоустойчивого кластера, вы можете создать резервную копию параметров и выполнить восстановление из резервной копии только серверов с ролью manager в Docker swarm.

Все файлы с резервной копией приложения сохраняются в один TAR-архив. Имя файла архива: data_kata_ddmmyyyyhhMM, где ddmmyyyy – дата, hhMM – часы и минуты создания резервной копии приложения. Имя базы данных резервной копии приложения – KATA6.0.sql для резервной копии приложения версии 6.0.

Пример:

Команда для создания резервной копии приложения:

```
kata-run.sh kata-backup-restore backup -b <path> -c -d <number of stored
files> -e -q -a -s -n -l <filepath>
```

Восстановление приложения из резервной копии в режиме Technical Support Mode

Для восстановления Kaspersky Anti Targeted Attack Platform из резервной копии нужно предварительно создать резервную копию текущего состояния приложения (см. раздел "Создание резервной копии параметров сервера Central Node из меню администратора приложения" на стр. 612) и загрузить ее на жесткий диск вашего компьютера (см. раздел "Загрузка файла с резервной копией параметров сервера с сервера Central Node или PCN на жесткий диск компьютера" на стр. 612). В случае сбоя при восстановлении приложения или при необходимости переустановить Kaspersky Anti Targeted Attack Platform вы сможете воспользоваться сохраненной копией приложения.
Версии восстанавливаемой и установленной на сервер приложений должны совпадать. Если версии приложений не совпадают, при запуске восстановления приложения отобразится сообщение об ошибке и процесс восстановления будет прерван.

► *Чтобы восстановить Kaspersky Anti Targeted Attack Platform из резервной копии, выполните следующую команду в режиме Technical Support Mode (см. раздел "Начало работы с приложением в режиме Technical Support Mode" на стр. 189) сервера:*

```
kata-run.sh kata-backup-restore restore
```

Вы также можете указать один или несколько параметров к этой команде (см. таблицу ниже).

Подсказка по использованию параметров доступна по команде `-h`.

Таблица 45. Параметры команды для восстановления Kaspersky Anti Targeted Attack Platform из резервной копии

Обязательный параметр	Параметр	Описание команды
Да	`-r <path>`	Восстановить данные из файла с резервной копией приложения, где <path> – полный путь к файлу с резервной копией приложения.
Нет	`-l <filepath>`	Сохранить результат выполнения команды в файл, где <filepath> – имя файла журнала событий, включая абсолютный или относительный путь к файлу.

Пример:

Команда для восстановления приложения из резервной копии:

```
kata-run.sh kata-backup-restore restore -r <path> -l <filepath>
```

Взаимодействие с внешними системами по API

Вы можете настроить интеграцию Kaspersky Anti Targeted Attack Platform с внешними системами (см. раздел "Интеграция внешней системы с Kaspersky Anti Targeted Attack Platform" на стр. 619), чтобы управлять действиями по реагированию на угрозы (см. раздел "API для управления действиями по реагированию на угрозы" на стр. 645), а также для проверки хранящихся в них файлов (см. раздел "API для проверки объектов внешних систем" на стр. 619) и предоставления внешним системам доступа к информации обо всех обнаружениях (см. раздел "API для получения внешними системами информации об обнаружениях приложения" на стр. 625) и событиях (см. раздел "API для получения внешними системами информации о событиях приложения" на стр. 633) приложения.

Взаимодействие внешних систем с Kaspersky Anti Targeted Attack Platform осуществляется с помощью интерфейса API. Вызовы методов API доступны только для авторизованных внешних систем. Для авторизации администратору приложения необходимо создать запрос на интеграцию внешней системы с приложением (см. раздел "Интеграция внешней системы с Kaspersky Anti Targeted Attack Platform" на стр. 619). После этого администратор должен обработать запрос в веб-интерфейсе Kaspersky Anti Targeted Attack Platform (см. раздел "Обработка запроса от внешней системы" на стр. 301).

Если вы развернули компоненты Central Node и Sensor в виде кластера (см. раздел "Установка и первоначальная настройка приложения" на стр. 110), вы можете настроить отказоустойчивую интеграцию с внешней системой одним из следующих способов:

- Использовать функцию Round Robin.
- Настроить параметры внешней системы таким образом, чтобы при возникновении таймаута внешняя система переключалась между IP-адресами серверов кластера.

► *Чтобы настроить отказоустойчивую интеграцию с внешней системой с помощью функции Round Robin:*

1. Настройте на сервере DNS функцию Round Robin для доменного имени, соответствующего кластеру Central Node.
2. В параметрах почтового сервера укажите это доменное имя.

Интеграция с почтовым сервером будет настроена по доменному имени. Почтовый сервер обратится к случайному серверу кластера. При отказе этого сервера почтовый сервер будет обращаться к другому работоспособному серверу кластера.

В этом разделе

Интеграция внешней системы с Kaspersky Anti Targeted Attack Platform 619

API для проверки объектов внешних систем 619

API для получения внешними системами информации об обнаружениях приложения 625

API для получения внешними системами информации о событиях приложения 633

API для управления действиями по реагированию на угрозы 645

Интеграция внешней системы с Kaspersky Anti Targeted Attack Platform

Для начала работы с API необходимо выполнить интеграцию внешней системы с Kaspersky Anti Targeted Attack Platform. Внешняя система должна пройти авторизацию на сервере Kaspersky Anti Targeted Attack Platform.

► *Чтобы выполнить интеграцию внешней системы с Kaspersky Anti Targeted Attack Platform:*

1. Сгенерируйте уникальный идентификатор внешней системы для авторизации в Kaspersky Anti Targeted Attack Platform – `sensorId`.
2. Сгенерируйте сертификат сервера внешней системы.
3. Создайте любой запрос от внешней системы в Kaspersky Anti Targeted Attack Platform, содержащий идентификатор `sensorId`. Например, вы можете создать запрос на проверку объекта из внешней системы в Kaspersky Anti Targeted Attack Platform (см. раздел "Запрос на проверку объектов" на стр. 620).

В веб-интерфейсе Kaspersky Anti Targeted Attack Platform отобразится запрос на авторизацию от внешней системы. Обратитесь к администратору приложения для обработки запроса (см. раздел "Обработка запроса от внешней системы" на стр. 301).

Если вам нужно сменить сертификат сервера внешней системы, выполните действия по интеграции внешней системы в Kaspersky Anti Targeted Attack Platform повторно.

API для проверки объектов внешних систем

Kaspersky Anti Targeted Attack Platform предоставляет HTTPS REST интерфейс проверки объектов, хранящихся во внешних системах.

Для проверки объектов, хранящихся во внешних системах, рекомендуется использовать следующий сценарий взаимодействия с Kaspersky Anti Targeted Attack Platform:

a. **Создание запроса на проверку объектов HTTP-методом `POST` (см. раздел "`Запрос на проверку объектов`" на стр. 620)**

b. **Создание запроса на получение результатов проверки HTTP-методом `GET` (см. раздел "`Запрос на получение результатов проверки`" на стр. 621)**

   Интерфейс API является асинхронным, то есть Kaspersky Anti Targeted Attack Platform выполняет проверку объектов не в момент обращения внешней системы, а в фоновом режиме. Поэтому для получения результатов проверки требуется периодически отправлять запрос от внешней системы HTTP-методом `GET`. Рекомендуемая периодичность отправки запроса 1 раз в минуту.

   Вы также можете настроить отправку уведомлений об обнаруженных объектах в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.

c. **Создание запроса на удаление результатов проверки HTTP-методом `DELETE` (см. раздел "`Запрос на удаление результатов проверки`" на стр. 623)**

   Вы можете удалить результаты проверки указанного объекта или всех объектов.

Работа с кластером

Если внешняя система представляет собой несколько серверов, объединенных в кластер, рекомендуется использовать один идентификатор (`sensorId`) для всех серверов. В этом случае в веб-интерфейсе Kaspersky Anti Targeted Attack Platform будет отображаться один запрос на интеграцию для всей системы (см. раздел "Обработка запроса от внешней системы" на стр. 301). При необходимости разграничить получение результатов проверки по отдельным серверам вы можете назначить каждому серверу уникальный идентификатор экземпляра (`sensorInstanceId`).

Ограничения

В конфигурационном файле Kaspersky Anti Targeted Attack Platform установлены максимально допустимое количество запросов на проверку объектов от внешних систем и максимально допустимый размер проверяемого объекта.

Если превышено максимально допустимое количество одновременных запросов на проверку объектов, Kaspersky Anti Targeted Attack Platform перестает обрабатывать дальнейшие запросы до тех пор, пока количество запросов на проверку объектов не станет меньше максимально допустимого. До этого времени выдается код возврата 429. Необходимо повторить запрос на проверку позже.

Если превышен максимально допустимый размер объекта, Kaspersky Anti Targeted Attack Platform не проверяет этот объект. При создании запроса HTTP-методом `POST` выдается код возврата 413. Вы можете узнать максимально допустимый размер объекта, просмотрев список ограничений приложения на проверку объектов с помощью метода `GET` (см. раздел "`Запрос на вывод ограничений приложения на проверку объектов`" на стр. 624).

Запрос на проверку объектов

Для создания запроса на проверку объектов используется HTTP-метод `POST`. Создать запрос можно, например, с помощью утилиты командной строки cURL.

Вы можете задавать параметры выполнения команды cURL с помощью дополнительных ключей (см. таблицу ниже).

Подробную информацию о ключах команд cURL см. в документации cURL.

