

Kaspersky Anti Targeted Attack Platform

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 3.0.0.253

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.

Дата редакции документа: 27.03.2018

Обозначение документа: **643.46856491.00086-03 90 01**

© АО "Лаборатория Касперского", 2017.

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

Содержание

Об этом руководстве	14
Условные обозначения.....	14
Источники информации о программе	16
Источники для самостоятельного поиска информации	16
Обсуждение программ "Лаборатории Касперского" на форуме.....	17
Kaspersky Anti Targeted Attack Platform	18
О Kaspersky Anti Targeted Attack Platform	18
Что нового.....	19
О ресурсе virustotal.com	20
О Kaspersky Threat Intelligence Portal	21
Инсталляционный комплект.....	21
Аппаратные и программные требования.....	21
Указания по эксплуатации и требования к среде	24
Безопасное состояние (сертифицированная конфигурация) программы	25
Лицензирование программы	26
О Лицензионном соглашении	26
О лицензии	26
О лицензионном сертификате	27
О ключе	27
О файле ключа	28
Просмотр информации о лицензии и добавленных ключах	28
Добавление ключа	29
Замена ключа	29
Удаление ключа	29
Режимы работы программы в соответствии с лицензией	30
Лицензирование операционных систем и программ, необходимых для работы компонента Sandbox	31
О предоставлении данных	33
Данные в журналах и файлах трассировки компонентов Central Node и Sensor	35
Данные в обнаружениях и событиях	38
Данные о политиках, задачах и фильтрах.....	43
Данные компонента Sandbox	44
Данные компонента Endpoint Sensors.....	44
Архитектура программы	49
Компонент Sensor	49
Компонент Central Node	50
Компонент Sandbox	50
Компонент Endpoint Sensors	51

Принцип работы программы	52
Интерфейс Kaspersky Anti Targeted Attack Platform	53
Типовые схемы развертывания и установки компонентов программы	54
Подготовка к установке компонентов программы	55
Подготовка IT-инфраструктуры к установке компонентов программы	55
Подготовка IT-инфраструктуры к интеграции с почтовым сервером для приема сообщений по протоколу POP3	56
Подготовка IT-инфраструктуры к интеграции с почтовым сервером для отправки сообщений по протоколу SMTP	57
Порядок установки и настройки компонентов программы	58
Установка компонента Sandbox	59
Шаг 1. Просмотр Лицензионного соглашения	59
Шаг 2. Выбор диска для установки компонента Sandbox	59
Шаг 3. Создание учетной записи администратора Sandbox	60
Шаг 4. Выбор управляющего сетевого интерфейса в списке	60
Шаг 5. Назначение адреса и маски сети управляющего интерфейса	61
Шаг 6. Настройка статического сетевого маршрута	61
Настройка компонента Sandbox через веб-интерфейс	62
Обновление баз компонента Sandbox	63
Запуск обновления баз вручную	63
Выбор источника обновления баз	63
Включение и отключение использования прокси-сервера для обновления баз	64
Настройка параметров соединения с прокси-сервером для обновления баз	64
Настройка соединения компонентов Sandbox и Central Node	64
Создание запроса на подключение к Sandbox в меню администратора Central Node	65
Обработка запросов на подключение от серверов Central Node в веб-интерфейсе Sandbox	66
Настройка сетевых интерфейсов компонента Sandbox	66
Настройка параметров DNS	66
Настройка параметров управляющего сетевого интерфейса	67
Настройка параметров сетевого интерфейса для доступа обрабатываемых объектов в интернет	67
Добавление, изменение и удаление статических сетевых маршрутов	68
Обновление системы Sandbox	69
Установка даты и времени системы Sandbox	70
Установка и настройка образов операционных систем и программ для работы компонента Sandbox	70
Загрузка ISO-образов операционных систем и программ для работы компонента Sandbox	71
Создание виртуальных машин с образами операционных систем и программ для работы компонента Sandbox	71
Активация операционных систем и программ для работы компонента Sandbox	72
Установка виртуальных машин с образами операционных систем и программ для работы компонента Sandbox	73
Удаление всех виртуальных машин, ожидающих установки	73
Установка максимального количества одновременно запускаемых виртуальных машин	74

Загрузка журнала системы Sandbox на жесткий диск	74
Экспорт параметров Sandbox	74
Импорт параметров Sandbox	75
Перезагрузка сервера Sandbox	76
Выключение сервера Sandbox	76
Изменение пароля учетной записи администратора Sandbox	76
Начало установки компонентов Central Node и Sensor	77
Шаг 1. Начало установки подготовленной среды для компонентов Central Node и Sensor	77
Шаг 2. Просмотр Лицензионного соглашения	77
Шаг 3. Установка подготовленной среды для компонентов Central Node и Sensor	78
Шаг 4. Начало установки компонентов Central Node и Sensor	78
Шаг 5. Просмотр Лицензионного соглашения	78
Шаг 6. Выбор диска для установки компонентов Central Node и Sensor	79
Шаг 7. Выбор роли сервера для установки компонентов Central Node и Sensor	79
Установка и настройка компонентов Central Node и Sensor на одном сервере	80
Шаг 1. Создание учетной записи для работы в меню администратора и в консоли управления сервером	81
Шаг 2. Назначение имени хоста	82
Шаг 3. Первоначальное включение сетевого интерфейса	82
Шаг 4. Настройка сетевого маршрута для использования по умолчанию	82
Настройка сетевого маршрута с помощью DHCP-сервера	82
Настройка статического сетевого маршрута	83
Шаг 5. Настройка параметров DNS	83
Назначение DNS-адресов с помощью DHCP-сервера	84
Назначение статических DNS-адресов	84
Шаг 6. Настройка параметров соединения с прокси-сервером	85
Включение и отключение использования прокси-сервера	85
Настройка параметров соединения с прокси-сервером	85
Включение и отключение использования прокси-сервера при подключении к локальным адресам	86
Шаг 7. Установка часового пояса	86
Шаг 8. Настройка синхронизации времени с NTP-сервером	87
Шаг 9. Указание адреса сервера с компонентом Sandbox	88
Шаг 10. Создание учетной записи администратора веб-интерфейса	88
Шаг 11. Выделение диска для базы данных компонента Targeted Attack Analyzer	89
Шаг 12. Настройка получения зеркалированного трафика со SPAN-портов	89
Шаг 13. Настройка интеграции с прокси-сервером по протоколу ICAP	90
Шаг 14. Настройка интеграции с почтовым сервером по протоколу POP3	90
Шаг 15. Настройка интеграции с почтовым сервером по протоколу SMTP	92
Шаг 16. Просмотр Положения о KSN и настройка участия в KSN	93
Участие в KSN	94
Отказ от участия в KSN	94

Установка и настройка компонента Central Node на отдельном сервере	95
Шаг 1. Создание учетной записи для работы в меню администратора и в консоли управления сервером.....	96
Шаг 2. Назначение имени хоста	97
Шаг 3. Первоначальное включение сетевого интерфейса	97
Шаг 4. Настройка сетевого маршрута для использования по умолчанию	97
Настройка сетевого маршрута с помощью DHCP-сервера	97
Настройка статического сетевого маршрута.....	98
Шаг 5. Настройка параметров DNS.....	98
Назначение DNS-адресов с помощью DHCP-сервера.....	99
Назначение статических DNS-адресов.....	99
Шаг 6. Настройка параметров соединения с прокси-сервером.....	100
Включение и отключение использования прокси-сервера	100
Настройка параметров соединения с прокси-сервером	100
Включение и отключение использования прокси-сервера при подключении к локальным адресам	101
Шаг 7. Установка часового пояса	101
Шаг 8. Настройка синхронизации времени с NTP-сервером.....	102
Шаг 9. Указание адреса сервера с компонентом Sandbox	103
Шаг 10. Создание учетной записи администратора веб-интерфейса	103
Шаг 11. Выделение диска для базы данных компонента Targeted Attack Analyzer	103
Шаг 12. Просмотр Положения о KSN и настройка участия в KSN	104
Участие в KSN.....	104
Отказ от участия в KSN.....	105
Установка и настройка компонента Sensor на отдельном сервере	106
Шаг 1. Создание учетной записи для работы в меню администратора и в консоли управления сервером.....	106
Шаг 2. Назначение имени хоста	107
Шаг 3. Первоначальное включение сетевого интерфейса	107
Шаг 4. Настройка сетевого маршрута для использования по умолчанию	108
Настройка сетевого маршрута с помощью DHCP-сервера	108
Настройка статического сетевого маршрута.....	108
Шаг 5. Настройка параметров DNS.....	109
Назначение DNS-адресов с помощью DHCP-сервера.....	109
Назначение статических DNS-адресов.....	109
Шаг 6. Настройка параметров соединения с прокси-сервером.....	110
Включение и отключение использования прокси-сервера при подключении к локальным адресам	110
Настройка параметров соединения с прокси-сервером	111
Шаг 7. Установка часового пояса	111
Шаг 8. Настройка синхронизации времени с NTP-сервером.....	112
Шаг 9. Указание адреса сервера с компонентом Central Node	113

Шаг 10. Настройка получения зеркалированного трафика со SPAN-портов	113
Шаг 11. Настройка интеграции с прокси-сервером по протоколу ICAP	114
Шаг 12. Настройка интеграции с почтовым сервером по протоколу POP3	114
Шаг 13. Настройка интеграции с почтовым сервером по протоколу SMTP	115
Шаг 14. Просмотр Положения о KSN и настройка участия в KSN	117
Участие в KSN	117
Отказ от участия в KSN	118
Настройка перенаправления трафика с компонентов Endpoint Sensors на компонент Sensor	119
Включение и отключение перенаправления трафика с компонентов Endpoint Sensors	119
Авторизация компонента Sensor на сервере с компонентом Central Node	120
Установка и удаление компонента Endpoint Sensors	122
Установка компонента Endpoint Sensors	122
Подготовка SSL-соединения к обмену данными между компонентами Endpoint Sensors и Central Node	123
Скачивание SSL-сертификата с сервера с компонентом Central Node	124
Создание SSL-сертификата на сервере с компонентом Central Node	124
Загрузка самостоятельно подготовленного SSL-сертификата на сервер с компонентом Central Node	125
Подготовка и загрузка SSL-сертификата в Active Directory	126
Удаление компонента Endpoint Sensors	128
Управление компонентами Endpoint Sensors в консоли администрирования Kaspersky Security Center ..	129
Создание установочного пакета Endpoint Sensors	129
Удаленная установка компонента Endpoint Sensors	131
Удаленное изменение параметров компонента Endpoint Sensors	132
Удаленная деинсталляция компонента Endpoint Sensors	134
Удаленный запуск и остановка компонента Endpoint Sensors	135
Создание политики для удаленного управления компонентом Endpoint Sensors	135
Изменение параметров политики для удаленного управления компонентом Endpoint Sensors	136
Получение данных от компонента Endpoint Sensors в консоли администрирования Kaspersky Security Center	138
Создание выборки компьютеров по наличию на них или свойствам компонентов Endpoint Sensors ..	138
Получение данных о состоянии компонента Endpoint Sensors на определенном компьютере	140
Начало работы с программой	141
Начало работы в веб-интерфейсе программы	141
Начало работы в меню администратора программы	141
Начало работы с программой в режиме Technical Support Mode	142
Настройка получения данных из KSN	144
Просмотр Положения о KSN	144
Настройка участия в KSN	145
Отказ от участия в KSN	145
Настройка получения данных из KPSN	147
Подготовка серверов к использованию KPSN	147

Настройка использования KPSN	148
Управление учетными записями администраторов и пользователей программы	149
Об учетных записях администраторов и пользователей программы	149
Создание учетной записи администратора для работы в меню администратора и в консоли серверов с компонентами программы	152
Создание учетной записи администратора веб-интерфейса при установке программы	153
Создание учетной записи администратора или пользователя веб-интерфейса программы	154
Включение и отключение учетной записи администратора или пользователя веб-интерфейса программы	155
Изменение пароля доступа к веб-интерфейсу программы учетной записи Administrator	155
Изменение пароля доступа к веб-интерфейсу программы учетной записи администратора или пользователя	156
Изменение пароля учетной записи администратора Sandbox	157
Проверка безопасности и работоспособности Kaspersky Anti Targeted Attack Platform	158
О журналах Kaspersky Anti Targeted Attack Platform	158
Просмотр журнала работоспособности сервера с компонентом Central Node	158
Просмотр журнала работоспособности сервера с компонентом Sandbox	159
Просмотр журнала аудита безопасности сервера с компонентом Central Node	160
Просмотр журнала аудита безопасности сервера с компонентом Sandbox	160
Проверка целостности файлов Kaspersky Anti Targeted Attack Platform	161
Проверка целостности значений параметров Kaspersky Anti Targeted Attack Platform	163
Ограничение размера проверяемых файлов	164
Мониторинг работы программы	165
О графиках и схемах расположения графиков	165
Создание новой схемы расположения графиков	166
Добавление графика на текущую схему расположения графиков	167
Перемещение графика на текущей схеме расположения графиков	167
Перемещение графика и создание новой схемы расположения графиков	168
Удаление графика с текущей схемы расположения графиков	168
Удаление графика и создание новой схемы расположения графиков	169
Выбор схемы расположения графиков из списка	169
Назначение схемы расположения графиков для использования по умолчанию	169
Переименование схемы расположения графиков	170
Удаление схемы расположения графиков	170
Сохранение схемы расположения графиков в PDF	170
Настройка периода отображения данных на графиках	171
Настройка размера отображения графиков на текущей схеме расположения графиков	172
Настройка размера отображения графиков и создание новой схемы расположения графиков	172
Основные принципы работы с графиками типа "Топ 10"	173
Основные принципы работы с графиками типа "Обнаружения"	173
Работа с графиками типа "Общая информация"	175
Мониторинг работоспособности модулей и компонентов программы	175

Мониторинг приема и обработки входящих данных.....	177
Мониторинг обработки данных модулями и компонентами программы	179
Таблица обнаружений	181
Фильтрация и поиск обнаружений.....	184
Фильтрация обнаружений по принадлежности группе.....	184
Фильтрация и поиск обнаружений по времени	185
Фильтрация обнаружений по степени важности.....	185
Фильтрация и поиск обнаружений по категориям обнаруженных объектов	186
Фильтрация и поиск обнаружений по полученной информации	187
Фильтрация и поиск обнаружений по адресу источника	187
Фильтрация и поиск обнаружений по названиям модулей и компонентов программы	188
Фильтрация и поиск обнаружений по состоянию их обработки пользователем	189
Быстрое создание фильтра обнаружений.....	190
Сохранение фильтра обнаружений	190
Изменение имени фильтра обнаружений	191
Создание фильтра обнаружений на основе существующего фильтра	191
Сброс фильтра обнаружений	192
Удаление фильтра обнаружений	192
Просмотр обнаружений	193
Просмотр информации об обнаружении	194
Общая информация об обнаружении	195
Информация в блоке Информация об объекте	195
Информация в блоке Информация об обнаружении	196
Информация в блоке Сетевое событие.....	196
Информация в блоке Результаты проверки.....	197
Информация в блоке Удаленные хосты	198
Информация о сетевой активности компьютера в блоке Процессы	198
Информация в блоке Данные учетной записи пользователя.....	199
Информация в блоке Модули, загруженные процессом	199
Информация в блоке История изменения обнаружения	200
Отправка данных об обнаружении.....	200
Действия пользователей над обнаружениями.....	202
Назначение обнаружения определенному пользователю.....	202
Назначение обнаружения себе	203
Отметка о завершении обработки обнаружения	203
Отметка о принадлежности обнаружения группе VIP	204
Добавление комментария к обнаружению	204
Сохранение списка всех обнаружений на жесткий диск компьютера	205
Информация о событиях.....	206
Просмотр таблицы событий.....	206
Просмотр информации о событии	208