Синтаксис команды

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого
ключа> -X POST "<URL-адрес сервера с компонентом Central Node>:<порт, по
умолчанию 443>/kata/scanner/v1/sensors/<идентификатор
sensorId>/scans?sensorInstanceId=<идентификатор sensorInstanceId>" -F
"content=<путь к файлу, который вы хотите проверить>" -F
scanId=<идентификатор запроса на проверку> -F "objectType=file"
```

При успешной обработке запроса отобразится статус `"OK"`.

Параметры

Параметр	Тип	Описание
sensorId	string	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
content	file	Содержимое проверяемого объекта.
scanId	string	Уникальный идентификатор запроса на проверку. Должен быть сформирован на стороне внешней системы. Не может содержать пробелы и специальные символы. Не используйте имена файлов в качестве идентификатора запроса на проверку. Если этот параметр не указан, просмотр результатов проверки недоступен.
objectType	string	Тип проверяемого объекта. Возможное значения параметра: file.
sensorInstanceId	string	Уникальный идентификатор экземпляра внешней системы. Экземплярами внешней системы считаются также серверы, объединенные в кластер. Параметр не является обязательным.

Возвращаемое значение

Код возврата	Описание
200	Проверка выполнена успешно.
401	Требуется авторизация.
429	Превышено количество запросов. Повторите запрос позднее.
500	Внутренняя ошибка сервера. Повторите запрос позднее.

Пример ввода команды с параметрами

```
curl --cert /root/cert.pem --key /root/server.key -
X POST "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-
111c-b11a-11001b1f1111/scans?sensorInstanceId=instance1" -
F "content=@/tmp/test" -F scanId=1 -F "objectType=file"
```

Запрос на получение результатов проверки

Для создания запроса на получение результатов проверки используется HTTP-метод GET. Создать запрос можно, например, с помощью утилиты командной строки cURL.

Вы можете задавать параметры выполнения команды cURL с помощью дополнительных ключей (см. таблицу ниже).

Подробную информацию о ключах команд cURL см. в документации cURL.

Синтаксис команды

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого
ключа> -X GET<URL-адрес сервера с компонентом Central Node>:<порт, по
умолчанию 443>/kata/scanner/v1/sensors/<идентификатор
sensorId>/scans/state?sensorInstanceId=<идентификатор
sensorInstanceId>&state=<один или несколько статусов проверки, которые вы
хотите отобразить в результатах проверки>"
```

При успешной отправке запроса отобразится список запросов на проверку объектов (см. раздел "Запрос на проверку объектов" на стр. 620) и результаты проверки этих объектов. Результаты проверки будут отфильтрованы по статусам, которые вы указали в параметре `state`. Например, если в запросе на получение результатов проверки вы указали статусы `state=processing,detect`, отобразятся только запросы на проверку объектов, которые находятся в обработке или в которых приложение обнаружило угрозу.

Параметры

Параметр	Тип	Описание
`sensorId`	string	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
`state`	array (тип элементов string)	Статус проверки объекта. При указании этого параметра результаты проверки будут отфильтрованы по статусу. Указывайте один или несколько статусов через запятую. Возможны следующие значения параметра: • `detect`; • `not detected`; • `processing`; • `timeout`; • `error`.
`sensorInstanceId`	string	Уникальный идентификатор экземпляра внешней системы. Экземплярами внешней системы считаются также серверы, объединенные в кластер. Параметр не является обязательным.

Ответ

HTTP-код: 200

Формат: JSON

```
type Response []Scans


type Scans struct {
   ScanID  integer `json:"scanId"`
   State   array   `json:"state"`
}
```

Возвращаемое значение

Код возврата	Описание
204	Нет содержимого.
404	Не найдены результаты проверки по указанному идентификатору.
500	Внутренняя ошибка сервера. Повторите запрос позднее.

Пример ввода команды с параметрами, если вы хотите отобразить все статусы проверки объектов в результатах проверки

```
curl --cert /root/cert.pem --key /root/server.key -
X GET "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-
b11a-11001b1f1111/scans/state?sensorInstanceId=instance1&state=detect,not
detected,processing,error,timeout"
```

Запрос на удаление результатов проверки

Для создания запроса на удаление результатов проверки одного или нескольких объектов (см. раздел "Запрос на проверку объектов" на стр. 620) используется метод DELETE. Создать запрос можно, например, с помощью утилиты командной строки cURL.

Синтаксис команды

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого
ключа> -X DELETE "<URL-адрес сервера с компонентом Central Node>:<порт, по
умолчанию 443>/kata/scanner/v1/sensors/<идентификатор
sensorId>/scans/<идентификатор scanId>"
```

При успешной обработке запроса результаты проверки объекта будут удалены. Отобразится статус "OK".

Параметры

Параметр	Тип	Описание
sensorId	string	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
scanId	string	Уникальный идентификатор запроса на проверку объекта (см. раздел "Запрос на проверку объектов" на стр. 620). Если этот параметр не задан, будут удалены результаты проверки всех объектов.

Возвращаемое значение

Код возврата	Описание
200	Проверка выполнена успешно.
401	Требуется авторизация.
404	Не найдены результаты проверки по указанному идентификатору.
500	Внутренняя ошибка сервера. Повторите запрос позднее.

Пример ввода команды

```
curl --cert /root/cert.pem --key /root/server.key -
X DELETE "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-
111c-b11a-11001b1f1111/scans/1"
```

Запрос на вывод ограничений приложения на проверку объектов

Для создания запроса на вывод ограничений приложения на проверку объектов (например, по размеру) используется HTTP-метод GET. Создать запрос можно, например, с помощью утилиты командной строки cURL.

Синтаксис команды

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого
ключа> -X GET "<URL-адрес сервера с компонентом Central Node>:<порт, по
умолчанию 443>/kata/scanner/v1/sensors/<идентификатор
sensorId>/scans/filters"
```

При успешной обработке запроса отобразятся ограничения приложения на проверку объектов. Например, ограничение maxObjectSize – максимально допустимый размер объекта, который вы можете отправить на проверку.

Параметры

Параметр	Тип	Описание
sensorId	string	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.

Ответ

HTTP-код: 200

Формат: JSON

```
type Response struct {
   MaxObjectSize integer `json:"maxObjectSize"`
   Version       string  `json:"version"`
}
```

Возвращаемое значение

Код возврата	Описание
401	Требуется авторизация.
500	Внутренняя ошибка сервера. Повторите запрос позднее.

Пример ввода команды

```
curl --cert /root/cert.pem --key /root/server.key -
X GET "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-
b11a-11001b1f1111/scans/filters"
```

API для получения внешними системами информации об обнаружениях приложения

Kaspersky Anti Targeted Attack Platform предоставляет интерфейс API для доступа внешних систем к информации обо всех обнаружениях приложения, а не только о результатах проверки объектов, хранящихся в этих внешних системах.

Вы можете указать в параметрах запроса фильтры, чтобы получить информацию только о тех обнаружениях, которые удовлетворяют требуемым условиям.

При появлении новых обнаружений приложение не отправляет информацию о них автоматически на основе предыдущих запросов. Для получения актуальной информации требуется отправить повторный запрос.

Особенности работы в распределенном решении

Если приложение работает в режиме распределенного решения (см. раздел "Распределенное решение и мультитенантность" на стр. 75), то вам нужно настроить интеграцию с внешней системой (см. раздел "Взаимодействие с внешними системами по API" на стр. 618) для каждого сервера PCN и SCN, с которого вы хотите получать информацию об обнаружениях, отдельно. Ограничение связано с тем, что в веб-интерфейсе сервера PCN отображается информация обо всех обнаружениях, однако в базе обнаружений хранятся только те обнаружения, которые были зарегистрированы на этом сервере.

В этом разделе

Запрос на вывод информации об обнаружениях 626

Состав передаваемых данных 628

Запрос на вывод информации об обнаружениях

Для создания запроса на вывод информации об обнаружениях Kaspersky Anti Targeted Attack Platform используется HTTP-метод `GET`. Создать запрос можно, например, с помощью утилиты командной строки cURL.

Синтаксис команды

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого
ключа> -X GET "<URL-адрес сервера с компонентом Central Node>:<порт, по
умолчанию 443>/kata/scanner/v1/sensors/<идентификатор
sensorId>/detects?detect_type=<одна или несколько технологий, с помощью
которых выполнено обнаружение>&limit=<количество обнаружений в ответе на
запрос>&token=<идентификатор запроса>"
```

При успешной обработке запроса отобразится список обнаружений, выполненных приложением Kaspersky Anti Targeted Attack Platform на сервере внешней системы.

Параметры

Параметр	Тип	Описание
`sensorId`	String	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
`detect_type`	Array	Технология, с помощью которой выполнено обнаружение. Возможно указать несколько технологий через запятую. Возможные значения: • `am` – Anti-Malware Engine; • `sb` – Sandbox; • `yara` – YARA; • `url_reputation` – URL Reputation; • `ids` – Intrusion Detection System; Если параметр не указан, предоставляется информация обо всех обнаружениях.
`limit`	Integer	Количество объектов, информация о которых будет предоставлена в ответ на запрос. Допустимые значения: целые числа от 1 до 10000. По умолчанию установлено значение `1000`.
`token`	String	Идентификатор запроса. При указании этого параметра в повторном запросе не отображается информация об обнаружениях, полученная в предыдущих запросах. Это позволяет избежать дублирования информации об одних и тех же обнаружениях при повторных запросах. Если этот параметр не указан, предоставляется информация обо всех обнаружениях.

Ответ

HTTP-код: 200

Формат: JSON

```
type Response struct {
   Detects array  `json:"detects"`
   Token   string `json:"token"`
}
```

Возвращаемое значение

Код возврата	Описание
400	Ошибка ввода параметров.
429	Превышено количество запросов.
401	Требуется авторизация.
500	Внутренняя ошибка сервера. Повторите запрос позднее.

Пример ввода команды с параметрами

```
curl --cert /root/cert.pem --key /root/server.key -
X GET "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-
b11a-
11001b1f1111/detects?detect_type=am,sb&limit=100&token=7b226f666673657422
3a20307d"
```

Состав передаваемых данных

Информация, передаваемая о каждом обнаружении, представлена в таблице ниже.

Таблица 46. Состав передаваемых данных об обнаружении

Параметр	Значение	Описание
alertID	Целочисленное значение.	Идентификатор обнаружения.
eventTimeStamp	Дата и время.	Время события.
detectTimestamp	Дата и время.	Время занесения информации об обнаружении в базу Kaspersky Anti Targeted Attack Platform.
importance	Одно из следующих значений: • high; • medium; • low.	Важность обнаружения.
objectSource	Одно из следующих значений: • web; • mail; • endpoint; • external; • dns.	Источник обнаруженного объекта.
technology	Одно из следующих значений: • am – Anti-Malware Engine; • sb – Sandbox; • yara – YARA; • url_reputation – URL Reputation; • ids – Intrusion Detection System.	Технология, с помощью которой обнаружен объект.
objectType	Одно из следующих значений: • file. • URL. • host (для удаленных доменов или хостов).	Тип обнаруженного объекта.
object	Зависит от типа обнаруженного объекта.	Данные об обнаруженном объекте (см. раздел "Данные об обнаруженных объектах" на стр. 630).
detection	Зависит от технологии, с помощью которой обнаружен объект.	Данные о найденных угрозах (на стр. 630).
details	Зависит от источника обнаруженного объекта.	Данные об окружении обнаруженных объектов (на стр. 631).

kaspersky

В этом разделе

Данные об обнаруженных объектах....630

Данные о найденных угрозах....630

Данные об окружении обнаруженных объектов....631

Данные об обнаруженных объектах

Состав передаваемых данных об обнаруженных объектах в зависимости от типа объекта приведен в таблице ниже.

Таблица 47. Данные об обнаруженных объектах

	Параметр	Тип данных	Описание	Пример
file	processedObject.MD5	MD5	MD5-хеш файла или составного объекта, переданного на проверку.	1839a1e9621c58dadf782e131df3821f
	processedObject.SHA256	SHA256	SHA256-хеш файла или составного объекта, переданного на проверку.	7bbfc1d690079b0c591e146c4294305da1cee857e12db40f4318598fdb503a47
	processedObject.fileName	String	Имя файла или составного объекта, переданного на проверку.	EICAR-CURE.com
	processedObject.fileType	String	Тип файла или составного объекта, переданного на проверку.	GeneralTxt
	processedObject.fileSize	Integer	Размер файла или составного объекта, переданного на проверку, в байтах.	184
	detectedObject.MD5	MD5	MD5-хеш файла (простого объекта или файла внутри составного объекта), в котором обнаружена угроза.	1839a1e9621c58dadf782e131df3821f
	detectedObject.fileName	String	Имя файла (простого объекта или файла внутри составного объекта), в котором обнаружена угроза.	EICAR-CURE.com
	detectedObject.fileSize	Integer	Размер файла (простого объекта или файла внутри составного объекта), в котором обнаружена угроза, в байтах.	184
URL	detectedObject	String	URL-адрес обнаруженного объекта.	http://example.com/link
host	detectedObject	Array	Список доменов, к которым относятся обнаруженные объекты. Для технологии URL, а также для объектов с параметром objectSource=dns список может содержать несколько доменов.	example.org, example.net

Данные о найденных угрозах

Состав передаваемых данных о найденных угрозах в зависимости от технологии, с помощью которой выполнено обнаружение, приведен в таблице ниже.

Таблица 48. Данные о найденных угрозах

Технология	Параметр	Описание	Тип данных	Пример
Одна из следующих технологий: • Anti-Malware Engine. • YARA. • Intrusion Detection System.	detect	Список найденных угроз.	Array	HEUR:Trojan.Win32.Generic, Trojan-DDoS.Win32.Macri.avy, UDS:DangerousObject.Multi.Generic
	dataBaseVersion	Версия баз, с помощью которых проверен файл.	Integer	201811190706
Sandbox	detect	Список найденных угроз.	Array	HEUR:Trojan.Win32.Generic, Trojan-DDoS.Win32.Macri.avy, UDS:DangerousObject.Multi.Generic
	image	Имя образа виртуальной машины, на которой был проверен файл.	String	Win7
	dataBaseVersion	Версия баз в следующем формате: <версия баз приложения, с помощью которых проверен файл> / <версия баз модуля IDS>.	Integer	201902031107/ 201811190706
URL Reputation	detect	Список категорий URL Reputation для обнаруженного объекта (для объектов типа URL или host).	Array	Phishing host, Malicious host, Botnet C&C(Backdoor.Win32.Mokes)

Данные об окружении обнаруженных объектов

Состав передаваемых данных об окружении обнаруженных объектов в зависимости от источника объекта приведен в таблице ниже.

Таблица 49. Данные об окружении обнаруженных объектов

Источник объекта	Параметр	Описание	Тип данных	Пример
web	sourceIP	IP-адрес компьютера, установившего соединение.	IP address	192.0.2.0
	sourceHostname	Имя компьютера, установившего соединение.	String	example.com
	destinationIp	IP-адрес компьютера, с которым установлено соединение.	IP address	198.51.100.0

Источник объекта	Параметр	Описание	Тип данных	Пример
	destinationPort	Порт компьютера, с которым установлено соединение.	Integer	3128
	URL	URL-адрес интернет-ресурса, к которому выполнено обращение. Для обнаружений, выполненных технологией IDS, этот параметр отсутствует. Для обнаружений, выполненных технологией URL, этот параметр совпадает с параметром detectedObject.	String	https://example.com:443/
	method	Метод HTTP-запроса.	String	Connect
	referrer	URL-адрес, на который была выполнена переадресация.	String	https://example.com:443/
	agentString	Заголовок User agent из HTTP-запроса, содержащий название и версию клиентского приложения.	String	Mozilla/4.0
mail	mailFrom	Адрес электронной почты отправителя.	String	sender@example.com
	mailTo	Список адресов электронной почты получателей через запятую.	Array	recipient1@example.com, recipient2@example.com
	subject	Тема сообщения.	String	'You are the winner'
	messageId	ID сообщения электронной почты.	String	1745028736.156014.1542897410859.JavaMail.svc_jira_pool@hqconflapp2
• endpoint • external	hostName	Имя компьютера, на котором выполнено обнаружение.	String	computername.example.com
	IP	IP-адрес компьютера, на котором выполнено обнаружение.	IP address	198.51.100.0
dns	sourceIp	IP-адрес компьютера, инициировавшего соединение по протоколу DNS.	IP address	192.0.2.0
	destinationIp	IP-адрес компьютера, с которым установлено соединение по протоколу DNS (как правило, DNS-сервера).	IP address	198.51.100.0
	destinationPort	Порт компьютера, с которым установлено соединение по протоколу DNS (как правило, DNS-сервера).	Integer	3128
	dnsMessageType	Тип DNS-сообщения: • Request. • Response.	String	Request

Источник объекта	Параметр	Описание	Тип данных	Пример
	dnsRequestType	Один из следующих типов записи DNS-запроса: • A. • AAA. • CNAME. • MX.	String	MX
	domainToBeResolved	Имя домена из DNS-запроса.	String	example.com

API для получения внешними системами информации о событиях приложения

Kaspersky Anti Targeted Attack Platform предоставляет интерфейс API для доступа внешних систем к информации о зарегистрированных приложением событиях.

Вы можете указать в параметрах запроса фильтры, чтобы получить информацию только о тех событиях, которые удовлетворяют требуемым условиям.

> При появлении новых событий приложение не отправляет информацию о них автоматически на основе предыдущих запросов. Для получения актуальной информации требуется отправить повторный запрос.

Информация о новых событиях доступна для получения не более двух часов после их появления в базе Kaspersky Anti Targeted Attack Platform.

Особенности работы в распределенном решении

Если приложение работает в режиме распределенного решения (см. раздел "Распределенное решение и мультитенантность" на стр. 75), то вам нужно настроить интеграцию с внешней системой (см. раздел "Взаимодействие с внешними системами по API" на стр. 618) для каждого сервера PCN и SCN, с которого вы хотите получать события, отдельно. Ограничение связано с тем, что в веб-интерфейсе сервера PCN отображается информация обо всех событиях, однако в базе событий хранятся только те события, которые были зарегистрированы на этом сервере.

Запрос на вывод информации о событиях

Для создания запроса на вывод информации о событиях используется HTTP-метод GET.

При первом запросе Kaspersky Anti Targeted Attack Platform создает *ContinuationToken* (далее также "токен"). Приложение передает события, доступные в системе на момент создания токена. При создании нового токена Kaspersky Anti Targeted Attack Platform отправляет события, доступные в системе на момент создания этого токена.

Токен содержит информацию о том, какие данные были переданы последними. Если вы хотите получать события, записанные с момента последнего запроса, вам нужно сохранить созданный токен и использовать его в следующих запросах.

Синтаксис команды

Для первого запроса:

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого
ключа> -X GET "<URL-адрес сервера с компонентом Central Node>:<порт, по
умолчанию 443>/kata/events_api/v1/<идентификатор external_system_id>/events"
```

При успешной обработке запроса отобразится информация о запрошенных событиях и значение токена.

Для следующих запросов:

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого
ключа> -X GET "<URL-адрес сервера с компонентом Central Node>:<порт, по
умолчанию 443>/kata/events_api/v1/<идентификатор
external_system_id>/events&continuation_token=<значение токена, полученное
при первом запросе>"
```

При успешной обработке запроса отобразится информация о событиях, полученных с момента последнего запроса.

Вы можете создать запрос на вывод информации о событиях, указав максимальные время сбора и количество событий, а также параметры фильтрации событий:

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого
ключа> -X GET "<URL-адрес сервера с компонентом Central Node>:<порт, по
умолчанию 443>/kata/events_api/v1/<идентификатор
external_system_id>/events?filter=<фильтр для
событий>&max_timeout=<максимальное время сбора
событий>&max_events=<максимальное количество
событий>&continuation_token=<значение токена, полученное при первом запросе>"
```

Если при первом запросе вы указали значение параметра `filter`, при повторном запросе вы можете его не указывать: параметры фильтрации сохраняются от предыдущего запроса и используются в случае, если не указаны новые. Если вы не хотите использовать фильтрацию, не указывайте значение для параметра.

Параметры

Параметр	Тип	Описание
`external_system_id`	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
`filter`	string	Параметры фильтрации событий. Задаются с помощью языка запросов для работы с событиями (см. раздел "Язык запросов для фильтрации событий" на стр. 637).
`max_timeout`	int	Максимальное время сбора событий. Указывается в формате PT<значение, выраженное целым числом>S. Например, PT300S. Сервер отправляет информацию о событиях, собранную за указанное время. Значение по умолчанию – 5 минут. Это значение используется, если в запросе не указано другое. Максимальное время сбора событий не должно превышать 5 минут. Если вы укажете значение, превышающее 5 минут, сервер Central Node вернет ошибку. Фактическое полное время ожидания событий может быть увеличено.

Параметр	Тип	Описание
max_events	int	Максимальное количество событий. Если в запросе не указано значение, Kaspersky Anti Targeted Attack Platform вычисляет его, исходя из количества хостов, на которые установлен компонент Endpoint Agent. Примеры значений для типовых конфигураций: • Для 1000 хостов – 64000. • Для 5000 хостов – 128000. • Для 10000 хостов – 208000. • Для 15000 хостов – 288000. • Для 30000 хостов – 528000. Указанное в запросе значение не должно их превышать.
continuation_token	string	Значение токена.