Информация о запуске процесса	208
Информация об удаленном соединении	210
Информация о загрузке модуля	212
Информация о срабатывании запрета запуска файла	214
Информация о блокировании документа	216
Информация о создании файла	219
Информация о событии в журнале Windows	221
Информация об изменении в реестре	222
Информация о прослушивании порта	223
Информация о загрузке драйвера	224
Информация об изменении имени хоста	226
Поиск угроз по базе событий	227
Поиск событий с помощью режима конструктора	227
Поиск событий с помощью режима исходного кода	230
Изменение условий поиска событий	230
Скачивание файла с описанием событий на локальный компьютер	231
Импорт IOC-файла для поиска событий	231
Сохранение условия поиска событий	232
Работа с задачами	233
Просмотр таблицы задач	233
Просмотр информации о задаче	235
Создание задачи завершения процесса	235
Создание задачи выполнения программы	236
Создание задачи получения файла	237
Создание задачи удаления файла	238
Создание задачи помещения файла в Карантин	239
Создание задачи восстановления файла из Карантина	239
Создание копии задачи	240
Удаление задачи	240
Фильтрация задач по времени создания	240
Фильтрация задач по типу	241
Фильтрация задач на основе имени и пути к файлу	242
Фильтрация задач по описанию	242
Фильтрация задач по автору	243
Фильтрация задач по статусу	243
Фильтрация результатов выполнения задачи по имени хоста	244
Работа с политиками	246
Просмотр таблицы запретов	246
Просмотр информации о запрете	247
Создание запрета	248
Включение и отключение запрета	248

Удаление запрета	249
Фильтрация запретов по имени	249
Фильтрация запретов по хешу файла	249
ИОС-проверка событий	251
Просмотр таблицы ИОС-файлов	251
Просмотр информации об ИОС-файле	252
Загрузка ИОС-файла	253
Скачивание ИОС-файла на локальный компьютер	254
Включение и отключение использования ИОС-файла при проверке событий	254
Изменение ИОС-файла	255
Удаление ИОС-файла	255
Настройка расписания ИОС-проверки	256
Поиск результатов ИОС-проверки в базе обнаружений	256
Поиск результатов ИОС-проверки в базе событий	257
Фильтрация и поиск ИОС-файлов по степени важности	257
Фильтрация и поиск ИОС-файлов по имени файла	258
Фильтрация и поиск ИОС-файлов по их состоянию	258
Индикаторы компрометации на компьютерах с компонентом Endpoint Sensors	258
Работа с объектами в Хранилище	264
Просмотр таблицы объектов, помещенных в Хранилище	265
Скачивание объектов из Хранилища	266
Проверка объектов из Хранилища	266
Удаление объектов из Хранилища	267
Фильтрация объектов в Хранилище по типу	267
Фильтрация объектов в Хранилище по описанию	268
Фильтрация объектов в Хранилище по результатам проверки	268
Фильтрация объектов в Хранилище по IP-адресу или имени хоста	269
Фильтрация объектов по времени помещения в Хранилище	269
Управление компонентом Endpoint Sensors	271
Просмотр таблицы компьютеров с компонентом Endpoint Sensors	272
Просмотр информации о хосте	275
Фильтрация и поиск компьютеров с компонентом Endpoint Sensors по имени хоста	276
Фильтрация и поиск компьютеров с компонентом Endpoint Sensors по IP-адресу	277
Фильтрация и поиск компьютеров с компонентом Endpoint Sensors по версии операционной системы	278
Фильтрация и поиск компьютеров с компонентом Endpoint Sensors по версии Endpoint Sensor	279
Фильтрация и поиск компьютеров с компонентом Endpoint Sensors по их активности	279
Фильтрация и поиск компьютеров с компонентом Endpoint Sensors по имени сервера Central Node	280
Фильтрация и поиск компьютеров по типу установленного компонента Endpoint Sensors	281
Фильтрация и поиск компьютеров по состоянию компонента Endpoint Sensors	281
Фильтрация и поиск компьютеров с компонентом Endpoint Sensors по статусу хоста	282

Фильтрация и поиск компьютеров по наличию ошибок в работе компонента Endpoint Sensors	283
Быстрое создание фильтра компьютеров с компонентом Endpoint Sensors	283
Настройка показателей активности Endpoint Sensors	284
Работа с отчетами	285
Просмотр таблицы шаблонов и отчетов	285
Создание отчета	286
Просмотр отчета	286
Удаление отчета	287
Фильтрация отчетов по времени создания	287
Фильтрация отчетов по имени шаблона	287
Фильтрация отчетов по имени пользователя, создавшего отчет	288
Создание шаблона отчетов	288
Изменение шаблона отчетов	289
Удаление шаблона отчетов	290
Фильтрация шаблонов по имени шаблона	290
Фильтрация шаблонов по имени пользователя, создавшего шаблон	291
Фильтрация шаблонов по времени создания	291
Обновление баз программы	293
Об обновлении баз	293
Просмотр состояния обновления баз	294
Загрузка базы YARA-правил	294
Обновление базы YARA-правил	294
Удаление базы YARA-правил	295
Устранение уязвимостей и установка критических обновлений системы Kaspersky Anti Targeted Attack Platform	296
Работа с белым списком	299
Добавление записи в белый список	299
Удаление записи из белого списка	300
Изменение записи в белом списке	300
Импорт белого списка	301
Экспорт белого списка	301
Фильтрация и поиск записей в белом списке по типу правила	301
Фильтрация и поиск записей в белом списке по значению правил	302
Работа со списком адресов группы VIP	303
Добавление записи в список адресов группы VIP	303
Удаление записи из списка адресов группы VIP	304
Изменение записи в списке адресов группы VIP	304
Импорт списка адресов группы VIP	304
Экспорт списка адресов группы VIP	305
Фильтрация и поиск адресов группы VIP по типу правила	305
Фильтрация и поиск адресов группы VIP по значению правил	306

Фильтрация и поиск адресов группы VIP по описанию	306
Отправка уведомлений об обнаружениях	307
Состав данных, передаваемых в уведомлениях об обнаруженных событиях	307
Создание правила для отправки уведомлений	310
Включение и отключение правила для отправки уведомлений	311
Изменение правила для отправки уведомлений	311
Удаление правила для отправки уведомлений	312
Фильтрация и поиск правил отправки уведомлений по степени важности	312
Фильтрация и поиск правил отправки уведомлений по теме уведомлений	313
Фильтрация и поиск правил отправки уведомлений по их состоянию	313
Настройка интеграции с SIEM-системой	315
Включение и отключение записи событий в локальный журнал	315
Включение и отключение записи событий в удаленный журнал	316
Настройка основных параметров интеграции с SIEM-системой	316
Включение и отключение TLS-шифрования соединения с SIEM-системой	316
Загрузка TLS-сертификата	317
Содержание и свойства syslog-сообщений об обнаружениях	318
Настройка интеграции с почтовым сенсором	324
Обработка запроса на интеграцию от почтового сенсора	324
Удаление почтового сенсора из списка разрешенных к интеграции	325
Настройка приоритета обработки трафика от почтовых сенсоров	325
Настройка интеграции с Kaspersky Security Center	327
Включение и отключение интеграции с Kaspersky Security Center	328
Настройка параметров интеграции с Kaspersky Security Center	328
Работа с программой в режиме Technical Support Mode	329
Обращение в Службу технической поддержки	330
Способы получения технической поддержки	330
Техническая поддержка по телефону	330
Техническая поддержка через Kaspersky CompanyAccount	330
Глоссарий	332
АО "Лаборатория Касперского"	337
Информация о стороннем коде	339
Уведомления о товарных знаках	340
Соответствие терминов	341
Приложение. Значения параметров программы в сертифицированной конфигурации	342
Предметный указатель	344

Об этом руководстве

Этот документ представляет собой руководство администратора Kaspersky Anti Targeted Attack Platform. Руководство администратора адресовано специалистам, которые осуществляют установку и администрирование Kaspersky Anti Targeted Attack Platform, а также специалистам, которые осуществляют техническую поддержку организаций, использующих Kaspersky Anti Targeted Attack Platform.

В этом руководстве вы можете найти информацию о настройке и использовании Kaspersky Anti Targeted Attack Platform.

Также из этого руководства вы можете узнать об источниках информации о программе и способах получения технической поддержки.

Условные обозначения

В этом документе используются условные обозначения (см. таблицу ниже).

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание на то, что...	Предупреждения выделены красным цветом и заключены в рамку. Предупреждения содержат информацию о действиях, которые могут иметь нежелательные последствия.
Рекомендуется использовать...	Примечания заключены в рамку. Примечания содержат дополнительную и справочную информацию.
Пример: ...	Примеры приведены в блоках на голубом фоне под заголовком "Пример".
<i>Обновление</i> – это... Возникает событие <i>Базы</i> <i>устарели.</i>	Курсивом выделены следующие элементы текста: <ul style="list-style-type: none"> • новые термины; • названия статусов и событий программы.
Нажмите на клавишу ENTER . Нажмите комбинацию клавиш ALT+F4 .	Названия клавиш клавиатуры выделены полужирным шрифтом и прописными буквами. Названия клавиш, соединенные знаком + (плюс), означают комбинацию клавиш. Такие клавиши требуется нажимать одновременно.
Нажмите на кнопку Включить .	Названия элементов интерфейса программы, например, полей ввода, пунктов меню, кнопок, выделены полужирным шрифтом.

Пример текста	Описание условного обозначения
<p>► <i>Чтобы настроить расписание задачи, выполните следующие действия:</i></p>	<p>Вводные фразы инструкций выделены курсивом и значком "стрелка".</p>
<p>В командной строке введите текст <code>help</code></p> <p>Появится следующее сообщение:</p> <p>Укажите дату в формате ДД:ММ:ГГ.</p>	<p>Специальным стилем выделены следующие типы текста:</p> <ul style="list-style-type: none"> • текст командной строки; • текст сообщений, выводимых программой на экран; • данные, которые требуется ввести с клавиатуры.
<p><Имя пользователя></p>	<p>Переменные заключены в угловые скобки. Вместо переменной требуется подставить соответствующее ей значение, опустив угловые скобки.</p>

Источники информации о программе

Этот раздел содержит описание источников информации о программе.

Вы можете выбрать наиболее удобный источник информации в зависимости от важности и срочности вопроса.

В этом разделе

Источники для самостоятельного поиска информации	16
Обсуждение программ "Лаборатории Касперского" на форуме	17

Источники для самостоятельного поиска информации

Вы можете использовать следующие источники для самостоятельного поиска информации о программе:

- Страница на веб-сайте "Лаборатории Касперского".
- Справка веб-интерфейса программы.
- Документация.

Если вы не нашли решения возникшей проблемы самостоятельно, рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского" (https://support.kaspersky.ru/kata/about_kata).

Для использования источников информации на веб-сайте "Лаборатории Касперского" требуется подключение к интернету.

Страница на веб-сайте "Лаборатории Касперского"

Веб-сайт "Лаборатории Касперского" содержит отдельную страницу для каждой программы.

На странице (https://support.kaspersky.ru/kata/about_kata) программы вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Справка веб-интерфейса

Справка содержит информацию о том, как решать основные задачи пользователя через веб-интерфейс программы (далее также "веб-интерфейс").

Документация

В инсталляционный комплект программы включено Руководство администратора Kaspersky Anti Targeted Attack Platform. Руководство администратора программы содержит наиболее полную информацию о решении задач администратора программы.

Обсуждение программ "Лаборатории Касперского" на форуме

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями на нашем форуме (<https://forum.kaspersky.com>).

На форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

Kaspersky Anti Targeted Attack Platform

В этом разделе представлена общая информация о программе.

В этом разделе

О Kaspersky Anti Targeted Attack Platform	18
Что нового.....	19
О ресурсе virstotal.com	20
О Kaspersky Threat Intelligence Portal	21
Инсталляционный комплект.....	21
Аппаратные и программные требования.....	21
Указания по эксплуатации и требования к среде	24
Безопасное состояние (сертифицированная конфигурация) программы	25

О Kaspersky Anti Targeted Attack Platform

Kaspersky Anti Targeted Attack Platform – решение (далее также "программа"), предназначенное для защиты IT-инфраструктуры организации и своевременного обнаружения таких угроз, как, например, *атаки "нулевого дня"*, *целевые атаки* и сложные целевые атаки *advanced persistent threats* (далее также "APT").

Программа разработана для корпоративных пользователей и может интегрироваться в IT-инфраструктуру организации следующими способами:

- Интегрироваться в локальную сеть, получать и обрабатывать *зеркалированный трафик* и извлекать объекты и метаинформацию HTTP-, FTP-, SMTP- и DNS-протоколов, а также SMTP-протокола.
- Подключаться к прокси-серверу, получать и обрабатывать *ICAP-данные* HTTP- и FTP-трафика, а также HTTPS-трафика, если администратор настроил подмену SSL-сертификата на прокси-сервере.
- Подключаться к почтовому серверу и обрабатывать копии сообщений электронной почты, поступающие по протоколам POP3(S) и SMTP.
- Устанавливаться на отдельные компьютеры, входящие в IT-инфраструктуру организации и работающие под управлением операционной системы Microsoft® Windows®, осуществлять постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами. Вы можете настроить правила запрета запуска файлов в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.
- Интегрироваться с программой "Лаборатории Касперского" Kaspersky Secure Mail Gateway и обрабатывать копии сообщений электронной почты. Вы можете получить подробную информацию о Kaspersky Secure Mail Gateway из *Руководства администратора Kaspersky Secure Mail Gateway*.
- Интегрироваться с программой "Лаборатории Касперского" Kaspersky Private Security Network (далее также "KPSN"), чтобы получать доступ к репутационным базам Kaspersky Security Network, а также другим статистическим данным, не отправляя данные в Kaspersky Security Network со своих компьютеров. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

- Интегрироваться с программой "Лаборатории Касперского" Kaspersky Endpoint Security и наблюдать за процессами, открытыми сетевыми соединениями и изменяемыми файлами пользователей Kaspersky Endpoint Security в сети вашей организации. Вы можете получить подробную информацию о Kaspersky Endpoint Security из *Руководства администратора Kaspersky Endpoint Security*.
- Интегрироваться с программой "Лаборатории Касперского" Kaspersky Security Center версии 10 SP3. После интеграции доступны: удаленная установка, удаление, включение, отключение, а также мониторинг состояния работы компонента Endpoint Sensors на рабочих станциях сети. Добавлена возможность получения сведений о работе Endpoint Sensors как в интерфейсе KSC, так и в веб-интерфейсе Kaspersky Anti Targeted Attack Platform. Вы можете получить подробную информацию о Kaspersky Security Center из *Справки Kaspersky Security Center*.
- Интегрироваться с информационной системой "Лаборатории Касперского" Kaspersky Threat Intelligence Portal, которая содержит и отображает информацию о репутации файлов и URL-адресов.