Пример ввода команд с параметрами

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого
ключа> -X GET "https://10.10.0.22:443/kata/events_api/v1/c440a37b-5c01-
4505-a30e-3d23b20dd609/events"
```

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого
ключа> -X GET "https://10.10.0.22:443/kata/events_api/v1/c440a37b-5c01-
4505-a30e-3d23b20dd609/events?
filter=EventType=='threatdetect' OR
EventType=='threatprocessingresult'&max_timeout=PT300S&max_events=64000&co
ntinuation_token=
CiQyZDcyNjNiOS0zZmNlLTQxNzktYTdhOC03N2E0ZmUwNjNjMTkSBAgAEAoSBAgBEAMSBAgCEA
sSBAgDEAcSBAgEEAgSBAgFEAkSBAgGEAQSBAg
HEAUSBAgIEAcSBAgJEAMYiYyCmvIw"
```

Если значения параметров содержат специальные символы, вам необходимо в запросах использовать кодирование URL или команду `--data-urlencode`.

Пример ввода команд с параметрами с использованием кодирования URL

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого
ключа> -X GET "https://10.10.0.22:443/kata/events_api/v1/c440a37b-5c01-
4505-a30e-3d23b20dd609/events?
filter=EventType=='threatdetect' OR
EventType=='threatprocessingresult'&max_timeout=PT300S&max_events=64000&co
ntinuation_token=
CiQ%3Dcy%7ENiOS0zZmNlLTQxNzktYTdhOC03N2E0Z40%wNjNjMTkSBAgAEAoSBAgB%5EMSB%3
CEAsSBAgDEAcSBAgEEAgSBAgFEAkSBAgGEAQSBAg
HEAUSBAgIEAcSBAgJEAMYiYyCmvIw"
```

Пример ввода команд с параметрами с использованием команды `--data-urlencode`

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого
ключа> --GET -d "max_events=64000" -d "max_timeout=PT300S" -d
"filter=EventType=='threatdetect'" --data-urlencode "continuation_token=
CiQ?Dcy~NiOS0zZmNlLTQxNzktYTdhOC03N2E0Z@wNjNjMTkSBAgAEAoSBAgB^MSB?CEAsSBAgDE
AcSBAgEEAgSBAgFEAkSBAgGEAQSBAg
HEAUSBAgIEAcSBAgJEAMYiYyCmvIw"
https://10.10.0.22:443/kata/events_api/v1/c440a37b-5c01-4505-a30e-
3d23b20dd609/events
```

Ответ

HTTP-код: 200

Формат: JSON

```
type Respons struct {
   Events             array  `json:"events"`
   ContinuationToken  string `json:"continuationToken"`
}
```

Возвращаемое значение

Код возврата	Описание
400	Ошибка ввода параметров.
401	Требуется авторизация.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Язык запросов для фильтрации событий

Язык запросов для фильтрации событий поддерживает следующие функции и операторы:

- Функции: `in`.
- Операторы сравнения для значений типа String или Boolean:
  - `==`.
  - `!=`.
- Операторы сравнения для чисел и переменных:
  - `AND`.
  - `OR`.
  - `NOT`.
  - `==`.
  - `!=`.
  - `>`.
  - `>=`.
  - `<`.
  - `<=`.

Вы можете посмотреть список полей, по которым можно отфильтровать события, в разделе Поля для фильтрации событий (на стр. 638).

Если вы хотите получить информацию о событиях разного типа, вам нужно создать отдельный запрос для каждого типа событий.

```
EventType=='threatdetect' OR EventType=='threatprocessingresult'
```

Поддерживаются константы числового и строкового типа. Строковые константы заключаются в апострофы: `'example'`. Для строковых констант поддерживаются метасимволы * и ?. Если вы не хотите использовать метасимволы, вам нужно экранировать их: `\*`, `\?`. Также в строковых константах вам нужно экранировать специальные символы.

Поля для фильтрации событий

Список полей для фильтрации событий приведен в таблице ниже.

Если значения полей содержат специальные символы, вам необходимо в запросах использовать кодирование URL или команду `--data-urlencode`.

Таблица 50. Список полей для фильтрации событий

Название поля	Тип	Описание
HostName	string	Имя хоста.
HostIp	string	IP-адрес хоста.
EventType	string	Тип события. Может иметь следующие значения: process – запущен процесс. process_terminate – завершен процесс. module – загружен модуль. connection – удаленное соединение. applock – правило запрета. blockdocument – заблокирован документ. filechange – изменен файл. windowsevent – журнал событий ОС. registry – изменение в реестре. portlisten – прослушан порт. driver – загружен драйвер. threatdetect – обнаружение. threatprocessingresult – результат обработки обнаружения. amsiscan – AMSI-проверка. process_interpretated_file_run – интерпретированный запуск файла. process_console_interactive_input – интерактивный ввод команд в консоли.
UserName	string	Имя пользователя.
OsFamily	string	Семейство операционной системы.
OsVersion	string	Версия операционной системы, используемой на хосте.
Ioa.Rules.Id	string	Идентификатор правила ТАА (IOA).
Ioa.Rules.Name	string	Информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила ТАА (IOA), по которому было выполнено обнаружение.
Ioa.Rules.Techniques	string	Техника MITRE.
Ioa.Rules.Tactics	string	Тактика MITRE.

Ioa.Severity	string	Степень важности, присвоенная событию, выполненному по этому правилу ТАА (IOA). Может иметь следующие значения: Low. Medium. High.
Ioa.Confidence	string	Уровень надежности в зависимости от вероятности ложных срабатываний правила. Может иметь следующие значения: Low. Medium. High.
FileCreationTime	integer	Время создания файла.
DllCreationTime	integer	Время создания библиотеки DLL.
DroppedCreationTime	integer	Время создания измененного файла.
InterpretedFileCreationTime	integer	Время создания интерпретируемого файла.
FileName	string	Имя файла.
DllName	string	Имя библиотеки DLL.
DroppedName	string	Имя измененного файла.
BlockedName	string	Имя заблокированного файла.
InterpretedFileName	string	Имя интерпретируемого файла.
FilePath В случае фильтрации событий по этому полю необходимо использовать URL Encode.	string	Путь к директории, в которой располагается файл.
DllPath	string	Путь к директории, в которой располагается библиотека DLL.
DroppedPath	string	Путь к директории, в которой располагается измененный файл.
BlockedPath	string	Путь к директории, в которой располагается заблокированный файл.
InterpretedFilePath	string	Путь к директории, в которой располагается интерпретируемый файл..
FileFullName В случае фильтрации событий по этому полю необходимо использовать URL Encode.	string	Полный путь к файлу. Включает путь к директории и имя файла.
DllFullName	string	Полный путь к библиотеке DLL. Включает путь к директории и имя файла.
DroppedFullName	string	Полный путь к измененному файлу. Включает путь к директории и имя файла.
BlockedFullName	string	Полный путь к заблокированному файлу. Включает путь к директории и имя файла.

DetectedName	string	Полный путь к обнаруженному файлу. Включает путь к директории и имя файла.
OriginalFileName	string	Полный путь к исходному файлу. Включает путь к директории и имя файла.
InterpretedFileFullName	string	Полный путь к интерпретируемому файлу. Включает путь к директории и имя файла.
FileModificationTime	integer	Время изменения файла.
DllModificationTime	integer	Время изменения библиотеки DLL.
DroppedModificationTime	integer	Время изменения измененного файла.
InterpretedFileModificationTime	integer	Время изменения интерпретируемого файла.
FileSize	integer	Размер файла.
DllSize	integer	Размер библиотеки DLL.
DroppedSize	integer	Размер измененного файла.
InterpretedFileSize	integer	Размер интерпретируемого файла.
Md5	string	MD5-хеш файла.
DllMd5	string	MD5-хеш библиотеки DLL
DroppedMd5	string	MD5-хеш измененного файла.
InterpretedMd5	string	MD5-хеш интерпретируемого файла.
DetectedMd5	string	MD5-хеш обнаруженного файла.
Sha256	string	SHA256-хеш файла.
DllSha256	string	SHA256-хеш библиотеки DLL.
DroppedSha256	string	SHA256-хеш измененного файла.
BlockedSha256	string	SHA256-хеш заблокированного файла.
InterpretedSha256	string	SHA256-хеш интерпретируемого файла.
DetectedSha256	string	SHA256-хеш обнаруженного файла.
HijackingPath	string	Вредоносная DLL, помещенная в директорию по стандартному пути обхода, чтобы система загрузила ее раньше, чем исходную DLL.
LogonRemoteHost	string	IP-адрес хоста, с которого был выполнен удаленный вход.
RealUserName	string	Имя пользователя, назначенное ему при регистрации в системе.
EffectiveUserName	string	Имя пользователя, которое было использовано для входа в систему.
Environment	string	Переменные окружения.

ProcessType	integer	Тип процесса. Может иметь следующие значения: 1 – exec. 2 – fork. 3 – vfork. 4 – clone.
LinuxOperationResult	string	Результат операции. Может иметь следующие значения: success. failed.
SystemPid	integer	Идентификатор процесса.
ParentFileFullName В случае фильтрации событий по этому полю необходимо использовать URL Encode.	string	Путь к файлу родительского процесса.
ParentMd5	string	MD5-хеш файла родительского процесса.
ParentSha256	string	SHA256-хеш файла родительского процесса.
StartupParameters	string	Параметры запуска.
ParentSystemPid	integer	Идентификатор родительского процесса.
Method	string	Метод HTTP-запроса.
Direction	string	Направление соединения. Может иметь следующие значения: inbound. outbound.
LocalIp	string	IP-адрес локального компьютера, с которого была произведена попытка удаленного соединения.
LocalPort	integer	Порт локального компьютера, с которого была произведена попытка удаленного соединения.
RemoteHostName	string	Имя компьютера, на который была произведена попытка удаленного соединения.
RemoteIp	string	IP-адрес компьютера, на который была произведена попытка удаленного соединения.
RemotePort	integer	Порт компьютера, на который была произведена попытка удаленного соединения.
URI	string	Адрес ресурса, к которому произведен запрос HTTP.
KeyName	string	Путь к ключу реестра.
ValueName	string	Имя параметра реестра.
ValueData	string	Значение параметра реестра.