Программа обнаруживает следующие события, происходящие внутри IT-инфраструктуры организации:

- На компьютер локальной сети организации был загружен файл или была предпринята попытка загрузки файла.
- На адрес электронной почты пользователя локальной сети организации был отправлен файл.
- На компьютере локальной сети организации была открыта ссылка на веб-сайт.
- IP-адрес или доменное имя компьютера локальной сети организации были замечены в сетевой активности.
- На компьютере локальной сети организации были запущены процессы.

Kaspersky Anti Targeted Attack Platform оценивает события и рекомендует пользователю обратить внимание на каждое обнаруженное событие (*обнаружение*) в соответствии с тем, какое влияние это обнаружение может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".

Пользователь Kaspersky Anti Targeted Attack Platform самостоятельно принимает решение о дальнейших действиях над обнаружениями.

Что нового

В Kaspersky Anti Targeted Attack Platform появились следующие возможности:

1. Решение Kaspersky Anti Targeted Attack Platform теперь включает в себя два функциональных блока:
 - Kaspersky Anti Targeted Attack (далее также "КАТА"), обеспечивающий периметральную защиту IT-инфраструктуры предприятия.
 - Kaspersky Endpoint Detection and Response (далее также "KEDR"), обеспечивающий защиту рабочих станций сети предприятия.

KEDR лицензируется отдельно от КАТА. Для активации этой функциональности вам нужно использовать отдельный ключ. Вы можете приобрести KEDR вместе с КАТА или отдельно от нее.
2. С функциональностью KEDR программу добавлены следующие возможности:
 - Создана система хранения событий с рабочих станций на сервере Central Node (например, запуск и завершение процессов, загрузка DLL, попытки соединения с удаленным хостом, отправка HTTP-запросов, создание файлов, события SuccessfulLogin и FailedLogin журнала событий)

Windows).

- Создан интерфейс для поиска и просмотра данных мониторинга рабочих станций. Реализована визуализация дерева событий, полученных с рабочих станций.
 - Создан интерфейс для реагирования на события, обнаруженные на рабочих станциях. Доступны следующие действия: Kill Process (завершить процесс), Delete File (удалить файл), Get File (получить файл с рабочей станции и отправить в Хранилище на сервере Central Node), Quarantine File (удалить файл на рабочей станции и отправить в Карантин на сервере Central Node), Restore File (восстановить файл из Карантина), Run Program (запустить программу).
 - Добавлена блокировка запуска исполняемых файлов и скриптов, открытия документов Microsoft Office на рабочих станциях с возможностью настроить правила блокировки на всех или выбранных рабочих станциях.
 - Добавлена проверка на наличие индикаторов компрометации (IOC-проверка) в базе событий, полученных с рабочих станций. Добавлена IOC-проверка непосредственно на рабочих станциях. Используется формат описания индикаторов компрометации OpenIOC.
3. Добавлена возможность получения файлов с рабочих станций. Полученные файлы помещаются в специальные хранилища – Хранилище и Карантин. Все файлы, помещенные в хранилища, по умолчанию проходят проверку технологиями AM, YARA и Sandbox.
 4. В веб-интерфейс программы добавлен раздел Отчеты, в котором вы можете создавать отчеты по обнаружениям в форме таблиц и графиков, а также настраивать их дизайн, например, для публикации отчетов на фирменном бланке вашей компании.
 5. Возможность интеграции Kaspersky Anti Targeted Attack Platform с программой "Лаборатории Касперского" Kaspersky Security Center (далее также "KSC") версии 10 SP3. После интеграции доступны: удаленная установка, удаление, включение, отключение, а также мониторинг состояния работы компонента Endpoint Sensors на рабочих станциях сети. Добавлена возможность получения сведений о работе Endpoint Sensors как в интерфейсе KSC, так и в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.
 6. Реализована возможность использовать сервер Sensor в качестве посредника (прокси) при передаче трафика между компонентом Endpoint Sensors и сервером Central Node.
 7. Добавлена поддержка CEF-формата файлов для интеграции с SIEM-системами. Реализован веб-интерфейс настройки параметров интеграции с SIEM-системами.
 8. Добавлена IDS-проверка сетевой активности файлов, запускаемых в Sandbox.
 9. Реализована визуализация дерева событий, обнаруженных в Sandbox.
 10. Реализована приоритетная очередь проверки почтового трафика с серверов программы "Лаборатории Касперского" Kaspersky Secure Mail Gateway (далее также "KSMG"), полученных с рабочих станций и размещенных в Хранилище сервера Central Node.
 11. Реализована возможность обновления баз на серверах Sensor и Sandbox с сервера Central Node.
 12. Реализована возможность обновления Kaspersky Anti Targeted Attack Platform с версии 2.0 до версии 3.0.

О ресурсе [virustotal.com](https://www.virustotal.com)

Для получения дополнительной информации о файлах, которые вы считаете подозрительными, вы можете перейти на веб-сайт стороннего открытого ресурса [virustotal.com](https://www.virustotal.com), который анализирует каждый файл на содержание в нем вредоносного кода и отображает информацию о репутации этого файла среди всех известных антивирусных программ.

Например, если файл заражен вирусом, на [virustotal.com](http://www.virustotal.com) (<http://www.virustotal.com>) отобразится список антивирусных программ и названия этого вируса, используемые различными антивирусными программами.

Если файл безопасен, на [virustotal.com](http://www.virustotal.com) (<http://www.virustotal.com>) отобразится список антивирусных программ и заключения этих антивирусных программ о безопасности файла.

"Лаборатория Касперского" не несет ответственности за отображение информации о репутации файлов ресурсом [virustotal.com](http://www.virustotal.com) (<http://www.virustotal.com>). Пользователь программы самостоятельно принимает решение о переходе на этот ресурс.

О Kaspersky Threat Intelligence Portal

Для получения дополнительной информации о файлах, которые вы считаете подозрительными, вы можете перейти на веб-сайт программы "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 программе Kaspersky Threat Intelligence предоставляется на платной основе. Для авторизации на веб-сайте программы на вашем компьютере в хранилище сертификатов должен быть установлен сертификат доступа к программе. Кроме того, у вас должны быть имя пользователя и пароль доступа к программе. Подробнее о программе Kaspersky Threat Intelligence Portal см. веб-сайт "Лаборатории Касперского".

Инсталляционный комплект

В инсталляционный комплект программы входят следующие файлы:

1. Образ диска (файл с расширением iso) с установочными файлами операционной системы CentOS 6.9 и компонентов Sensor, Central Node.
2. Образ диска (файл с расширением iso) с установочными файлами операционной системы CentOS 6.9 и компонента Sandbox.
3. Образы дисков (файлы с расширением iso) операционных систем Windows XP SP3, 32-разрядной Windows 7 и 64-разрядной Windows 7, в которых компонент Sandbox будет запускать файлы.
4. Установочный пакет компонента Endpoint Sensors (файл с расширением msi).
5. Лицензионное соглашение.
6. Файл с информацией о стороннем коде, используемом в Kaspersky Anti Targeted Attack Platform.

Аппаратные и программные требования

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

- Mozilla™ Firefox™ версии 50.
- Google Chrome™ для Windows версии 58.
- Google Chrome для Linux® версии 44.
- Microsoft Edge версии 41.
- Safari версии 5.1.10.

Серверы и компьютеры, на которые устанавливаются компоненты программы, должны удовлетворять перечисленным ниже требованиям.

Программные требования к компьютерам для установки компонента Endpoint Sensors

Одна из следующих операционных систем:

- Windows 7 x32, x64.
- Windows 8.1 x32, x64.
- Windows Server® 2008 R2 x64.
- Windows Server 2012 x64.
- Windows Server 2012 R2 x64.
- Windows 10.
- Windows Server 2016.

На компьютерах, на которые вы хотите установить компонент Endpoint Sensors, могут быть установлены другие антивирусные программы. Компонент Endpoint Sensors совместим со следующими антивирусными программами:

- McAfee® Endpoint Protection (кроме режима "максимальная защита").
- Symantec™ Endpoint Protection 12.1.
- Trend Micro™ OfficeScan Endpoint Security.
- Sophos Endpoint Protection.

Если на компьютерах, на которых будет устанавливаться компонент Endpoint Sensors, установлена антивирусная программа McAfee, в настройках параметров антивирусной программы McAfee необходимо отключить параметр Access Protection перед тем, как устанавливать компонент Endpoint Sensors.

Если на компьютерах, на которых будет устанавливаться компонент Endpoint Sensors, установлена программа RealTimes Desktop Service, рекомендуется ее удалить перед тем, как устанавливать компонент Endpoint Sensors.

У компонента Endpoint Sensors есть предустановленные параметры, которые определяют влияние компонента Endpoint Sensors на производительность локального компьютера в сценариях получения информации и взаимодействия с компонентом Central Node. При возникновении проблем с производительностью администратор Kaspersky Anti Targeted Attack Platform может изменить предустановленные параметры по рекомендации Службы технической поддержки "Лаборатории Касперского".

Аппаратные требования к компьютерам для установки компонента Endpoint Sensors

Минимальная конфигурация:

- Процессор:
 - Intel® Pentium® 1.0 ГГц или эквивалентный, если на компьютере установлена 32-разрядная операционная система Windows 7, Windows 8.1 или Windows Server.
 - Intel Pentium 2.0 ГГц или эквивалентный, если на компьютере установлена 64-разрядная операционная система Windows 7, Windows 8.1 или Windows Server.
- Объем оперативной памяти – 25 МБ.
- Дисковая подсистема – 1 ГБ свободного пространства.
- Один сетевой адаптер со скоростью передачи данных 1 Гбит/с.

При интеграции с программой "Лаборатории Касперского" Kaspersky Endpoint Security программа Kaspersky Anti Targeted Attack Platform имеет ограниченную функциональность, если на сервере с программой Kaspersky Endpoint Security установлена операционная система Windows Server 2008 SP2 x64.

Аппаратные требования к серверу для установки компонента Sandbox

Конфигурация сервера с компонентом Sandbox зависит от объема данных, обрабатываемых программой, от количества одновременно запускаемых виртуальных машин с образами операционных систем, а также от пропускной способности канала связи.

Минимальные аппаратные требования к серверу (пропускная способность канала связи 50 Мбит/сек.; 12 одновременно запускаемых виртуальных машин; 3500 файлов, обрабатываемых за одни сутки):

- Процессор Intel – с поддержкой VT-x и EPT, 8 ядер, 2.7 ГГц.

Процессоры AMD™ не поддерживаются.

- Объем оперативной памяти – 32 ГБ.
- Дисковая подсистема – 300 ГБ свободного пространства.
- Два сетевых адаптера со скоростью передачи данных по 1 Гбит/сек. каждый.

Рассчитывайте количество одновременно запускаемых виртуальных машин с образами операционных систем следующим образом: количество ядер процессора нужно умножить на 1,5. Для каждой виртуальной машины необходимо выделить по 1 ГБ оперативной памяти.

Аппаратные требования к серверу для установки компонента Central Node

Конфигурация сервера с компонентом Central Node зависит от объема данных, обрабатываемых программой и от пропускной способности канала связи.

Минимальные аппаратные требования к серверу (пропускная способность канала связи 50 Мбит/сек.; 1000 компьютеров с компонентом Endpoint Sensors):

- Процессор – 20 ядер, 2.7 ГГц.
- Объем оперативной памяти – 128 ГБ.
- Дисковая подсистема – два раздела: 2 ТБ свободного пространства для системного раздела и 4 ТБ свободного пространства для хранения данных компонента Targeted Attack Analyzer.
Рекомендуется использовать дисковый массив уровня RAID 0, 5, 10 или SSD-диск.
- Два сетевых адаптера со скоростью передачи данных по 1 Гбит/сек. каждый.

Аппаратные требования к серверу для установки компонента Sensor

Конфигурация сервера с компонентом Sensor зависит от объема данных, обрабатываемых программой, а также от пропускной способности канала связи.

Минимальные аппаратные требования к серверу (пропускная способность канала связи 50 Мбит/сек.; компонент обрабатывает зеркалированный трафик и сообщения электронной почты; скорость обработки составляет 120 сообщений в секунду):

- Процессор – 16 ядер, 2.7 ГГц.
- Объем оперативной памяти – 32 ГБ.
- Дисковая подсистема – 500 ГБ свободного пространства.
- Два сетевых адаптера со скоростью передачи данных по 1 Гбит/сек. каждый.

Указания по эксплуатации и требования к среде

При работе Kaspersky Anti Targeted Attack Platform должны выполняться следующие указания по эксплуатации и требования к среде:

1. Установка, настройка параметров и управление программой должны осуществляться в соответствии с эксплуатационной документацией.
2. Программа должна эксплуатироваться на компьютерах, отвечающих минимальным требованиям, приведенным в разделе Аппаратные и программные требования.
3. Должен быть обеспечен доступ программы ко всем объектам информационной системы, которые необходимы программе для реализации своих функциональных возможностей (к контролируемым объектам информационной системы).
4. Должна быть обеспечена совместимость программы с контролируемыми ресурсами

информационной системы.

5. Должна быть обеспечена возможность корректной совместной работы программы со средствами антивирусной защиты других производителей в случае их совместного использования в информационной системе.
6. Должна быть обеспечена физическая защита элементов информационной системы, на которых установлена программа.
7. Должна быть обеспечена синхронизация по времени между компонентами программы, а также между программой и средой ее функционирования.
8. Персонал, ответственный за функционирование программы, должен обеспечивать надлежащее функционирование программы, руководствуясь эксплуатационной документацией.
9. Должна быть обеспечена доверенная связь между программой и уполномоченными субъектами информационной системы (администраторами безопасности).
10. Функционирование программы должно осуществляться в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности программы.
11. Должен быть обеспечен доверенный канал получения обновлений БД ПКВ.
12. Должна быть обеспечена защищенная область для выполнения функций безопасности программы.
13. Управление атрибутами безопасности, связанными с доступом к функциям и данным программы, должно предоставляться только уполномоченным ролям (администраторам программы и информационной системы).
14. Администратор должен установить в среде ИТ максимальное число неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя с последующей блокировкой попыток аутентификации при превышении установленного значения.
15. 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.

Безопасное состояние (сертифицированная конфигурация) программы

Программа находится в безопасном состоянии (сертифицированной конфигурации), если параметры программы находятся в рамках допустимых значений, приведенных в приложении (см. стр. [342](#)) к этому документу.