RegistryOperationType	integer	Тип операции с реестром. Может иметь следующие значения: 0 – создан ключ реестра. 1 – удален ключ реестра. 2 – изменен реестр. 3 – переименован ключ реестра.
PreviousKeyName	string	Предыдущий путь к ключу реестра.
PreviousValueData	string	Предыдущее имя параметра реестра.
System.EventID.value	string	Идентификатор типа события безопасности в журнале Windows.
LinuxEventType (поле используется для получения типа события, зафиксированного в журнале событий операционных систем Linux и macOS)	string	Тип события. Может иметь следующие значения: NewUserCreated – создана учетная запись. UserAccountDeleted – учетная запись пользователя удалена. GroupCreated – создана группа. GroupDeleted – изменена группа. MemberAddedToGroup – учетная запись добавлена в группу. UserPasswordChanged – изменен пароль учетной записи. LinuxAuth – выполнена аутентификация в ОС Linux и macOS. LinuxSessionStart – запущена сессия в ОС Linux и macOS. LinuxSessionEnd – завершена сессия ОС Linux и macOS. ServiceStart – запущена служба. ChangeAccountExpirationDate – изменен срок действия учетной записи. OperatingSystemShuttingDown – выключена операционная система. OperatingSystemStarted – запущена операционная система. ModifyPromiscuousMode – изменена работа неразборчивого режима. AuditdConfigurationChanged – изменены настройки аудита
System.Channel.value	string	Имя журнала.
System.EventRecordID.value	string	Идентификатор записи в журнале
System.Provider.Name.value	string	Идентификатор системы, записавшей событие в журнал.
EventData.Data.TargetDomainName.value	string	Доменное имя удаленного компьютера.
EventData.Data.ObjectName.value	string	Имя объекта, инициировавшего событие.
EventData.Data.PackageName.value	string	Имя пакета, инициировавшего событие.
EventData.Data.ProcessName.value	string	Имя процесса, инициировавшего событие.
VerdictName	string	Имя обнаруженного объекта.
RecordId	integer	Идентификатор сработавшего правила.
ProcessingMode	string	Режим проверки. Может иметь следующие значения: Default – по умолчанию. OnDemand – при запросе. OnAccess – при доступе. OnExecute – при выполнении. OnDownload – при загрузке. OnStartup – при запуске приложений. OnMail – при отправке сообщения.

		OnPostpone – при отложенной проверке. OnDisinfect – при лечении. OnVulnerability – при поиске уязвимостей. OnFirstLaunch – при первом запуске. OnEngineLoad – при запуске системы. OnQuarantineRescan – при повторной проверке объектов в Хранилище. OnWebRequest – при веб-запросе. OnAmsiScan – при проверке AMSI. OnSystemWatcherScan – при анализе поведения приложений.
DetectedName	string	Имя объекта.
DetectedObjectType	string	Тип объекта. Может иметь следующие значения: Unknown – неизвестно. File – файл. LogicalDrive – логический диск. PhysicalDisk – физический диск. SystemMemory – системная память. MemoryProcess – память процесса. MemoryModule – модуль памяти. MailMsgRef – заголовок References сообщения электронной почты. MailMsgMime – MIME-вложения. MailMsgBody – текст сообщения электронной почты. MailMsgAttach – вложение сообщения электронной почты. StartUp – объекты автозапуска. Folder – директория. Script – скрипт. Url – URL-адрес. AmsiStream – поток проверки AMSI.
ThreatStatus	string	Режим обнаружения. Может иметь следующие значения: Untreated – объект не обработан. Untreatable – объект не поддается обработке. NotFound – объект не найден. Disinfected – объект вылечен. Deleted – объект удален. Quarantined – объект помещен на карантин. AddedByUser – объект добавлен пользователем. Unknown – неизвестно. AddedToExclude – объект добавлен в исключения. Terminated – обработка прервана. Clear – объект не заражен. FalseAlarm – ложное срабатывание. RolledBack – выполнен откат к предыдущему состоянию. IpNotBlocked – IP-адрес не заблокирован. IpBlocked – IP-адрес заблокирован. IpCannotBeBlocked – IP-адрес не может быть заблокирован. IpBlockIsNotRequired – не требуется блокировка IP-адреса.
UntreatedReason	string	Статус обработки объекта. Может иметь следующие значения: None – нет данных. NonCurable – объект невозможно вылечить. Locked – объект заблокирован. ReportOnly – приложение работает в режиме *Только отчет*. NoRights – нет прав на выполнение действия.

		Cancelled – обработка отменена. WriteProtect – объект защищен от записи. TaskStopped – задача на обработку прервана. Postponed – действие отложено. NonOverwritable – объект невозможно перезаписать. CopyFailed – не удалось создать копию объекта. WriteError – ошибка записи данных. OutOfSpace – нет места на диске. ReadError – ошибка чтения данных. DeviceNotReady – устройство не готово. ObjectNotFound – объект не найден. WriteNotSupported – запись данных не поддерживается. CannotBackup – не удалось создать резервную копию объекта. SystemCriticalObject – объект является критическим для системы. AlreadyProcessed – объект уже был обработан.
InteractiveInputText	string	Команда интерпретатора.
ObjectContent	string	Содержание скрипта, переданного на проверку.
ObjectContentType	integer	Тип содержимого скрипта. Может иметь следующие значения: 1 – текст. 2 – двоичный код.
FileOperationType	integer	Тип операции с файлом. Может иметь следующие значения: 1 – создан файл. 2 – изменен файл. 3 – переименован файл. 4 – изменены атрибуты файла. 5 – удален файл. 6 – прочитан файл.
PreviousFileName	string	Путь к директории, в которой файл располагался ранее.
PreviousFileFullName	string	Полное имя файла, включающее предыдущий путь к директории, в которой файл располагался ранее, и / или предыдущее имя файла.
DroppedFileType	integer	Тип измененного файла. Может иметь следующие значения: 0 – неизвестно. 1 – другие файлы. 2 – образ PE. 3 – PE DLL. 4 – ресурсы PE. 5 – файл ресурсов .NET. 6 – файл ELF.

API для управления действиями по реагированию на угрозы

Kaspersky Anti Targeted Attack Platform предоставляет интерфейс API для осуществления действий по реагированию на угрозы. Команды на выполнение операций поступают на сервер Central Node, после чего приложение передает их компоненту Endpoint Agent.

С помощью внешних систем вы можете выполнить следующие операции на хостах с компонентом Endpoint Agent:

- Управлять сетевой изоляцией хостов (см. раздел "Управление сетевой изоляцией хостов" на стр. 649).
- Управлять правилами запрета (см. раздел "Управление правилами запрета" на стр. 656).
- Запускать приложения (см. раздел "Управление задачей запуска приложения" на стр. 662).

Все перечисленные операции доступны на хостах, на которых в роли компонента Endpoint Agent используются приложения Kaspersky Endpoint Agent для Windows и Kaspersky Endpoint Security для Windows.

Если в роли компонента Endpoint Agent используется Kaspersky Endpoint Security для Linux, вы можете управлять сетевой изоляцией и запускать приложения.

В этом разделе

Запрос на получение списка хостов с компонентом Endpoint Agent 645

Запрос на получение информации о сетевой изоляции и наличии правил запрета для хостов с компонентом Endpoint Agent 647

Управление сетевой изоляцией хостов 649

Управление правилами запрета 656

Управление задачей запуска приложения 662

Запрос на получение списка хостов с компонентом Endpoint Agent

Для создания запроса на вывод информации о хостах с компонентом Endpoint Agent используется HTTP-метод GET.

Синтаксис команды

GET "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию 443>/kata/response_api/v1/<идентификатор external_system_id>/sensors"

При успешной обработке запроса отобразится список хостов с компонентом Endpoint Agent.

Вы можете создать запрос на вывод информации о хостах с фильтрами по IP-адресу, имени или идентификатору хоста. Вы можете указать один, несколько или все перечисленные фильтры.

При указании имени хоста вам нужно учитывать, что фильтр чувствителен к регистру символов.

GET "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию 443>/kata/response_api/v1/<идентификатор external_system_id>/sensors?ip=<IP-адрес хоста>&host=<имя хоста>&sensor_id=<идентификатор sensor_id>"

При успешной обработке запроса отобразится информация о выбранном хосте с компонентом Endpoint Agent.

Параметры

Параметр	Тип	Описание
external_system_id	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
sensor_id	UUID	Уникальный идентификатор хоста с компонентом Endpoint Agent.
ip	string	IP-адрес хоста с компонентом Endpoint Agent.
host	string	Имя хоста с компонентом Endpoint Agent.

Пример ввода команд с параметрами

```
GET "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/sensors"
```

```
GET "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/sensors?ip=10.16.40.243&host=host4&sensor_id=DF64838B-B518-414B-B769-2B8BE341A2F0"
```

Ответ

HTTP-код: 200

Формат: JSON

```
type Response Sensors

type Server struct {
   Version             string  `json:"version"`
},

type Sensors struct {
   SensorID            UUID    `json:"sensorId"`
   HostIP              string  `json:"hostIp"`
   LastAccessTimestamp         `json:"lastAccessTimestamp"`
   Version             string  `json:"version"`
   SelfDefenseState    boolean `json:"selfDefenseState"`
   LicenseStatus       string  `json:"licenseStatus"`
   OSFamily            string  `json:"osFamily"`
   OSName              string  `json:"osName"`
   Capabilities        array   `json:"capabilities"`
}
```

Возвращаемое значение

Код возврата	Описание
400	Требуется авторизация.
401	Ошибка ввода параметров.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Запрос на получение информации о сетевой изоляции и наличии правил запрета для хостов с компонентом Endpoint Agent

Для создания запроса на вывод информации о сетевой изоляции и наличии правил запрета для хостов с компонентом Endpoint Agent используется HTTP-метод GET.

Синтаксис команды

```
GET "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор
```

```
external_system_id>/settings?sensor_id=<идентификатор
sensor_id>&settings_type=<network_izolation или prevention>"
```

При успешной обработке запроса отобразится список хостов с компонентом Endpoint Agent, для которых на момент выполнения запроса применены правила запрета или сетевой изоляции.

Параметры

Параметр	Тип	Описание
external_system_id	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
sensor_id	UUID	Уникальный идентификатор хоста с компонентом Endpoint Agent.
settings_type	enum	Тип правила - network_izolation или prevention.

Пример ввода команды с параметрами

```
GET "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-
B0391CF21EF3/settings?sensor_id=DF64838B-B518-414B-B769-
2B8BE341A2F0&settings_type=network_izolation"
```

Ответ

HTTP-код: 200

Формат: JSON

```
type Response []Settings


type Settings struct {
   ExcludedRules              array   `json:"excludedRules"`
   AutoTurnoffTimeoutInSec    int     `json:"autoTurnoffTimeoutInSec"`
}
```

Возвращаемое значение

Код возврата	Описание
400	Требуется авторизация.
401	Ошибка ввода параметров.
404	Не найден указанный хост с компонентом Endpoint Agent.
500, 502, 503, 504	Внутренняя ошибка. Повторите запрос позднее.

Управление сетевой изоляцией хостов

Для изоляции хоста с компонентом Endpoint Agent с помощью интерфейса API рекомендуется использовать следующий сценарий взаимодействия с Kaspersky Anti Targeted Attack Platform:

a. **Создание запроса на получение списка хостов с компонентом Endpoint Agent (см. раздел "Запрос на получение списка хостов с компонентом Endpoint Agent" на стр. 645)**

b. **Создание запроса на получение информации о хостах, для которых уже включена сетевая изоляция (см. раздел "Запрос на получение информации о сетевой изоляции и наличии правил запрета для хостов с компонентом Endpoint Agent" на стр. 647)**

c. **Создание запроса на одну из следующих операций с хостами с компонентом Endpoint Agent:**

- включение сетевой изоляции (см. раздел "Запрос на включение сетевой изоляции" на стр. 649);
- отключение сетевой изоляции (см. раздел "Запрос на отключение сетевой изоляции" на стр. 651);
- добавление исключения в уже существующее правило сетевой изоляции (см. раздел "Запрос на добавление исключения в правило сетевой изоляции" на стр. 652).

Вы можете управлять созданными правилами сетевой изоляции в веб-интерфейсе приложения.

Запрос на включение сетевой изоляции

Чтобы включить сетевую изоляцию для выбранного хоста, вам требуется добавить правило сетевой изоляции. Для создания запроса используется HTTP-метод POST.

Параметры команды передаются в теле запроса в формате JSON.

Синтаксис команды

```
curl -k --<путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа>
-X POST "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор
external_system_id>/settings?sensor_id=<идентификатор
sensor_id>&settings_type=network_izolation" -H 'Content-Type:
application/json' -d '

{

"settings": {

"autoTurnoffTimeoutInSec": <время действия сетевой изоляции>}

}

'
```

При успешной обработке запроса правило сетевой изоляции будет добавлено. Сетевая изоляция для выбранного хоста действует с момента добавления правила.

По истечении времени, указанного при создании запроса, сетевая изоляция перестанет действовать. Правило сетевой изоляции при этом не удаляется. При необходимости вы можете удалить выбранное правило.

Для отключения сетевой изоляции вам требуется создать запрос на отключение выбранного правила (см. раздел "Запрос на отключение сетевой изоляции" на стр. 651).

Параметры

Параметр	Тип	Описание
external_system_id	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
sensor_id	UUID	Уникальный идентификатор хоста с компонентом Endpoint Agent.
autoTurnoffTimeoutInSec	integer	Время, в течение которого будет действовать сетевая изоляция хоста. Допустимый диапазон – от 1 до 9999 часов. Время сетевой изоляции указывается в секундах. Например, если вы хотите включить сетевую изоляцию хоста на два часа, вам требуется указать 7200 секунд.

Пример ввода команды с параметрами

```
curl -k --example.cert --example.key -X POST
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-
B0391CF21EF3/settings?sensor_id=DF64838B-B518-414B-B769-
2B8BE341A2F0&settings_type=network_izolation" -H 'Content-Type:
application/json' -d '
{
"settings": {
"autoTurnoffTimeoutInSec": 7200}
}
'
```

Ответ

HTTP-код: 200

Формат: JSON

```
type Response []Settings


type Settings struct {
   ExcludedRules              array   `json:"excludedRules"`
   AutoTurnoffTimeoutInSec    integer `json:"autoTurnoffTimeoutInSec"`
}
```

Возвращаемое значение

Код возврата	Описание
400	Ошибка ввода параметров.
401	Требуется авторизация.
404	Не найден указанный хост с компонентом Endpoint Agent.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Если вы хотите изменить параметры созданного правила сетевой изоляции, вам требуется создать новый запрос на добавление правила с нужными параметрами.

Запрос на отключение сетевой изоляции

Чтобы отключить сетевую изоляцию для выбранного хоста, вам требуется создать запрос на отключение правила сетевой изоляции. Для создания запроса используется HTTP-метод DELETE.

Синтаксис команды

```
curl -k --<путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа>
-X DELETE "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор
external_system_id>/settings?sensor_id=<идентификатор
sensor_id>&settings_type=network_izolation"
```

При успешной обработке запроса правило сетевой изоляции будет отключено.

Параметры

Параметр	Тип	Описание
external_system_id	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
sensor_id	UUID	Уникальный идентификатор хоста с компонентом Endpoint Agent.

Пример ввода команды с параметром DELETE

```
curl -k --example.cert --example.key -X DELETE
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-
B0391CF21EF3/settings?sensor_id=DF64838B-B518-414B-B769-
2B8BE341A2F0&settings_type=network_izolation"
```

Для того чтобы проверить отключение сетевой изоляции, выполните запрос на получение информации о задаче, используя HTTP-метод GET.

Пример ввода команды с параметром GET

```
curl -k --example.cert --example.key -X GET
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?sensor_id=DF64838B-B518-414B-B769-2B8BE341A2F0&settings_type=network_izolation"| python -m json.tool
```

Если сетевая изоляция отключена, то Kaspersky Anti Targeted Attack Platform возвращает ответ внешней системе в следующем формате:

```
{
  "error": "Not Found"
}
```

Возвращаемое значение

Код возврата	Описание
400	Ошибка ввода параметров.
401	Требуется авторизация.
404	Не найден указанный хост с компонентом Endpoint Agent.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Запрос на добавление исключения в правило сетевой изоляции

Чтобы добавить исключение для ранее созданного правила сетевой изоляции, вам требуется создать запрос на добавление исключения. Для создания запроса используется HTTP-метод POST.

Параметры команды передаются в теле запроса в формате JSON.

Синтаксис команды

```
curl -k --<путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа>
-X POST "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор
external_system_id>/settings?sensor_id=<идентификатор
sensor_id>&settings_type=network_izolation" -H 'Content-Type:
application/json' -d '
{
"settings": [
{
"excludedRules": [
{
"direction": "<outbound или inbound>",
```

```
"protocol": <номер IP-протокола>,
"remotePortRange": {
"fromPort": <номер порта>,
"toPort": <номер порта>
},

"localPortRange":
{
"fromPort": <номер порта>,
"toPort": <номер порта>
}
}
],
"autoTurnoffTimeoutInSec": <время действия сетевой изоляции>
}
}
'
```

При успешной обработке запроса исключение из правила сетевой изоляции будет добавлено.

Параметры

Параметр	Тип	Описание
external_system_id	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
sensor_id	UUID	Уникальный идентификатор хоста с компонентом Endpoint Agent.
direction	array	Направление сетевого трафика, которое не должно быть заблокировано. Может иметь следующие значения: • inbound; • outbound. Вы можете не указывать значение. В этом случае приложение разрешает передавать трафик в обоих направлениях.

protocol	integer	Номер IP-протокола, назначенный Internet Assigned Numbers Authority (IANA).
remoteIpv4Address/remoteIpv6Address	string	IP-адрес хоста с компонентом Endpoint Agent, сетевой трафик которого не должен быть заблокирован.
remotePortRange	string	Порт назначения. Вы можете указать порт, только если вы выбрали входящее или исходящее направление сетевого трафика. Для двунаправленного трафика нельзя задавать диапазон портов.
localPortRange	string	Порт, с которого устанавливается соединение. Вы можете указать порт, только если вы выбрали входящее или исходящее направление сетевого трафика. Для двунаправленного трафика нельзя задавать диапазон портов.
autoTurnoffTimeoutInSec	integer	Время, в течение которого будет действовать сетевая изоляция хоста. Допустимый диапазон – от 1 до 9999 часов. Время сетевой изоляции указывается в секундах. Например, если вы хотите включить сетевую изоляцию хоста на два часа, вам требуется указать 7200 секунд.

Пример ввода команды с параметрами

```
curl -k --example.cert --example.key -X POST
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-
B0391CF21EF3/settings?sensor_id=DF64838B-B518-414B-B769-
2B8BE341A2F0&settings_type=network_izolation" -H 'Content-Type:
application/json' -d '
{
"settings": [
{
"excludedRules": [
{
"direction": "inbound",
"protocol": 21,
"remoteIpv6Address": "2001:0db8:0000:0000:0000:ff00:0042",
"remotePortRange": {
"fromPort": 19010,
"toPort": 25689
},
"localPortRange":
{
"fromPort": 55409,
"toPort": 13957
}
}
],
"autoTurnoffTimeoutInSec": 7200
}
}
'
```

Ответ

HTTP-код: 200

Формат: JSON

```
type Response []Settings

type Settings struct {
   ExcludedRules             array   `json:"excludedRules"`
   AutoTurnoffTimeoutInSec   integer `json:"autoTurnoffTimeoutInSec"`
}
type ExcludedRules struct {
   Direction                 array   `json:"direction"`
   Protocol                  integer `json:"autoTurnoffTimeoutInSec"`
   RemotePortRange           string  `json:"remotePortRange"`
   LocalPortRange            string  `json:"localPortRange"`
}
```

Возвращаемое значение

Код возврата	Описание
400	Ошибка ввода параметров.
401	Требуется авторизация.
404	Не найден указанный хост с компонентом Endpoint Agent.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Если вы хотите изменить параметры созданного исключения, вам требуется создать новый запрос на добавление исключения с нужными параметрами.