Лицензирование программы

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием программы.

В этом разделе

О Лицензионном соглашении	26
О лицензии	26
О лицензионном сертификате	27
О ключе	27
О файле ключа	28
Просмотр информации о лицензии и добавленных ключах	28
Добавление ключа	29
Замена ключа	29
Удаление ключа	29
Режимы работы программы в соответствии с лицензией	30
Лицензирование операционных систем и программ, необходимых для работы компонента Sandbox.....	31

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать программу.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с программой.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки Kaspersky Anti Targeted Attack Platform.
- Прочитав документ license.txt. Этот документ включен в инсталляционный комплект программы.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы и не должны использовать программу.

О лицензии

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на основе Лицензионного соглашения.

Лицензия включает в себя право на получение следующих видов услуг:

- использование программы в соответствии с условиями Лицензионного соглашения;
- получение технической поддержки.

Объем предоставляемых услуг и срок использования программы зависят от типа лицензии, по которой была активирована программа.

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 программой и тестовых развертываний программы.
- Коммерческая – платная лицензия, предоставляемая при приобретении программы.

По истечении срока действия лицензии программа продолжает работу, но с ограниченной функциональностью (отключено обновление баз программы, недоступно соединение с базой знаний KSN). Чтобы использовать программу в режиме полной функциональности, вам нужно приобрести коммерческую лицензию или продлить срок действия коммерческой лицензии.

В текущей версии Kaspersky Anti Targeted Attack Platform функциональность программы также зависит от типа установленного ключа (см. раздел "О ключе" на стр. [27](#)).

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:

- номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о программе, которую можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать программу по предоставляемой лицензии);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

О ключе

Ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать программу в соответствии с условиями Лицензионного соглашения. Ключ создается специалистами "Лаборатории Касперского".

► *Чтобы добавить ключ в программу,*

загрузите файл ключа (см. раздел "Добавление ключа" на стр. [29](#)).

Ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если ключ заблокирован, для работы программы требуется добавить другой ключ.

В текущей версии Kaspersky Anti Targeted Attack Platform функциональность программы зависит от типа установленного ключа (см. стр. [29](#)):

- **Ключи KATA и KEDR.** Функциональность программы не ограничена.
- **Ключ KEDR.** Не выполняется прием и обработка данных из сетевого и почтового трафика.
- **Ключ KATA.** Ограничена функциональность разделов веб-интерфейса **Поиск угроз**, **Задачи**, **Политики**, **ИОС-проверка**, **Хранилище**, **Endpoint Sensors**. Нет возможности создавать и редактировать задачи, а также правила запрета запуска файлов. Нет возможности работать с событиями, выполнять ИОС-проверку объектов, просматривать результаты ИОС-проверки и осуществлять мониторинг работы компонента Endpoint Sensors.

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления ключа, активирующего программу.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения программы или после заказа пробной версии программы.


Чтобы активировать программу 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 в Службу технической поддержки "Лаборатории Касперского" (https://support.kaspersky.ru/kata/about_kata).

Просмотр информации о лицензии и добавленных ключах

► *Чтобы просмотреть информацию о лицензии и добавленных ключах,*


в нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Лицензия**.

В веб-интерфейсе отображается следующая информация о лицензии и добавленных ключах:

- буквенно-цифровая последовательность ключа;
- дата активации программы;
- дата окончания срока действия лицензии;
- количество дней до окончания срока действия лицензии.


Добавление ключа

► Чтобы добавить ключ, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **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 программу.


Замена ключа

► Чтобы заменить активный ключ программы другим ключом, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **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 программы.

Удаление ключа

► Чтобы удалить ключ, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **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 программы в соответствии с лицензией

В Kaspersky Anti Targeted Attack Platform предусмотрены различные режимы работы программы в зависимости от лицензии.

Без лицензии

В этом режиме программа работает с момента установки программы и запуска веб-интерфейса до тех пор, пока вы не добавите ключ (см. раздел "Добавление ключа" на стр. [29](#)).

В режиме Без лицензии программа не обновляет базы и не подключается к базе знаний Kaspersky Security Network.

Лицензия NFR

В этом режиме программа подключается к базе знаний Kaspersky Security Network и обновляет базы.

По истечении срока годности ключа для лицензии NFR программа прекращает обновление баз и не подключается к базе знаний Kaspersky Security Network.

Для возобновления работы программы необходимо добавить ключ для коммерческой лицензии (см. раздел "Добавление ключа" на стр. [29](#)).

Коммерческая лицензия

В этом режиме программа подключается к базе знаний Kaspersky Security Network и обновляет базы.

По истечении срока годности ключа для коммерческой лицензии программа прекращает обновление баз и не подключается к базе знаний Kaspersky Security Network.

Для возобновления работы программы необходимо заменить ключ (см. раздел "Замена ключа" на стр. [29](#)) или добавить новый ключ для коммерческой лицензии (см. раздел "Добавление ключа" на стр. [29](#)).

В текущей версии Kaspersky Anti Targeted Attack Platform функциональность программы также зависит от типа установленного ключа (см. стр. [29](#)):

- **Ключи КАТА и KEDR.** Функциональность программы не ограничена.
- **Ключ KEDR.** Не выполняется прием и обработка данных из сетевого и почтового трафика.
- **Ключ КАТА.** Ограничена функциональность разделов веб-интерфейса **Поиск угроз**, **Задачи**, **Политики**, **ИОС-проверка**, **Хранилище**, **Endpoint Sensors**. Нет возможности создавать и редактировать задачи, а также правила запрета запуска файлов. Нет возможности работать с событиями, выполнять ИОС-проверку объектов, просматривать результаты ИОС-проверки и осуществлять мониторинг работы компонента Endpoint Sensors.

Лицензирование операционных систем и программ, необходимых для работы компонента Sandbox

Kaspersky Anti Targeted Attack Platform использует операционные системы Microsoft Windows и программы Microsoft Office для работы компонента Sandbox (см. раздел "Компонент Sandbox" на стр. 50).

Ключи активации этих операционных систем Microsoft Windows и программ Microsoft Office не входят в инсталляционный комплект Kaspersky Anti Targeted Attack Platform. Вам нужно активировать эти операционные системы и программы с помощью своих ключей при установке Kaspersky Anti Targeted Attack Platform.

Необходимо активировать следующие операционные системы Microsoft Windows и программы Microsoft Office:

- 32-разрядную MICROSOFT WINDOWS 7 PROFESSIONAL SERVICE PACK 1.
- 64-разрядную MICROSOFT WINDOWS 7 PROFESSIONAL SERVICE PACK 1.
- 32-разрядную MICROSOFT WINDOWS XP PROFESSIONAL EDITION SERVICE PACK 3.
- MICROSOFT OFFICE 2010 DESKTOP APPLICATION SOFTWARE.
- MICROSOFT OFFICE 2007 DESKTOP APPLICATION SOFTWARE.
- MICROSOFT OFFICE 2003 DESKTOP APPLICATION SOFTWARE.

Рассчитывайте количество активаций при приобретении лицензий следующим образом:

- Количество активаций каждой из используемых версий Microsoft Windows должно быть равно максимальному количеству одновременно запускаемых виртуальных машин компонента Sandbox, деленному на 4.

32-разрядная MICROSOFT WINDOWS 7 PROFESSIONAL SERVICE PACK 1 и 64-разрядная MICROSOFT WINDOWS 7 PROFESSIONAL SERVICE PACK 1 лицензируются как одна версия Microsoft Windows.

- Количество активаций каждой из используемых версий Microsoft Office должно быть равно максимальному количеству одновременно запускаемых виртуальных машин компонента Sandbox.

Если вы увеличиваете количество виртуальных машин, вам нужно увеличить количество активаций.

Необходимо приобрести лицензии следующих типов:

- Volume License Key для активации:
 - 32-разрядную MICROSOFT WINDOWS XP PROFESSIONAL EDITION SERVICE PACK 3;
 - программы MICROSOFT OFFICE 2007 DESKTOP APPLICATION SOFTWARE;
 - программы MICROSOFT OFFICE 2003 DESKTOP APPLICATION SOFTWARE.
- Multiple Activation Key (MAK) для активации:
 - 32-разрядной операционной системы MICROSOFT WINDOWS 7 PROFESSIONAL SERVICE PACK 1;
 - 64-разрядной операционной системы MICROSOFT WINDOWS 7 PROFESSIONAL SERVICE PACK 1;

- программы MICROSOFT OFFICE 2010 DESKTOP APPLICATION SOFTWARE.

Вы можете ознакомиться с условиями лицензионных соглашений операционных систем и программ, необходимых для работы компонента Sandbox, при создании виртуальных машин в веб-интерфейсе Sandbox (см. раздел "Создание виртуальных машин с образами операционных систем и программ для работы компонента Sandbox" на стр. [71](#)).

О предоставлении 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 программы).

Согласно условиям Лицензионного соглашения, вы соглашаетесь в автоматическом режиме предоставлять "Лаборатории Касперского" информацию, перечисленную в Лицензионном соглашении (см. раздел "О Лицензионном соглашении" на стр. [26](#)) в пункте Предоставление информации. Лицензионное соглашение входит в инсталляционный комплект программы.

- В Положении о KSN (например, при установке программы или в меню администратора программы 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 инсталляционный комплект программы.

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".

"Лаборатория Касперского" использует полученную информацию только в обезличенном виде и в виде данных общей статистики. Данные общей статистики формируются автоматически из исходной полученной информации и не содержат персональных и иных конфиденциальных данных. Исходная полученная информация уничтожается по мере накопления (один раз в год). Данные общей статистики хранятся бессрочно.

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 программой Kaspersky Private Security Network находится за пределами вашей организации. Администратору Kaspersky Private Security Network необходимо обеспечить безопасность этих данных самостоятельно.

Работа с Kaspersky Anti Targeted Attack Platform из консоли управления в режиме Technical Support Mode (см. стр. [329](#)) с правами учетной записи суперпользователя позволяет выполнять следующие действия:

- управлять параметрами журнала трассировки;
- управлять параметрами записи файлов дампов;
- управлять параметрами работы программы с помощью конфигурационных файлов. При этом могут быть изменены параметры шифрования данных при передаче между узлами программы, параметры хранения и обработки объектов проверки.

В файлах дампов могут содержаться следующие данные пользователя:

- Пути к файлам, которые находятся на компьютере с компонентом Endpoint Sensors.
- Сообщения электронной почты: тело сообщения, вложения, адреса электронной почты отправителя и получателей сообщения, IP-адрес отправителя сообщения, информация, содержащаяся в служебных заголовках сообщения, идентификатор сообщения электронной почты.
- Содержимое файлов, дампов, карт памяти процессов.
- URL-адрес:
 - извлеченный из сообщения электронной почты;
 - с которого был скачан файл;
 - по которому пользователь совершил переход.
- Имя учетной записи пользователя, IP-адрес и имя компьютера пользователя.
- MachineID компьютера пользователя.
- UID компьютера пользователя в KSC.
- Уникальный идентификатор компьютера от компонента Endpoint Sensors.
- MAC-адрес компьютера пользователя.

Файлы дампов и журналов могут содержать конфиденциальные данные пользователя. По умолчанию формирование дампов в Kaspersky Anti Targeted Attack Platform отключено.

Администратору Kaspersky Anti Targeted Attack Platform необходимо обеспечить безопасность серверов Kaspersky Anti Targeted Attack Platform с перечисленными выше данными самостоятельно. Администратор Kaspersky Anti Targeted Attack Platform несет ответственность за доступ к данной информации.

В этом разделе

Данные в журналах и файлах трассировки компонентов Central Node и Sensor	35
Данные в обнаружениях и событиях	38
Данные о политиках, задачах и фильтрах	43
Данные компонента Sandbox	44
Данные компонента Endpoint Sensors	44

Данные в журналах и файлах трассировки компонентов Central Node и Sensor

Kaspersky Anti Targeted Attack Platform ведет запись в журналы действий пользователей, а также различных действий компонентов программы. В журналы могут попадать все данные, отображаемые в информации об обнаружениях, политиках, событиях, задачах и результатах их выполнения.

Данные на сервере Central Node хранятся в открытом незашифрованном виде и ротируются при достижении максимально разрешенного размера файла. Данные в журналах хранятся за последние 7 дней и безвозвратно удаляются при удалении программы.

Администратору Kaspersky Anti Targeted Attack Platform необходимо обеспечить безопасность этих данных самостоятельно.

Kaspersky Anti Targeted Attack Platform записывает данные в следующие журналы:

1. Журнал истории обработки. Хранится в папках \var\log\apt-history.log на серверах Central Node и Sensor. Ведется запись в журнал этапов обработки объектов, фактов внесения изменений в параметры, задач и запретов для последующего использования в разборе проблем, улучшения качества программы. Ниже перечислены данные, которые записываются в журнал истории обработки.
 - a. Факт отправки файла на проверку:
 - MD5-хеш файла.
 - Дата обработки файла.
 - Результат проверки.
 - Версия баз, с помощью которых проверялся файл.
 - Ядро, которое участвовало в проверке файла.
 - b. Факт обработки файла или URL-адреса по белому списку:
 - Имя, тип, размер файла, путь к файлу, MD5-, SHA256-хеш файла, URL-адрес, с которого был скачан файл.
 - URL-адрес.
 - Правило белого списка.
 - IP-адрес и порт компьютера, который установил соединение (клиент).
 - IP-адрес и порт компьютера, с которым было установлено соединение (сервер).
 - Тип HTTP-запроса (GET, POST).
 - Дата и время запроса (с точностью до секунды).
 - User Agent (данные о браузере) клиента.
 - Referrer.
 - Тип DNS-сообщения (request, response).
 - Тип DNS-запроса (A, MX).

- Дата и время DNS-сообщения (с точностью до секунды).
 - Список всех IP-серверов (для DNS-ответа A-записи).
 - Список всех доменных имен почтовых серверов, а также все IP-адреса, относящиеся к A-записи, извлеченные из секции Additional (для DNS-ответа MX записи).
 - Значение сработавшего правила белого списка: адрес электронной почты, IP-адрес, домен, тип файла, MD5-хеш файла.
- c. Факт обработки сообщения электронной почты по белому списку:
- Информация о сообщении: адреса электронной почты отправителя и получателей сообщения.
 - Тема сообщения.
- d. Факт создания обнаружения.
- Важность обнаружения.
 - Дата и время, когда обнаружено событие.
 - Модули и технологии, которыми проверялся файл.
 - Результаты проверки модулями и технологиями.
 - MD5-хеш проверенного файла.
 - Проверенный URL-адрес.
- e. Создание задач для компьютеров с компонентом Endpoint Sensors:
- Идентификатор задачи, время создания, таймаут выполнения задачи, тип задачи.
 - IP-адрес, имя хоста, которому назначена задача.
 - Параметры процесса, для которого запрашивается карта памяти.
 - Параметры процесса, для которого запрашивается дамп.
 - Список запрашиваемых областей памяти.
 - Имя, путь к запрашиваемому файлу, MD5-хеш запрашиваемого файла.
 - Приоритет выполнения задачи.
- f. Обработка результатов выполнения задач для компьютеров с компонентом Endpoint Sensors:
- Путь временного файла пакета от компьютера с компонентом Endpoint Sensors, размер пакета.
 - Имя хоста и IP-адрес компьютера с компонентом Endpoint Sensors.
 - Версия отчета от компьютера с компонентом Endpoint Sensors.
 - Информация о результатах проверки файла.
 - Идентификатор процесса, количество областей памяти.
 - Признак успешной обработки задачи.
 - Описание ошибки, возникшей при обработке задач компьютера с компонентом Endpoint Sensors. В описании ошибки, помимо технической информации, могут содержаться следующие данные пользователя:
 - Пути к файлам, которые находятся на компьютере с компонентом Endpoint Sensors.

- Сообщения электронной почты: тело сообщения, вложения, адреса электронной почты отправителя и получателей сообщения, IP-адрес отправителя сообщения, информация, содержащаяся в служебных заголовках сообщения, идентификатор сообщения электронной почты.
 - Содержимое файлов, дампов, карт памяти процессов.
 - URL-адреса, извлеченные из сообщения электронной почты, с которых был скачан файл или по которым пользователь совершил переход.
 - Имя учетной записи пользователя, IP-адрес и имя компьютера пользователя.
 - MachineID компьютера пользователя.
 - UID компьютера пользователя в KSC.
 - Уникальный идентификатор компьютера от компонента Endpoint Sensors.
 - MAC-адрес компьютера пользователя.
- г. Работа с политиками:
- Идентификатор запрета, дата и время внесения изменений в запрет.
 - MD5- или SHA256-хеш файла.
 - Уникальный идентификатор компьютера от компонента Endpoint Sensors.
 - Имя запрета.
 - MachineID хоста.
2. Журнал аудита. Хранится в папках `\var\log\apt-audit.log` на серверах Central Node и Sensor. Ведется запись в журнал действий с учетными записями, параметрами, запись изменений статусов работоспособности компонентов программы для последующего использования в разборе проблем. Ниже перечислены данные, которые записываются в журнал аудита.
- а. Факт внесения изменений в белый список:
- Имя учетной записи пользователя.
 - Значение элемента белого списка: MD5-хеш, формат, маска URL-адреса, подсеть, User Agent (данные о браузере), адрес электронной почты.
- б. Статусы компонентов защиты системы:
- Время, название компонента, IP-адрес, статус, описание ошибки.
 - Статус обновления баз.
- с. Действия с учетными записями пользователей:
- Тип события (создание, изменение, удаление).
 - Дата и время.
 - Имя учетной записи пользователя.
 - IP-адрес компьютера пользователя.
 - Роль пользователя.
 - Статус пользователя (активный/работа пользователя приостановлена);
 - Имя учетной записи пользователя, внесшего изменения.
- д. Изменение записей группы VIP:

- Тип события.
 - Дата и время.
 - Имя пользователя, создавшего или изменившего запись группы VIP.
 - IP-адрес, FQDN-имя компьютера, адрес электронной почты.
- e. Действия с обнаружениями:
- Идентификатор обнаружения.
 - Имя учетной записи пользователя, выполнившего действие с обнаружением.
3. Системный журнал и файлы трассировки хранятся на серверах Central Node и Sensor. Системный журнал хранится в папке `\var\log`. Файлы трассировки хранятся в папке `\var\log\kaspersky`.

В файлах трассировки в открытом (незашифрованном) виде могут сохраняться те же данные, которые входят в состав данных об обнаружениях, политиках, событиях, задачах и результатах их выполнения. Вы можете настроить запись файлов трассировки в syslog (в режиме Technical Support Mode).

В системный журнал пишется общая информация о состоянии программы, а также возникших ошибках и исключениях в работе различных компонентов программы (в том числе стороннего производителя) и операционной системы.

Помимо данных об обнаружениях, политиках, событиях, задачах и результатах их выполнения, в файлах трассировки и в системных журналах могут содержаться следующие данные пользователя:

- a. Пути к файлам, которые находятся на локальном компьютере.
- b. Сообщения электронной почты: тело сообщения, вложения, адреса электронной почты отправителя и получателей сообщения, IP-адрес отправителя сообщения, информация, содержащаяся в служебных заголовках сообщения, идентификатор сообщения.
- c. Содержимое файлов, дампов, карт памяти процессов.
- d. URL-адрес:
 - извлеченный из сообщения электронной почты;
 - с которого был скачан файл;
 - по которому пользователь совершил переход.
- e. Имя учетной записи пользователя, IP-адрес и имя компьютера пользователя.
- f. MachineID компьютера пользователя.
- g. UID компьютера пользователя в KSC.
- h. Уникальный идентификатор компьютера от компонента Endpoint Sensors.
- i. MAC-адрес компьютера пользователя.

Данные в обнаружениях и событиях

Данные пользователя могут содержаться в обнаружениях и событиях. Пользователь Kaspersky Anti Targeted Attack Platform может просматривать обнаружения и события через веб-интерфейс и отправлять уведомления об обнаружениях (см. раздел "Отправка уведомлений об обнаружениях" на стр. [307](#)). Информация об обнаружениях хранится в Хранилище на сервере с компонентом Central Node и ротируется по мере заполнения дискового пространства. Файлы, по результатам проверки которых возникло обнаружение, накапливаются на сервере с компонентом Central Node и ротируются по мере заполнения

дискового пространства.

Если обнаружен файл в сетевом или почтовом трафике, в Хранилище может содержаться следующая информация:

- Имя, размер, тип файла.
- MD5-, SHA256-хеш файла.
- Категория обнаруженного объекта (например, название вируса), 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".
- Версии баз компонентов Kaspersky Anti Targeted Attack Platform, с помощью которых было выполнено обнаружение.
- Для каждой виртуальной машины компонента Sandbox: имя виртуальной машины, версия баз компонента Sandbox, с помощью которых был проверен файл, журнал исследования поведения файла.
- Названия YARA-правил, с помощью которых было выполнено обнаружение.
- Статус проверки объекта технологиями и время проверки каждой технологией.
- IP-адрес и тип интеграции сервера, на котором произошло обнаружение.
- Для IDS-обнаружения: адрес источника, адрес назначения, URL-адрес, User Agent, метод.
- Если файл получен от компонента Endpoint Sensors: IP-адрес, имя, домен хоста (в формате FQDN), полный путь к файлу на компьютере с компонентом Endpoint Sensors и имя файла.
- Принадлежность группе VIP.

Если обнаружено сообщение электронной почты, в Хранилище может содержаться следующая информация:

- 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.
- Уникальный идентификатор сообщения электронной почты.
- Все служебные заголовки сообщения (так, как они выглядят в сообщении).
- IP-адрес и тип интеграции сервера, на котором обнаружено сообщение электронной почты.

Если обнаружение выполнено технологией URL Reputation, в Хранилище может содержаться следующая информация:

- URL-адрес, к которому обращался компьютер локальной сети организации, или доменное имя из DNS-запроса.
- URL-адрес, извлеченный из сообщения электронной почты, до нормализации.
- Категория обнаруженного объекта (например, вредоносный или фишинговый URL-адрес), важность обнаружения для пользователя Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние это событие может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского", имена обнаруженных АРТ-атак.

- Принадлежность группе VIP.

Если обнаружение выполнено технологией Intrusion Detection System, в Хранилище может содержаться следующая информация:

- Идентификатор правила IDS.
- Категория обнаруженного объекта по версии баз Intrusion Detection System.
- Категория обнаруженного объекта по классификации "Лаборатории Касперского".
- Версия баз Intrusion Detection System, с помощью которых было выполнено обнаружение.
- 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".
- Файл с трафиком, в котором произошло обнаружение.
- URL-адрес, извлеченный из файла с трафиком, User Agent, метод.
- IP-адрес и тип интеграции сервера, на котором произошло обнаружение.
- Принадлежность группе VIP.

Если обнаружение выполнено Targeted Attack Analyzer, в Хранилище может содержаться следующая информация:

- Имя хоста, имя пользователя, время выполнения обнаружения, имя обнаруженного объекта.
- Имя, владелец домена, дата регистрации домена, название организации, зарегистрировавшей домен.
- Популярность домена в мире.
- Дата и время обнаружения хоста, количество обращений к хосту.
- Объем данных, загруженных с компьютера локальной сети на этот хост.
- Информация о файле процесса: путь к файлу процесса; компания, выпустившая программу, к которой относится процесс; версия программы; размер и версия файла, MD5-, SHA256-хеш файла; автор сертификата, в котором содержится цифровая подпись к обнаруженному файлу, действительна ли подпись.
- Дата и время обнаружения процесса в локальной сети; количество раз, которое этот процесс был обнаружен в локальной сети; количество компьютеров, на которых был обнаружен подобный процесс.
- Популярность файла, запустившего процесс, в мире; популярность пути, по которому был загружен процесс, в мире.
- Имена DLL-библиотек, на которые пользователю Kaspersky Anti Targeted Attack Platform рекомендуется обратить внимание, журнал DLL-активности.
- Тип учетной записи, тип входа в компьютер; дата и время, когда учетная запись была впервые обнаружена в локальной сети; дата и время, когда учетная запись была впервые обнаружена на компьютере; количество компьютеров, на которых была обнаружена учетная запись.
- Журнал HTTP-запросов и ответов для обнаруженных процессов и доменов: каждый час данные по каждой паре процесс-домен (время, удаленный хост, путь к файлу процесса, количество запросов, объем запросов, объем ответов); в рамках каждого часа точный журнал (индивидуальные HTTP-запросы и ответы (IP-адрес и порт источника; IP-адрес, порт, название адресата, длина тела и заголовка запроса, длина тела и заголовка ответа, время запроса, URI, имя удаленного хоста, User

Agent, метод); заголовок и тело запроса и ответа для конкретной пары запрос – ответ.

- Журнал Process Activity для процессов, участвовавших в обнаружении: каждый час данные о количестве запусков в час по каждому из процессов, перечисленных в блоке **Процессы**; в рамках каждого часа информация о времени каждого запуска и связанной команде; для каждого запуска путь к файлу, MD5-, SHA256-хеш файла; путь к родительскому файлу, MD5-, SHA256-хеш родительского файла, имя, роль и домен учетной записи, тип входа в компьютер, команда, время запуска и завершения процесса.
- Информация об обнаружении в дампе соответствующего процесса.
- Принадлежность группе VIP.

Если выполнено комплексное обнаружение, в Хранилище может содержаться следующая информация:

- Уникальный идентификатор обнаружения.
- Дата и время выполнения обнаружения.
- Список обнаружений, входящих в комплексное обнаружение. Для каждого обнаружения: дата и время, важность, принадлежность группе VIP, адрес источника, адрес назначения, описание, почему обнаружение вошло в комплексное обнаружение.

Если событие произошло на компьютере пользователя, компонент Endpoint Sensors отправляет следующие данные в базу событий:

1. 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.
 - Поля заголовка события: ProviderName, EventId, Version, Level, Task, Opcode, Keywords, TimeCreatedSystemTime, EventRecordId, CorellationActivityId, ExecutionProcessID, ThreadID, Channel, Computer.
 - Поля тела события: AccessList, AccessMask, 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, PrivilegeList, 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.
2. Событие мониторинга реестра.
 - Сведения о процессе, изменившем реестр: ID процесса, имя файла процесса, MD5-, SHA256-хеш файла процесса.
 - Путь к ключу в реестре.
 - Имя переменной реестра.
 - Данные переменной реестра.
 3. Событие загрузки драйвера.
 - Имя файла.
 - Путь к файлу.
 - Полное имя файла.
 - MD5-, SHA256-хеш файла.
 - Размер файла.
 - Дата создания и изменения файла.
 4. 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.
 5. Событие в журнале Windows.
 - 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.
 6. Событие запуска процесса.
 - Сведения о файле, запустившем процесс: имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, размер файла, дата создания и изменения файла.
 - UniquePID.
 - Параметры командной строки.
 - Сведения о родительском процессе: UniquePID, Windows ID процесса, MD5-, SHA256-хеш файла процесса.

- Время окончания работы процесса.
7. Событие загрузки модуля.
- Сведения о файле, запустившем процесс: UniquePID, имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, размер файла.
 - Имя файла DLL.
 - Путь к файлу DLL.
 - Полное имя файла DLL.
 - MD5-, SHA256-хеш файла DLL.
 - Размер файла DLL.
 - Дата создания и изменения файла DLL.
8. 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.
9. 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.
10. Событие смены имени хоста.
- Время события.
 - Старое имя хоста.
 - Новое имя хоста.

Данные о политиках, задачах и фильтрах

Данные о политиках и задачах хранятся на сервере Central Node в незашифрованном виде.

Данные о политиках:

- MD5-, SHA256-хеш файла, который запрещен к запуску.
- Комментарий.
- Хосты, на которых запрещен запуск файла.
- Состояние запрета.

Данные о задачах:

- Идентификатор задачи.

- Время создания задачи.
- Имя хоста, которому назначена задача.
- Максимальное время выполнения задачи.
- Приоритет выполнения задачи.
- Путь к файлу (для задач получения и удаления файла, помещения файла в Хранилище, завершения процесса).
- От чьего имени требуется выполнить программу.
- Выполнить команду или запустить файл.
- Путь к файлу, аргументы или командная строка.
- Рабочий каталог.
- Путь к ключу реестра.

По результатам выполнения задачи формируется отчет, который хранится на сервере с компонентом Central Node. Отчет может содержать карту памяти, дампы или файлы.

Запрошенные файлы хранятся в Хранилище на сервере с компонентом Central Node в незашифрованном виде. Данные в Хранилище ротируются по мере заполнения дискового пространства.

Для пользователя с ограниченными правами, от имени которого работают компоненты программы, доступ к содержимому Хранилища на сервере с компонентом Central Node ограничен системными средствами на чтение и запись.

Запрошенные карты памяти и дампы сохраняются в базе данных программы.

Данные о фильтрах, созданных в веб-интерфейсе программы, сохраняются в Хранилище на сервере с компонентом Central Node.

Данные компонента 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.

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 владелец сервера в режиме Technical Support Mode.

Проверенный файл удаляется специальным скриптом по таймеру. По умолчанию один раз в 60 минут.

Данные пользователя могут содержаться в результатах работы компонента Sandbox после выполнения проверки. На сервере с компонентом Sandbox сохраняются только имена файлов и URL-адреса, отправленные на анализ.

Данные компонента Endpoint Sensors

Компонент Endpoint Sensors отправляет на компонент Central Node отчеты о выполнении задач, информацию о событиях и обнаружениях, произошедших на компьютерах с компонентом Endpoint Sensors, а также информацию о терминальных сессиях.