Управление правилами запрета

С помощью правил запрета вы можете заблокировать запуск файлов или процессов на выбранном хосте или всех хостах с компонентом Endpoint Agent. Например, вы можете запретить запуск приложений, использование которых считаете небезопасным. Приложение идентифицирует файлы по их хешу с помощью алгоритмов хеширования MD5 и SHA256. Правило запрета, созданное через внешние системы, может содержать несколько хешей файлов.

Через внешние системы вы можете управлять всеми правилами запрета, созданными для одного хоста или всех хостов, одновременно. При создании правила запрета для выбранного хоста через внешние системы

Kaspersky Anti Targeted Attack Platform заменяет все правила запрета, назначенные на этот хост, правилом с новыми параметрами. Например, если ранее вы добавили несколько правил запрета для выбранного хоста через веб-интерфейс приложения, а потом добавили правило запрета через внешние системы, все правила запрета, добавленные в веб-интерфейсе, будут заменены добавленным через внешние системы правилом.

При изменении параметров правила запрета, созданного через внешние системы, приложение сохраняет только новые параметры. Например, если вы создали правило запрета, которое содержит хеши для нескольких файлов, и хотите добавить в это правило еще один хеш, вам требуется создать запрос на добавление правила запрета и указать в нем все хеши, для которых вы создавали запрет ранее, и новый хеш.

Описанный сценарий также актуален для правил запрета, назначенных на все хосты.

Для создания правила запрета с помощью интерфейса API рекомендуется использовать следующий сценарий взаимодействия с Kaspersky Anti Targeted Attack Platform:

a. **Создание запроса на получение списка хостов с компонентом Endpoint Agent (см. раздел "Запрос на получение списка хостов с компонентом Endpoint Agent" на стр. 645)**

b. **Создание запроса на получение информации о хостах, для которых существуют правила запрета (см. раздел "Запрос на получение информации о сетевой изоляции и наличии правил запрета для хостов с компонентом Endpoint Agent" на стр. 647)**

c. **Создание запроса на одну из следующих операций с правилами запрета:**

- создание правила (см. раздел "Запрос на создание правила запрета" на стр. 658);
- удаление правила (см. раздел "Запрос на удаление правила запрета" на стр. 660).

Добавленные правила запрета отображаются в веб-интерфейсе приложения в разделе **Политики**, подразделе **Правила запрета**.

Если вы создаете через внешнюю систему правило запрета для всех хостов, вам требуется предварительно убедиться, что на сервере отсутствует и не применяется к одному или нескольким хостам правило запрета для этого же файла. Это условие также справедливо, если вы хотите создать через внешнюю систему правило запрета для выбранного хоста: вам требуется убедиться, что на сервере отсутствует и не применяется ко всем хостам правило запрета для этого же файла. В противном случае сервер вернет внешней системе ошибку со списком хостов, к которым уже применяется правило запрета.

Если правило запрета, создаваемое через внешнюю систему, содержит несколько хешей файлов, в информации об ошибке указывается только первый файл, вызвавший ошибку. Сведения о других дублирующихся правилах запрета не отображаются.

Для изменения уже созданного через веб-интерфейс или внешние системы правила запрета вам нужно создать запрос на добавление правила запрета с обновленными параметрами.

Запрос на создание правила запрета

Для создания запроса используется HTTP-метод POST. Параметры команды передаются в теле запроса в формате JSON.

Синтаксис команды

```
curl -k --<путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа>
-X POST "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор
external_system_id>/settings?sensor_id=<идентификатор sensor_id или all, если
вы хотите создать правило запрета для всех хостов>&settings_type=prevention"
-H 'Content-Type: application/json' -d '

{

"settings": {

"objects": [

{

"file": {

"<sha256 или md5>": "<SHA256- или MD5-хеш файла, запуск которого вы хотите
запретить>"

}

},

{

"file": {

"<sha256 или md5>": "<SHA256- или MD5-хеш файла, запуск которого вы хотите
запретить>"

}

'
```

При успешной обработке запроса правило запрета будет добавлено. Правило запрета действует с момента добавления.

При необходимости вы можете удалить правило запрета.

Параметры

Параметр	Тип	Описание
external_system_id	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
sensor_id	UUID	Уникальный идентификатор хоста с компонентом Endpoint Agent.
objects	string	Тип объекта, запуск которого вы хотите запретить. Возможное значения параметра: file.
sha256 или md5	string	SHA256- или MD5-хеш объекта, запуск которого вы хотите запретить.

Пример ввода команды с параметрами

```
curl -k --example.cert --example.key -X POST
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-
B0391CF21EF3/settings?sensor_id=all&settings_type=prevention" -H 'Content-
Type: application/json' -d '
{
"settings": {
"objects": [
{
"file": {
"sha256":
"830195824b742ee59390bc5b9302688c778fc95a64e7d597e28a74c03a04dd63"
}
"file": {
"md5": "d8e577bf078c45954f4531885478d5a9"
}
'
```

Ответ

HTTP-код: 200

Формат: JSON

```
type Response []Objects


type Objects struct {
type file struct {
   SHA256 string  `json:"sha256"`
},
type file struct {
   MD5    string  `json:"md5"`
}
}
```

Возвращаемое значение

Код возврата	Описание
400	Ошибка ввода параметров.
401	Требуется авторизация.
404	Не найден указанный хост с компонентом Endpoint Agent.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Запрос на удаление правила запрета

Вы можете удалить правило запрета с помощью нового запроса с пустыми значениями или запроса с параметром DELETE. Для создания запросов используются HTTP-методы POST и DELETE.

Синтаксис команды для нового запроса

Параметры команды передаются в теле запроса в формате JSON.

```
curl -k --<путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа>
-X POST "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор
external_system_id>/settings?sensor_id=<идентификатор sensor_id или all, если
вы хотите удалить правило запрета для всех хостов>&settings_type=prevention"
-H 'Content-Type: application/json' -d '

{
```

```
"settings": {
"objects": []
}
}
'
```

Синтаксис команды с параметром DELETE

```
curl -k --<путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа>
-X DELETE "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор
external_system_id>/settings?sensor_id=<идентификатор sensor_id или all, если
вы хотите удалить правило запрета для всех хостов>&settings_type=prevention"
```

Параметры

Параметр	Тип	Описание
external_system_id	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
sensor_id	UUID	Уникальный идентификатор хоста с компонентом Endpoint Agent.

Пример ввода команды для нового запроса

```
curl -k --example.cert --example.key -X POST
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-
B0391CF21EF3/settings?sensor_id=all&settings_type=prevention"-H 'Content-Type:
application/json' -d '
{
"settings": {
"objects": []
}
}
'
```

Пример ввода команды с параметром DELETE

```
curl -k --example.cert --example.key -X DELETE
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-
B0391CF21EF3/settings?sensor_id=all&settings_type=prevention"
```

При успешной обработке запроса правило запрета будет удалено.

Для того чтобы проверить удаление правила запрета, выполните запрос на получение информации о правиле запрета, используя HTTP-метод GET.

Пример ввода команды с параметром GET

```
curl -k --example.cert --example.key -X GET
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-
B0391CF21EF3/settings?sensor_id=all&settings_type=prevention"| python -m
json.tool
```

Если правило запрета было удалено, то Kaspersky Anti Targeted Attack Platform возвращает ответ внешней системе в следующем формате:

```
{
   "error": "Not Found"
}
```

Возвращаемое значение

Код возврата	Описание
400	Ошибка ввода параметров.
401	Требуется авторизация.
404	Не найден указанный хост с компонентом Endpoint Agent.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Управление задачей запуска приложения

Для управления задачей запуска приложения с помощью интерфейса API рекомендуется использовать следующий сценарий взаимодействия с Kaspersky Anti Targeted Attack Platform:

a. **Создание запроса на получение информации о параметрах, времени создания и статусе выполнения задачи (см. раздел "Запрос на получение информации о задаче" на стр. 662)**

b. **Создание запроса на одну из следующих операций с задачей:**

- создание задачи (см. раздел "Запрос на создание задачи" на стр. 664);
- удаление задачи (см. раздел "Запрос на удаление задачи" на стр. 666).

Добавленные задачи отображаются в веб-интерфейсе приложения в разделе **Задачи**.

Запрос на получение информации о задаче

Для создания запроса на получение информации о задаче используется HTTP-метод GET.

Синтаксис команды

```
GET "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию 443>/kata/response_api/v1/<идентификатор external_system_id>/tasks/<идентификатор task_id>?settings=<true или false>"
```

При успешной обработке запроса отобразится информация о параметрах, времени создания и статусе выполнения задачи.

Параметры

Параметры	Тип	Описание
external_system_id	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
sensor_id	UUID	Уникальный идентификатор хоста с компонентом Endpoint Agent.
task_id	UUID	Уникальный идентификатор задачи.
settings	boolean	Может иметь следующие значения: • true. При указании этого значения отображается информация о параметрах, времени создания и статусе выполнения задачи. • false. При указании этого значения отображается информация о времени создания и статусе выполнения задачи.

Пример ввода команды с параметрами

```
GET https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/tasks/2EEB4CBC-10C6-4DC4-BE0A-72A75CDB0BE8?settings=<true или false>
```

Ответ

HTTP-код: 200

Формат: JSON

```
type Response struct {
   State                     `json:"state"`
   LatestStartDateTime       `json:"latestStartDateTime"`
 type Task struct {
 type Schedule struct {
   StartNow           boolean `json:"startNow"`
   ExecCommand        string  `json:"execCommand"`
}
}
}
```

Возвращаемое значение

Код возврата	Описание
400	Ошибка ввода параметров.
401	Требуется авторизация.
409	Задача с указанным идентификатором уже существует.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Запрос на создание задачи

Для создания запроса на запуск приложения Kaspersky Anti Targeted Attack Platform используется HTTP-метод POST. Параметры команды передаются в теле запроса в формате JSON.

Синтаксис команды

```
curl -k --<путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа>
-X POST "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор
external_system_id>/tasks/<идентификатор task_id>?sensor_id=<идентификатор
sensor_id>&task_type=run_process" -H 'Content-Type: application/json' -d '

{

"task": {

"shedule": {"startNow": <true или false>},
```

```
"execCommand": "<название приложения, которую вы хотите запустить>",

"cmdLineParameters": "<дополнительные параметры запуска файла или выполнения команды>",

"workingDirectory": "<рабочая директория>"

}

}

'
```

При успешной обработке запроса задача на запуск приложения будет создана.