Перед отправкой на компонент Central Node отчеты, а также сопутствующие файлы временно сохраняются

на жестком диске компьютера с компонентом Endpoint Sensors. Отчеты о выполнении задач сохраняются в архивированном незашифрованном виде в папке ProgramData\Kaspersky Lab\Endpoint Sensor 3.1\Data\E7D729FA-47C4-4A16-BCA6-D238A6A3622B. Файлы с отчетами доступны для чтения любому пользователю, имеющему доступ на чтение к файлам в данном каталоге. При включенной самозащите у пользователей есть доступ только на чтение. При выключенной самозащите пользователи с правами учетной записи операционной системы System и Administrator могут также удалять файлы, изменять их содержимое и изменять права доступа к ним.

При выполнении задачи помещения файла в Карантин архив, содержащий этот файл, временно сохраняется в незашифрованном виде в папке C:\Windows\Temp. Компонент Endpoint Sensors не управляет правами доступа к данной папке и ее файлам. Доступ определяет системный администратор.

При выполнении задачи запуска программы на хосте компонент Endpoint Sensors локально хранит содержимое стандартных потоков вывода и ошибок запущенного процесса в открытом незашифрованном виде в папке C:\Windows\Temp до тех пор, пока отчет о выполнении задачи не будет отправлен на компонент Central Node. Компонент Endpoint Sensors не управляет правами доступа к данной папке и ее файлам. Доступ определяет системный администратор.

При выполнении запроса о предоставлении дампов процесса компонент Endpoint Sensors локально хранит содержимое дампов процесса в открытом незашифрованном виде в папке C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.1\Data до тех пор, пока отчет о выполнении запроса не будет отправлен на компонент Central Node. Компонент Endpoint Sensors не управляет правами доступа к данной папке и ее файлам. Доступ определяет системный администратор.

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 компонент Endpoint Sensors не будет удален с компьютера, но не более 21 дня.

Данные о событиях

Данные о событиях могут содержать следующую информацию:

- О файлах.
- Об исполняемых модулях.
- О сетевых соединениях.
- Об операционной системе и программном обеспечении, установленном на компьютере с компонентом Endpoint Sensors.
- О пользовательских сессиях в операционной системе.
- О журнале событий Windows.
- О реестре Windows.
- Персональные данные, в том числе фамилия, имя и отчество, если эти данные являются частью пути к файлам на компьютере.
- URL- и IP-адреса посещенных веб-сайтов, а также имя пользователя и пароль, если они содержатся в заголовках протокола HTTP.
- Имя компьютера.
- MD5-, SHA256-хеш файлов и их фрагментов.
- Уникальный идентификатор компьютера с компонентом Endpoint Sensors.

- Уникальные идентификаторы сертификатов.

Данные о событиях хранятся в бинарном виде в каталоге C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.1\Data в открытом незашифрованном виде. Файлы с данными о событиях доступны для чтения любому пользователю, имеющему доступ на чтение к файлам в данном каталоге. При включенной самозащите у пользователей есть доступ только на чтение. При выключенной самозащите пользователи с правами учетной записи операционной системы System и Administrator могут также удалять файлы, изменять их содержимое и изменять права доступа к ним. Компонент Endpoint Sensors не управляет правами доступа к данной папке и ее файлам.

Данные в файлах трассировки

Компонент Endpoint Sensors может выполнять запись отладочной информации компонента и драйверов компонента в соответствии с заданными параметрами в файлы трассировки. По умолчанию компонент Endpoint Sensors не записывает отладочную информацию. Автоматическая отправка файлов трассировки за пределы хоста, на котором они были сформированы, не производится. Файлы трассировки полностью удаляются при удалении компонента Endpoint Sensors.

Данные в файлах трассировки могут содержать следующую информацию:

- Время события.
- Номер потока выполнения.
- Компонент программы, в результате работы которого произошло обнаружение.
- Важности события.
- Описание выполнения команды компонента программы и результата выполнения этой команды.
- О файлах.
- Об исполняемых модулях.
- Об открытых портах.
- О сетевых соединениях.
- О содержимом ARP-кеша.
- О содержимом DNS-кеша.
- Об операционной системе и программном обеспечении, установленном на компьютере с компонентом Endpoint Sensors.
- О логических дисках.
- Об учетных записях пользователей операционной системы.
- О пользовательских сессиях в операционной системе.
- О сервисах операционной системы.
- О журнале событий Windows.
- О реестре Windows.
- Персональные данные, в том числе фамилия, имя и отчество, если эти данные являются частью пути к файлам на компьютере.
- Имя пользователя и пароль, если они содержатся в заголовках протокола HTTP.
- Имя учетной записи пользователей операционной системы, если имя учетной записи является частью имени файла.

- Адрес электронной почты или URL-адрес с именем учетной записи и паролем, если они содержатся в имени обнаруженного объекта.
- URL- и IP-адреса посещенных веб-сайтов, а также ссылки с этих веб-сайтов.
- При использовании прокси-сервера: IP-адрес прокси-сервера, имя компьютера, порт, имя пользователя прокси-сервера.
- Внешние IP-адреса, с которыми было установлено соединение с локального компьютера.

Файлы трассировки хранятся в каталоге C:\ProgramData\Kaspersky Lab\ в открытом незашифрованном виде. Файлы трассировки доступны для чтения любому пользователю, имеющему доступ на чтение к файлам в данном каталоге. При включенной самозащите у пользователей есть доступ только на чтение. При выключенной самозащите пользователи с правами учетной записи операционной системы System и Administrator могут также удалять файлы, изменять их содержимое и изменять права доступа к ним. Компонент Endpoint Sensors не управляет правами доступа к данной папке и ее файлам.

Данные в отчетах о выполнении задач

Отчеты о выполнении задач содержат следующую информацию:

- О результатах выполнения задач.
- О файлах.
- Об исполняемых модулях.
- О процессах операционной системы.
- Об учетных записях пользователей.
- О пользовательских сессиях.
- Персональные данные, в том числе фамилия, имя и отчество, если эти данные являются частью пути к файлам на компьютере.
- Имя компьютера.
- MD5-, SHA256-хеш файлов и их фрагментов.
- Уникальный идентификатор компьютера с компонентом Endpoint Sensors.
- Дампы компьютера с компонентом Endpoint Sensors.
- Карты памяти с компонентом Endpoint Sensors.
- Файлы компьютера с компонентом Endpoint Sensors.
- Содержимое стандартного потока вывода процесса.
- Содержимое стандартного потока ошибок процесса.

Данные в журнале установки

Администратор может включить запись журнала установки компонента Endpoint Sensors (стандартными средствами msiehex) 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 msiehex, которая содержит адрес сервера с компонентом Central Node и путь к файлу журнала установки.

Данные в файлах дампов

Файлы дампов компонента Endpoint Sensors формируются операционной системой при сбоях программы,

хранятся в папке, заданной параметрами операционной системы, и перезаписываются при каждом сбое. В файлы дампов могут попасть любые данные, включая фрагменты анализируемых файлов, расшифрованные данные и ключи шифрования, персональные данные пользователя или конфиденциальные данные вашей организации.

Рекомендуется не использовать компонент Endpoint Sensors на тех компьютерах, передача данных с которых запрещена политикой вашей организации.

Данные, полученные от компонента Endpoint Sensors, хранятся на сервере с компонентом Central Node и ротируются по мере заполнения дискового пространства.

Файлы дампов, подготовленные к отправке компонентом Endpoint Sensors на сервер с компонентом Central Node, хранятся на компьютерах с компонентом Endpoint Sensors в открытом незашифрованном виде в той директории, которая по умолчанию используется для хранения файлов дампов перед отправкой на каждом компьютере с компонентом Endpoint Sensors.

Файлы дампов с компьютеров с компонентом Endpoint Sensors отправляются на сервер с компонентом Central Node напрямую или через сервер с компонентом Sensor, если администратор настроил использование сервера Sensor в качестве посредника (прокси) при передаче трафика, по защищенному SSL-соединению (см. раздел "Подготовка SSL-соединения к обмену данными между компонентами Endpoint Sensors и Central Node" на стр. [123](#)).

Файлы, зашифрованные на компьютерах с компонентом Endpoint Sensors с помощью программ Windows Encrypting File System или Kaspersky File Level Encryption (в программе Kaspersky Endpoint Security для Windows), передаются на сервер с компонентом Central Node в расшифрованном виде.

Kaspersky Anti Targeted Attack Platform поддерживает возможность изменения параметров локального компьютера с компонентом Endpoint Sensors, влияющих на производительность компьютера при взаимодействии с компонентом Central Node.

Изменение параметров следует производить исключительно по рекомендации Службы технической поддержки "Лаборатории Касперского".

Самостоятельное изменение параметров может ухудшить производительность локального компьютера.

Администратору Kaspersky Anti Targeted Attack Platform необходимо обеспечить безопасность компьютеров с компонентом Endpoint Sensors и серверов Kaspersky Anti Targeted Attack Platform с перечисленными выше данными самостоятельно. Администратор Kaspersky Anti Targeted Attack Platform несет ответственность за доступ к данной информации.

Архитектура программы

В состав программы входят следующие основные компоненты:

- *Sensor*. Выполняет прием данных.
- *Central Node*. Выполняет проверку данных, исследование поведения объектов, а также публикацию результатов исследования в веб-интерфейс программы.
- *Sandbox*. Запускает виртуальные образы операционных систем (32-разрядной Windows XP SP3, 32-разрядной Windows 7 и 64-разрядной Windows 7). 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 Sensors*. Устанавливается на отдельные компьютеры, входящие в IT-инфраструктуру организации и работающие под управлением операционной системы Microsoft Windows. Осуществляет постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами.

В этом разделе

Компонент Sensor	49
Компонент Central Node	50
Компонент Sandbox.....	50
Компонент Endpoint Sensors	51

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.
- *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 программ "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 – сервер или виртуальная машина, на которой установлена программа "Лаборатории Касперского" Kaspersky Secure Mail Gateway (далее также "KSMG"). KSMG отправляет сообщения электронной почты на обработку в Kaspersky Anti Targeted Attack Platform. По результатам обработки сообщений электронной почты в Kaspersky Anti Targeted Attack Platform KSMG может блокировать пересылку сообщений.

Если в качестве компонента Sensor используется программа Kaspersky Secure Mail Gateway, то белые списки, настроенные по получателям сообщений и MD5-суммам файлов, не передаются в KSMG и не применяются при обработке сообщений программой Kaspersky Secure Mail Gateway.

Компонент Central Node

На каждом сервере с компонентом Central Node работают следующие модули, ядра и технологии Kaspersky Anti Targeted Attack Platform:

- *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.
- *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.
- *Risk Score Engine* (далее также *Risk Score* и *RS Engine*). Выполняет эвристический анализ поведения исполняемых файлов формата APK в операционной системе Android™.
- *Targeted Attack Analyzer* (далее также *TAA*, *TA Analyzer*). Выполняет статистический анализ и проверку сетевой активности программного обеспечения, установленного на компьютеры локальной сети организации. 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 образы следующих операционных систем:

- Windows XP SP3, 32-разрядная.
- Windows 7, 32-разрядная.
- Windows 7, 64-разрядная.

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 программой.

Максимальный уровень вложенности проверяемых архивов составляет 32.

Максимальное количество объектов, которое может находиться в очереди на проверку компонентом Sandbox за одни сутки, составляет 10 тысяч объектов. По достижении этого ограничения программа удаляет 10% объектов, поступивших на проверку раньше остальных, и заменяет их новыми объектами, поступившими на проверку. Удаленные объекты сохраняются в программе со статусом NOT_SCANNED (непроверенные).

Компонент Endpoint Sensors

Компонент Endpoint Sensors устанавливается на отдельных компьютерах, входящих в IT-инфраструктуру организации и работающих под управлением операционной системы Microsoft Windows (далее также "компьютеры локальной сети организации" или "компьютеры"). На этих компьютерах компонент постоянно наблюдает за процессами, открытыми сетевыми соединениями и изменяемыми файлами и отправляет данные наблюдения на сервер с компонентом Central Node. По результатам проверки этих данных компонентом Central Node компонент Endpoint Sensors также может отправить файлы, дампы и карты памяти, связанные с обнаруженными событиями, на сервер с компонентом Central Node.

Компьютеры, предназначенные для установки компонента Endpoint Sensors, должны удовлетворять аппаратным и программным требованиям.

В качестве компонента Endpoint Sensors также может использоваться программа "Лаборатории Касперского" Kaspersky Endpoint Security. Endpoint Sensors в составе программы Kaspersky Endpoint Security могут наблюдать за процессами, открытыми сетевыми соединениями и изменяемыми файлами и отправлять данные наблюдения на сервер с компонентом Central Node.

Если вы установите программу Kaspersky Endpoint Security на компьютер с компонентом Endpoint Sensors, компонент Endpoint Sensors будет удален независимо от того, включен ли компонент Endpoint Sensors в состав программы Kaspersky Endpoint Security или нет.

Кроме того, Kaspersky Anti Targeted Attack Platform позволяет интегрироваться с программой Kaspersky Security Center и получать статистику работы компонента Endpoint Sensors.

Принцип работы программы

После интеграции в ИТ-инфраструктуру организации программа публикует информацию об обнаруженных признаках целевых атак и вторжений в ИТ-инфраструктуру организации в веб-интерфейс. Принцип работы программы показан на рис. ниже.