Параметры

Параметр	Тип	Описание
external_system_id	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
sensor_id	UUID	Уникальный идентификатор хоста с компонентом Endpoint Agent.
task_id	UUID	Уникальный идентификатор задачи.

Пример ввода команды с параметрами

```
curl -k --example.cert --example.key -X POST
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-
B0391CF21EF3/tasks/2EEB4CBC-10C6-4DC4-BE0A-
72A75CDB0BE8?sensor_id=DF64838B-B518-414B-B769-
2B8BE341A2F0&task_type=run_process" -H 'Content-Type: application/json' -d
'

{

"task": {

"schedule": {"startNow": true},

"execCommand": "Example.exe",

"cmdLineParameters": "C:\Windows\System32\",

"workingDirectory": "/all"

}

}

'
```

Ответ

HTTP-код: 200

Формат: JSON

```
type Response struct {
   State                     `json:"state"`
   LatestStartDateTime       `json:"latestStartDateTime"`
 type Task struct {
 type Schedule struct {
   StartNow           boolean `json:"startNow"`
   ExecCommand        string  `json:"execCommand"`
}
}
}
```

Возвращаемое значение

Код возврата	Описание
400	Ошибка ввода параметров.
401	Требуется авторизация.
404	Задача с указанным идентификатором не найдена.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Если вы хотите изменить параметры созданной задачи, вам требуется создать новый запрос на добавление задачи с нужными параметрами.

Запрос на удаление задачи

Для создания запроса на удаление задачи Kaspersky Anti Targeted Attack Platform используется HTTP-метод DELETE.

Синтаксис команды

```
curl -k --<путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа>
-X DELETE "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор
external_system_id>/tasks/<идентификатор task_id>"
```

При успешной обработке запроса задача на запуск приложения будет удалена.

Параметры

Параметр	Тип	Описание
external_system_id	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
task_id	UUID	Уникальный идентификатор задачи.

Пример ввода команды с параметром DELETE

```
curl -k --example.cert --example.key -X DELETE
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-
B0391CF21EF3/tasks/2EEB4CBC-10C6-4DC4-BE0A-72A75CDB0BE8"
```

При успешной обработке запроса правило запрета будет удалено.

Для того чтобы проверить удаление задачи, выполните запрос на получение информации о задаче, используя HTTP-метод GET.

Пример ввода команды с параметром GET

```
curl -k --example.cert --example.key -X GET
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-
B0391CF21EF3/tasks/2EEB4CBC-10C6-4DC4-BE0A-
72A75CDB0BE8?settings=false"| python -m json.tool
```

Если задача была удалена, то Kaspersky Anti Targeted Attack Platform возвращает ответ внешней системе в следующем формате:

```
{
   "error": "Not Found"
}
```

Возвращаемое значение

Код возврата	Описание
400	Ошибка ввода параметров.
401	Требуется авторизация.
404	Задача с указанным идентификатором не найдена.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Действия после сбоя или неустранимой ошибки в работе программы

Приложение автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда приложение не может восстановить свою работу, вам требуется переустановить приложение или ее компонент. Вы также можете обратиться за помощью в Службу технической поддержки (см. раздел "Способы получения технической поддержки" на стр. 670).

Устранение уязвимостей и установка критических обновлений

Для сохранения бинарной целостности запрещается устанавливать обновления версии сертифицированного программного изделия, не прошедшие сертификационные испытания. Критические обновления, направленные на устранение уязвимостей, могут быть установлены в особом порядке до окончания сертификационных испытаний.

"Лаборатория Касперского" может выпускать обновления приложения, направленные на устранение уязвимостей и недостатков безопасности (критические обновления). Срочные пакеты обновлений публикуются на серверах автоматизированной установки обновлений "Лаборатории Касперского". Уведомления о выпуске критических обновлений публикуются на веб-сайте (https://support.kaspersky.ru/general/certificates) и рассылаются по адресам электронной почты, указанным при заказе приложения, а также подписчикам рассылки (подписаться на рассылку можно по ссылке: http://support.kaspersky.ru/subscribe).

Порядок получения критических обновлений изложен в формуляре.

Лицо, ответственное за эксплуатацию приложения, должно периодически (не реже одного раза в три месяца) проверять отсутствие обнаруженных уязвимостей в приложении, используя веб-сайт "Лаборатории Касперского" (https://support.kaspersky.ru/vulnerability), банк данных угроз безопасности информации ФСТЭК России (http://www.bdu.fstec.ru) и иные общедоступные источники.

Вы можете сообщать об обнаруженных недостатках безопасности или уязвимостях приложения следующими способами:

- По адресу электронной почты vulnerability@kaspersky.com.
- В сообществе пользователей "Лаборатории Касперского" (https://community.kaspersky.com/).

В Kaspersky Anti Targeted Attack Platform могут содержаться данные пользователей и другая конфиденциальная информация.
Администратору Kaspersky Anti Targeted Attack Platform необходимо обеспечить безопасность этих данных самостоятельно при создании резервной копии приложения, обновлении приложения, замене оборудования, на котором установлено приложение и в прочих случаях, когда может потребоваться удаление данных без возможности восстановления. Администратор Kaspersky Anti Targeted Attack Platform несет ответственность за доступ к данным, хранящимся на серверах Kaspersky Anti Targeted Attack Platform.

В случае сбоя приложения рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского" или переустановить Kaspersky Anti Targeted Attack Platform.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

Способы получения технической поддержки 670

Техническая поддержка через Kaspersky CompanyAccount 670

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о Kaspersky Anti Targeted Attack Platform, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Anti Targeted Attack Platform.

Kaspersky предоставляет поддержку Kaspersky Anti Targeted Attack Platform в течение жизненного цикла (см. страницу жизненного цикла приложений (https://support.kaspersky.com/corporate/lifecycle)). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules/ru_ru).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- посетить сайт Службы технической поддержки (https://support.kaspersky.ru/b2b);
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих приложения "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/faq/companyaccount_help).

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки приложения.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Adobe, Flash являются либо зарегистрированными товарными знаками, либо товарными знаками компании Adobe в США и/или других странах.

AMD – товарный знак или зарегистрированный товарный знак Advanced Micro Devices, Inc.

Apple, Mac, Macintosh, macOS и Safari – товарные знаки Apple Inc.

Ubuntu является зарегистрированным товарным знаком Canonical Ltd.

Snort является зарегистрированным товарным знаком или товарным знаком Cisco Systems, Inc. и/или ее аффилированных компаний в США и в определенных других странах.

Citrix – товарный знак Citrix Systems, Inc. и/или дочерних компаний, зарегистрированный в патентном офисе США и других стран.

Docker и логотип Docker являются товарными знаками или зарегистрированными товарными знаками компании Docker, Inc. в США и/или других странах. Docker, Inc. и другие стороны могут также иметь права на товарные знаки, описанные другими терминами, используемыми в настоящем документе.

Google, Google Chrome, Android – товарные знаки Google LLC.

Intel, Core и Xeon – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Active Directory, Excel, Internet Explorer, Microsoft Edge, PowerPoint, PowerShell, Win32, Windows и Windows Server, Windows XP являются товарными знаками группы компаний Microsoft.

Mozilla и Firefox являются товарными знаками Mozilla Foundation в США и других странах.

NVIDIA является зарегистрированным товарным знаком NVIDIA Corporation.

Java – зарегистрированный товарный знак компании Oracle и/или аффилированных компаний.

Python – товарный знак или зарегистрированный товарный знак Python Software Foundation.

CentOS – товарный знак или зарегистрированный в США и других странах товарный знак Red Hat, Inc. или дочерних компаний.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

VMware ESXi – товарный знак VMware, Inc. или зарегистрированный в США или других юрисдикциях товарный знак VMware, Inc.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

Приложение. Значения параметров приложения в сертифицированной конфигурации

Этот раздел содержит перечень параметров приложения, влияющих на сертифицированную конфигурацию приложения. В таблице ниже приведены значения этих параметров в сертифицированной конфигурации приложения.

Если вы меняете какие-либо из перечисленных значений параметров (диапазон значений) в сертифицированной конфигурации приложения на другие значения, вы выводите программу из сертифицированной конфигурации.

Таблица 51. Параметры и их значения при работе программы в сертифицированной конфигурации

Раздел и подраздел, к которому относится параметр	Название параметра	Значение параметра в сертифицированной конфигурации	Пользователи, которым доступно управление параметром
Параметры – Уведомления	**Добавить** (Добавить правило отправки уведомлений)	Требуется создать и включить правило отправки уведомлений о событиях обнаружения вторжений и нарушения безопасности.	**Администратор**, **Старший сотрудник службы безопасности**
Параметры – Уведомления	**Отключить** (Отключить правило отправки уведомлений)	Отключение правил отправки уведомлений может привести к выходу из сертифицированной конфигурации.	**Администратор**, **Старший сотрудник службы безопасности**
Параметры – Уведомления	**Удалить** (Отключить правило отправки уведомлений)	Удаление правил отправки уведомлений может привести к выходу из сертифицированной конфигурации.	
Параметры – Endpoint Agents	**Предупреждение** Количество дней бездействия Endpoint Agents, при котором приложение отображает предупреждение.	Установка значений, превышающих значение по умолчанию, может привести к выходу из сертифицированной конфигурации.	**Администратор**

Раздел и подраздел, к которому относится параметр	Название параметра	Значение параметра в сертифицированной конфигурации	Пользователи, которым доступно управление параметром
Параметры – Endpoint Agents	**Критическое бездействие (активность Endpoint Agents)** Количество дней бездействия Endpoint Agents, которое приложение отображает как критическое.	Установка значений, превышающих значение по умолчанию, может привести к выходу из сертифицированной конфигурации.	
Пользовательские правила – YARA	**Удалить**	Удаление правил YARA может привести к выходу из сертифицированной конфигурации.	**Старший сотрудник службы безопасности**
Информация о правиле TAA	**Добавить в исключения**	Добавление правил TAA (IOA) "Лаборатории Касперского" в исключения может привести к выходу из сертифицированной конфигурации.	**Старший сотрудник службы безопасности**