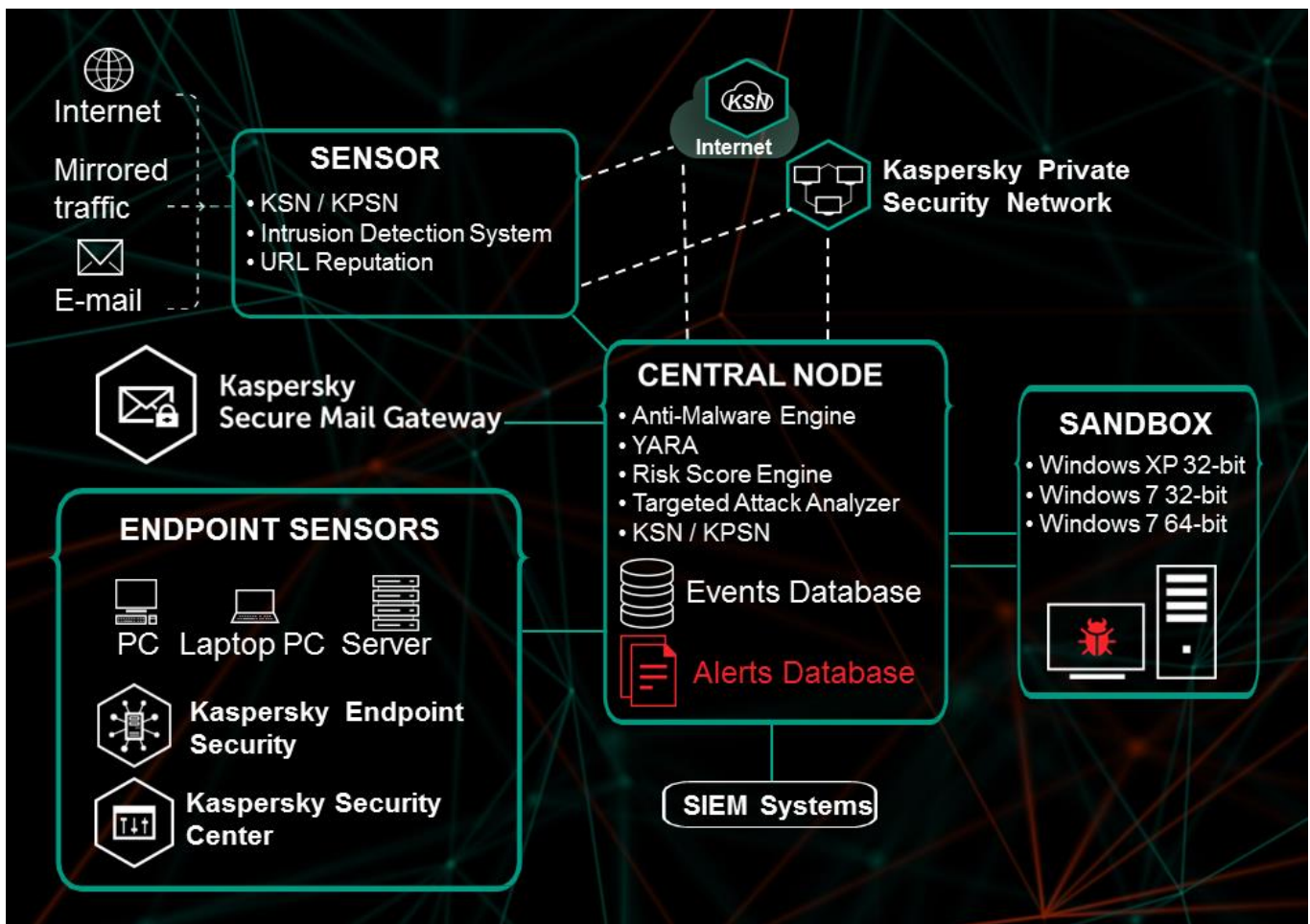


Figure 1: Принцип работы программы

Интерфейс Kaspersky Anti Targeted Attack Platform

Работа с программой осуществляется через веб-интерфейс.

Окно веб-интерфейса программы содержит следующие элементы:

- разделы в левой части и в нижней части окна веб-интерфейса программы;
- закладки в верхней части окна веб-интерфейса программы для некоторых разделов программы;
- рабочую область в нижней части окна веб-интерфейса программы.

Разделы окна веб-интерфейса программы

Веб-интерфейс программы поделен на следующие разделы:

- **Мониторинг.** Содержит данные мониторинга Kaspersky Anti Targeted Attack Platform.
- **Обнаружения.** Содержит информацию об обнаружениях в сети вашей организации.
- **Поиск угроз.** Содержит информацию о событиях, найденных на компьютерах вашей организации.
- **Задачи.** Содержит информацию о задачах, с помощью которых вы можете работать с файлами и программами на хостах.
- **Политики.** Содержит информацию о политиках, с помощью которых вы можете управлять запретами запуска файлов на выбранных хостах.
- **IOC-проверка.** Содержит информацию об IOC-проверке событий и работе с IOC-файлами.
- **Хранилище.** Содержит информацию о работе с объектами в Хранилище и Карантине.
- **Endpoint Sensors.** Содержит информацию об управлении компонентом Endpoint Sensors и просмотре данных.
- **Отчеты.** Содержит конструктор отчетов и список созданных отчетов об обнаружениях.
-  Содержит разделы **Лицензия**, **Пользователи**, **YARA-правила**, **Белый список**, **Группа VIP**, **Отправка уведомлений** и **Endpoint Sensors**, а также раздел **Интеграции**, в котором вы можете настроить интеграцию Kaspersky Anti Targeted Attack Platform со следующими системами и программами: **KSC**, **SIEM-система**, **Почтовый сенсор**.

Рабочая область окна веб-интерфейса программы

В рабочей области отображается информация, просмотр которой вы выбираете в разделах и на закладках окна веб-интерфейса программы, а также элементы управления, с помощью которых вы можете настроить отображение информации.

Типовые схемы развертывания и установки компонентов программы

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

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

Для оптимальной работы программы рекомендованы две типовые схемы развертывания:

- Схема развертывания на два сервера. На одном сервере устанавливаются компоненты Sensor и Central Node, а на втором сервере устанавливается компонент Sandbox (см. рис. ниже).

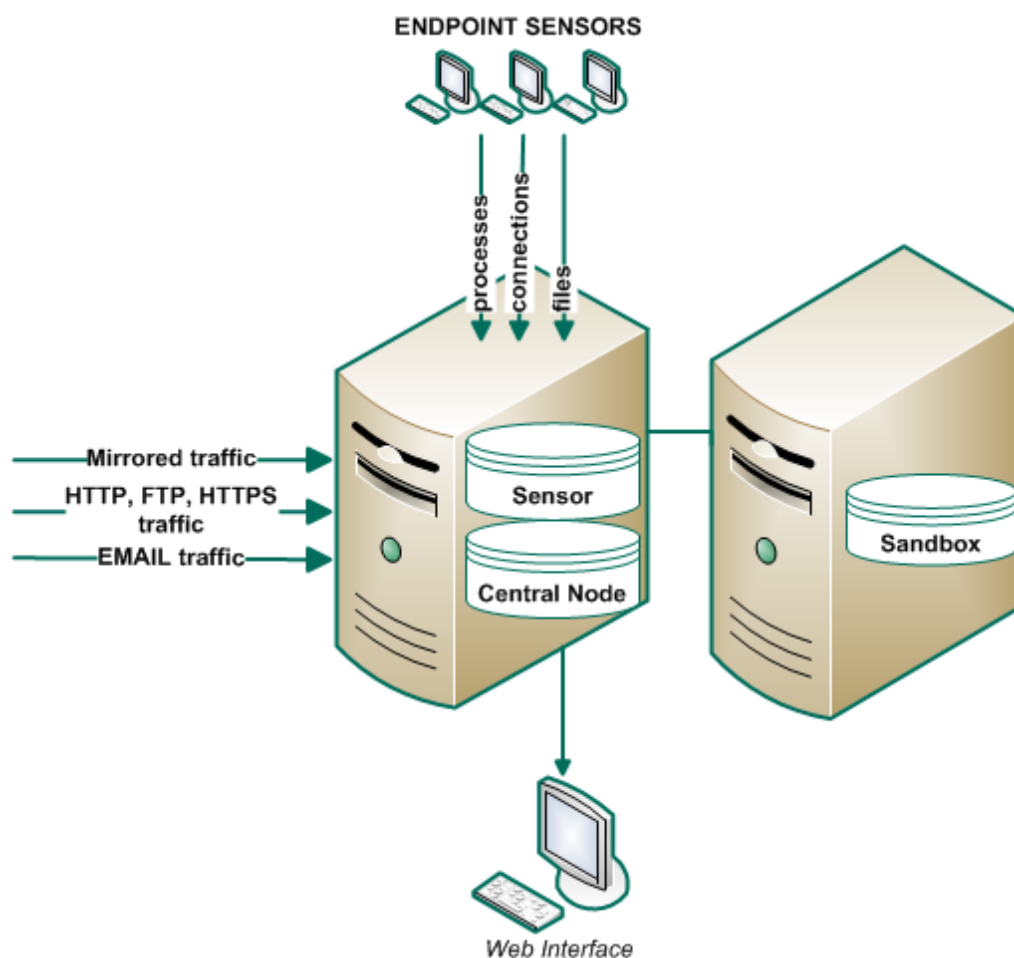


Figure 2: Схема развертывания на два сервера

- Схема развертывания на три и более серверов. Для каждого из компонентов программы Central Node, Sandbox и Sensor выделяется один или более серверов (в зависимости от объема данных, обрабатываемых программой).

Подготовка к установке компонентов программы

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

При установке версии 3.0 все данные, накопленные в процессе работы предыдущих версий программы (например, события и сопутствующая информация), будут потеряны. Если вы хотите сохранить накопленные данные, перед установкой версии 3.0 обратитесь в Службу технической поддержки "Лаборатории Касперского" (https://support.kaspersky.ru/kata/about_kata).

В этом разделе

Подготовка IT-инфраструктуры к установке компонентов программы	55
Подготовка IT-инфраструктуры к интеграции с почтовым сервером для приема сообщений по протоколу POP3	56
Подготовка IT-инфраструктуры к интеграции с почтовым сервером для отправки сообщений по протоколу SMTP	57

Подготовка IT-инфраструктуры к установке компонентов программы

► *Перед установкой программы 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 программы, и компьютеры, на которых устанавливается компонент Endpoint Sensors, удовлетворяют аппаратным и программным требованиям.
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 обновления баз и анализа поведения объектов.
 - c. Для второго сетевого интерфейса разрешите входящее соединение сервера с компонентом Sandbox на порты 22, 443 и 8443.
3. Произведите следующую предварительную подготовку IT-инфраструктуры организации к установке компонента Central Node:
 - a. Разрешите входящее соединение сервера с компонентом Central Node на порты 22, 8081 (если компонент Sensor устанавливается на отдельные серверы), 443 и 8443.
 - b. Разрешите исходящее соединение сервера с компонентом Central Node на порт 161 (если

компонент Sensor устанавливается на отдельные серверы).

4. Произведите следующую предварительную подготовку IT-инфраструктуры организации к установке компонента Sensor:
 - a. Разрешите входящее соединение сервера с компонентом Sensor на порт 22.
 - b. Разрешите исходящее соединение сервера с компонентом Sensor на порт 8081.
5. Разрешите входящее соединение компьютеров с компонентом Endpoint Sensors и сервера с компонентом Central Node напрямую, без использования прокси-сервера.

При необходимости вы можете назначить другие порты для работы компонентов программы 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, выполните следующие действия:*

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, выполните следующие действия:*

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, выполните следующие действия:*

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, выполните следующие действия:*

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.

Порядок установки и настройки компонентов программы

Выполняйте действия по установке программы в следующем порядке:

1. Установите образ диска с подготовленной средой для компонента Sandbox.
2. Установите образ диска с компонентом Sandbox.
3. Настройте компонент Sandbox через веб-интерфейс Sandbox.
4. Установите образы дисков операционных систем Microsoft Windows для работы компонента Sandbox.
5. Установите образ диска с подготовленной средой для компонентов Central Node и Sensor.
6. Установите образ диска с компонентами Central Node и Sensor в зависимости от схемы развертывания и установки программы:
 - Если вы используете схему развертывания на два сервера, установите компоненты Central Node и Sensor на одном сервере.
 - Если вы используете схему развертывания на три и более серверов, установите компоненты Central Node и Sensor в следующем порядке:
 1. Установите компонент Central Node на одном сервере.
 2. Установите компонент Sensor на втором сервере или на нескольких серверах.
7. Установите компонент Endpoint Sensors на компьютерах, входящих в IT-инфраструктуру организации.

Установка компонента Sandbox

Этот раздел представляет собой пошаговую инструкцию по установке компонента Sandbox.

► *Чтобы приступить к установке компонента Sandbox,*

запустите образ диска с компонентом Sandbox.

Запустится мастер установки.

В этом разделе

Шаг 1. Просмотр Лицензионного соглашения	59
Шаг 2. Выбор диска для установки компонента Sandbox.....	59
Шаг 3. Создание учетной записи администратора Sandbox	60
Шаг 4. Выбор управляющего сетевого интерфейса в списке	60
Шаг 5. Назначение адреса и маски сети управляющего интерфейса	61
Шаг 6. Настройка статического сетевого маршрута	61

Шаг 1. Просмотр Лицензионного соглашения

Для продолжения установки вам нужно просмотреть Лицензионное соглашение и принять его условия. Если условия Лицензионного соглашения не приняты, установка не выполняется.

► *Чтобы принять условия Лицензионного соглашения, выполните следующие действия:*

1. Выберите язык для просмотра Лицензионного соглашения в списке.
Например, если вы хотите просмотреть Лицензионное соглашение на английском языке, выберите **English**.
2. Нажмите на клавишу **ENTER**.
Откроется окно с текстом Лицензионного соглашения.
3. Ознакомьтесь с Лицензионным соглашением.
4. Если вы принимаете условия Лицензионного соглашения, нажмите на кнопку **I accept the terms**.

Мастер установки перейдет к следующему шагу.

Шаг 2. Выбор диска для установки компонента Sandbox

На этом шаге выберите физический диск для установки компонента Sandbox.

► *Чтобы выбрать диск для установки компонента Sandbox, выполните следующие действия:*

1. В окне **Select device** в списке дисков выберите диск для установки компонента Sandbox.

2. Нажмите на клавишу **ENTER**.

Архив с установочными файлами распакуется на диск. Сервер перезагрузится.

Мастер установки перейдет к следующему шагу.

Шаг 3. Создание учетной записи администратора Sandbox

На этом шаге 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, выполните следующие действия:*

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**.

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 только внутри сети.

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

На этом шаге выберите сетевой интерфейс, который вы хотите использовать в качестве управляющего.

► Чтобы выбрать управляющий сетевой интерфейс, выполните следующие действия:

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, выполните следующие действия:

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. Настройка статического сетевого маршрута

► Чтобы настроить статические сетевые маршруты, выполните следующие действия для каждого сетевого маршрута:

1. В окне **IPv4 Routes** выберите **New**.
2. Нажмите на клавишу **ENTER**.
Откроется окно **IPv4 Static Route**.
3. В поле **Address/Mask** введите IP-адрес и маску подсети, для которой вы хотите настроить сетевой маршрут.
4. В поле **Gateway** введите IP-адрес шлюза.
5. Нажмите на кнопку **Ok**.

Перейдите к настройке компонента Sandbox через веб-интерфейс.

Настройка компонента Sandbox через веб-интерфейс

Веб-интерфейс Sandbox расположен на сервере с компонентом Sandbox.

Веб-интерфейс Sandbox защищен от *CSRF-атак* (см. стр. [332](#)) 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 настройки параметров убедитесь, что прокси-сервер не модифицирует заголовок Referrer HTTP-запроса POST.

► Чтобы начать работу в веб-интерфейсе Sandbox, выполните следующие действия:

1. В браузере на любом компьютере, на котором разрешен доступ к серверу с компонентом Sandbox, введите IP-адрес сервера с компонентом Sandbox (см. стр. [61](#)).
Откроется окно ввода учетных данных администратора компонента Sandbox.
2. Введите имя пользователя и пароль администратора компонента Sandbox, который вы задали при установке компонента Sandbox (см. стр. [60](#)).

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.

В этом разделе

Обновление баз компонента Sandbox	63
Настройка соединения компонентов Sandbox и Central Node	64
Настройка сетевых интерфейсов компонента Sandbox	66
Обновление системы Sandbox	69
Установка даты и времени системы Sandbox	70
Установка и настройка образов операционных систем и программ для работы компонента Sandbox	70
Загрузка журнала системы Sandbox на жесткий диск	74
Экспорт параметров Sandbox	74
Импорт параметров Sandbox	75
Перезагрузка сервера Sandbox	76
Выключение сервера Sandbox	76
Изменение пароля учетной записи администратора Sandbox	76

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.

В этом разделе

Запуск обновления баз вручную.....	63
Выбор источника обновления баз	63
Включение и отключение использования прокси-сервера для обновления баз	64
Настройка параметров соединения с прокси-сервером для обновления баз	64

Запуск обновления баз вручную

► *Чтобы запустить обновление баз вручную, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Database Update**.
В блоке параметров **Last update** отобразятся время и статус последней попытки обновления баз Sandbox.
2. Нажмите на кнопку **Update**.

Выбор источника обновления баз

► *Чтобы выбрать источник обновления баз, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Database Update**.
2. В блоке параметров **Update source** выберите источник, из которого вы хотите получать пакет обновлений:
 - **Kaspersky Lab update server**.
 - **Custom server**.
3. Если вы выбрали **Custom server**, в поле под названием этого параметра укажите URL-адрес пакета обновлений на вашем FTP- или HTTP-сервере или укажите полный путь к директории с пакетом обновлений.
4. Нажмите на кнопку **Apply** 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*, выполните следующие действия:

1. В окне веб-интерфейса *Sandbox* выберите раздел **Database Update**.
2. В рабочей области выполните одно из следующих действий:
 - Включите переключатель рядом с названием блока параметров **Proxy server**, если вы хотите использовать прокси-сервер при обновлении баз компонента *Sandbox*.
 - Выключите переключатель рядом с названием блока параметров **Proxy server**, 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*, выполните следующие действия:

1. В окне веб-интерфейса *Sandbox* выберите раздел **Database Update**.
2. Включите переключатель рядом с названием блока параметров **Proxy server**.
3. В поле **Address** введите адрес прокси-сервера.
4. В поле **Port** укажите номер порта прокси-сервера.
5. В поле **User name** введите имя пользователя прокси-сервера.
6. В поле **Password** введите пароль подключения к прокси-серверу.
7. Выполните одно из следующих действий:
 - Установите флажок **Bypass proxy server for local addresses**, если вы не хотите использовать прокси-сервер для внутренних адресов электронной почты вашей организации.
 - Снимите флажок **Bypass proxy server for local addresses**, если вы хотите использовать прокси-сервер независимо от принадлежности адресов электронной почты к вашей организации.
8. Нажмите на кнопку **Apply** в нижней части окна.

Настройка соединения компонентов *Sandbox* и *Central Node*

Предусмотрен следующий порядок настройки соединения компонента *Sandbox* с компонентом *Central Node*:

1. В меню администратора каждого сервера с компонентом *Central Node* создается запрос на подключение к компоненту *Sandbox*.
2. В веб-интерфейсе *Sandbox* отображаются запросы на подключение.

Вы можете принять или отклонить каждый запрос.

Создание запроса на подключение к Sandbox в меню администратора Central Node

Для создания соединения между компонентами Central Node и Sandbox, необходимо отправить запрос на подключение к компоненту Sandbox с каждого компонента Central Node.

► Чтобы создать запрос на подключение к компоненту Sandbox, выполните следующие действия:

1. Зайдите в консоль сервера Central Node, с которого вы хотите создать запрос на подключение к Sandbox, по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя пользователя **admin** и пароль, заданный при установке и настройке компонента Central Node (см. раздел "Шаг 1. Создание учетной записи для работы в меню администратора и в консоли управления сервером" на стр. [81](#)).

Отобразится меню администратора программы.

3. В меню администратора программы выберите **Program Settings**.

4. Нажмите на клавишу **ENTER**.

Откроется окно выбора действия.

5. Выберите действие **Configure Sandbox connection**.

6. Нажмите на клавишу **ENTER**.

Откроется окно **Sandbox access**.

7. Выберите **New**.

8. Нажмите на клавишу **ENTER**.

Откроется окно **Sandbox node**.

9. В поле **Sandbox name** введите доменное имя сервера Sandbox, запрос на подключение к которому вы создаете.

10. В поле **Sandbox node** введите IP-адрес сервера Sandbox, запрос на подключение к которому вы создаете.

11. Нажмите на кнопку **Ok**.

Откроется окно выбора действия.

12. Выберите строку с IP-адресом сервера Sandbox.

13. Нажмите на клавишу **ENTER**.

14. Откроется окно **Sandbox key fingerprint**, содержащее отпечаток сертификата Sandbox и просьбу подтвердить подлинность отпечатка сертификата.

15. Убедитесь, что отпечаток сертификата соответствует отпечатку сертификата в веб-интерфейсе Sandbox, запрос на подключение к которому вы создаете.

16. После того, как вы убедились, что отпечатки сертификатов идентичны, нажмите на кнопку **Yes**.

Откроется окно подтверждения отправки запроса на подключения к компоненту Sandbox.

17. Нажмите на кнопку **Yes**.

Вы вернетесь к окну выбора действия с IP-адресом сервера Sandbox.

Если запрос на подключение к компоненту Sandbox отправлен успешно, напротив названия параметра

Enabled отобразится значение **Yes**.

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.

► *Чтобы принять, отклонить или отозвать запрос на подключение от серверов Central Node, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **KATA Authorization**.

В разделе **Central Node connection requests** отобразится список запросов на подключение от компонентов Central Node.

В каждом запросе на подключение содержится следующая информация:

- **IP** – IP-адрес сервера Central Node.
- **Certificate fingerprint** – отпечаток TLS-сертификата Central Node, с помощью которого устанавливается зашифрованное соединение между серверами.
- **State** – состояние запроса на подключение.

Может иметь значения **Pending** или **Accepted**.

2. Убедитесь, что отпечаток сертификата Central Node соответствует отпечатку сертификата на стороне Central 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:

- **Accept**, если вы хотите принять запрос на подключение.
- **Reject**, если вы хотите отклонить запрос на подключение.
- **Revoke**, если вы хотите отозвать ранее принятый запрос на подключение.

4. Нажмите на кнопку **Apply** в нижней части окна.

Настройка сетевых интерфейсов компонента Sandbox



В этом разделе содержится информация о настройке сетевых интерфейсов компонента Sandbox.

Настройка параметров DNS

► *Чтобы настроить параметры DNS, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Network Interfaces**.
2. В поле **Host name** введите имя сервера, на который вы устанавливаете компонент Sandbox, в

формате FQDN (например, sandbox).

3. Справа от названия параметра **DNS servers** нажмите на кнопку **Add**.
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 "Шаг 4. Выбор управляющего сетевого интерфейса в списке" на стр. [60](#)).

Вы также можете настроить управляющий сетевой интерфейс в веб-интерфейсе Sandbox.

► *Чтобы настроить управляющий сетевой интерфейс в веб-интерфейсе Sandbox, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Network Interfaces**.
2. В группе параметров **Management interface** в раскрывающемся списке **Interface** 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 **Mask** введите маску сети, в которой вы хотите использовать этот сетевой интерфейс.
5. Нажмите на кнопку **Apply** 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 только внутри сети.

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 вредоносную программу 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, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Network Interfaces**.
2. В группе параметров **Internet interface** в списке **Interface** 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 **Mask** введите маску сети, в которой вы хотите использовать этот сетевой интерфейс.
5. В поле **Default gateway** введите адрес шлюза сети, в которой вы хотите использовать этот сетевой интерфейс.
6. Нажмите на кнопку **Apply** в нижней части окна.




Добавление, изменение и удаление статических сетевых маршрутов

Вы можете настроить статические сетевые маршруты во время установки компонента Sandbox (см. раздел "Шаг 6. Настройка статического сетевого маршрута" на стр. [61](#)).


Вы также можете добавить, удалить или изменить статические сетевые маршруты в веб-интерфейсе Sandbox.

► *Чтобы добавить статический сетевой маршрут, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Network Interfaces**.

2. В группе параметров **Static Routes** нажмите на кнопку **Add**.
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 **Mask** введите маску подсети.
 5. В поле **Gateway** введите IP-адрес шлюза.
 6. В списке **Interface** выберите сетевой интерфейс, для которого вы хотите добавить статический сетевой маршрут.
 7. Нажмите на кнопку .
 8. Нажмите на кнопку **Apply** в нижней части окна.
- *Чтобы удалить статический сетевой маршрут, выполните следующие действия:*
1. В окне веб-интерфейса Sandbox выберите раздел **Network Interfaces**.
 2. В группе параметров **Static Routes** в строке со статическим сетевым маршрутом, который вы хотите удалить, нажмите на кнопку .
 3. Нажмите на кнопку **Apply** в нижней части окна.
- *Чтобы изменить статический сетевой маршрут, выполните следующие действия:*
1. В окне веб-интерфейса Sandbox выберите раздел **Network Interfaces**.
 2. В группе параметров **Static Routes** 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 **Mask** измените маску подсети.
 5. В поле **Gateway** измените IP-адрес шлюза.
 6. В списке **Interface** выберите сетевой интерфейс, для которого вы редактируете сетевой маршрут.
 7. Нажмите на кнопку .
 8. Нажмите на кнопку **Apply** в нижней части окна.

Обновление системы Sandbox

"Лаборатория Касперского" может выпускать пакеты обновлений Kaspersky Anti Targeted Attack Platform и отдельных компонентов программы. Например, могут выпускаться срочные пакеты обновлений, устраняющие уязвимости и ошибки, плановые обновления, добавляющие новые или улучшающие существующие функции программы и ее компонентов.

После выпуска обновлений Sandbox вы можете установить их через веб-интерфейс Sandbox.

Перед установкой обновлений через веб-интерфейс Sandbox вам нужно загрузить пакет обновления в формате TGZ и инструкцию по установке данного обновления с сайта "Лаборатории Касперского" на ваш

компьютер.

► Чтобы обновить систему Sandbox через веб-интерфейс, выполните следующие действия:


1. В окне веб-интерфейса Sandbox выберите раздел **System Upgrade**.
Справа от названия параметра **Current version** отобразится текущая версия компонента Sandbox.
2. Нажмите на кнопку **Browse** справа от поля **Upgrade package**.
Откроется окно выбора файлов.
3. Выберите файл обновления, который вы хотите загрузить, и нажмите на кнопку **Открыть**.
Окно выбора файлов закроется.

Вы можете следить за ходом обновления системы Sandbox в окне **Upgrade Log** раздела **System Upgrade** веб-интерфейса Sandbox.

Пакет обновления будет установлен автоматически. Процесс обновления может занять несколько минут. Сервер Sandbox перезагрузится. Компонент Sandbox будет недоступен во время обновления системы.

Установка даты и времени системы Sandbox

► Чтобы установить дату и время сервера с компонентом Sandbox, выполните следующие действия:

1. В окне веб-интерфейса Sandbox выберите раздел **Date and Time**.
2. В раскрывающемся списке **Country** выберите нужную страну.
3. В раскрывающемся списке **Time zone** выберите нужный часовой пояс.
4. Если вы хотите синхронизировать время с NTP-сервером, включите переключатель справа от названия параметра **Synchronization with NTP servers**.
5. Если вы хотите установить дату и время вручную, не включайте переключатель справа от названия параметра **Synchronization with NTP servers** и выполните следующие действия:
 - a. В поле **Date** введите текущую дату или нажмите на кнопку  и выберите дату в календаре.
 - b. В поле **Time** введите текущее время.
6. Нажмите на кнопку **Apply** в нижней части окна.

Установка и настройка образов операционных систем и программ для работы компонента Sandbox

В инсталляционном комплекте вы получаете три ISO-образа операционных систем Windows XP SP3, 32-разрядной Windows 7, 64-разрядной Windows 7 и программ, необходимых для работы компонента Sandbox. Компонент Sandbox будет запускать объекты в этих операционных системах и анализировать поведение этих объектов для выявления вредоносной активности, признаков целевых атак и вторжений в

IT-инфраструктуру организации.

Вам нужно установить образы этих операционных систем и программ, а также активировать их (см. раздел "Лицензирование операционных систем и программ, необходимых для работы компонента Sandbox" на стр. [31](#)).

Загрузка ISO-образов операционных систем и программ для работы компонента Sandbox

► Чтобы загрузить ISO-образ операционной системы и программ, необходимых для работы компонента Sandbox, выполните следующие действия для каждого ISO-образа:

1. В окне веб-интерфейса Sandbox выберите раздел **Virtual Machines**.
2. В группе параметров **ISO Images** нажмите на кнопку **Upload ISO**.
Откроется окно выбора файлов.
3. Выберите файл формата ISO, который вы хотите загрузить, и нажмите на кнопку **Открыть**.
Окно выбора файлов закроется.

В списке **ISO Images** отобразится загруженный образ операционной системы и программ, необходимых для работы компонента Sandbox.

Выполните действия по загрузке образов операционных систем и программ, необходимых для работы компонента Sandbox, для каждого ISO-образа.

Создание виртуальных машин с образами операционных систем и программ для работы компонента Sandbox

► Чтобы создать виртуальную машину с образом операционной системы и программ, необходимых для работы компонента Sandbox, выполните следующие действия для каждой виртуальной машины:

1. В окне веб-интерфейса Sandbox выберите раздел **Virtual Machines**.
2. В списке **ISO Images** в строке с названием образа операционной системы и программ для работы компонента Sandbox нажмите на кнопку **Add VM**.

Откроется окно **EULA**, содержащее тексты следующих лицензионных соглашений:

- MICROSOFT WINDOWS 7 PROFESSIONAL SERVICE PACK 1.
- MICROSOFT WINDOWS XP PROFESSIONAL EDITION SERVICE PACK 3.
- MICROSOFT OFFICE 2010 DESKTOP APPLICATION SOFTWARE.
- MICROSOFT OFFICE 2007 DESKTOP APPLICATION SOFTWARE.
- MICROSOFT OFFICE 2003 DESKTOP APPLICATION SOFTWARE.
- ADOBE® Personal Computer Software License Agreement.

- MICROSOFT VISUAL C++ 2005 RUNTIME LIBRARIES.
- MICROSOFT VISUAL C++ 2008 RUNTIME LIBRARIES (X86, IA64 AND X64), SERVICE PACK 1.
- MICROSOFT VISUAL C++ 2010 RUNTIME LIBRARIES.
- MICROSOFT VISUAL C++ 2012 RUNTIME LIBRARIES.
- MICROSOFT VISUAL C++ REDISTRIBUTABLE FOR VISUAL STUDIO 2013.
- MICROSOFT VISUAL STUDIO 2017 TOOLS, ADD-ONS and C++ REDISTRIBUTABLE.

Ключи активации этих операционных систем Microsoft Windows и программ Microsoft Office не входят в установочный комплект Kaspersky Anti Targeted Attack Platform. Вам нужно активировать эти операционные системы и программы с помощью своих ключей.

3. Ознакомьтесь с текстами лицензионных соглашений и нажмите на кнопку **Accept** в правом нижнем углу окна **EULA**.
Откроется окно **Unpack**. Архив с образом операционной системы и программ для работы компонента Sandbox будет распакован.
4. В списке **Not installed VMs** окна **Virtual Machines** появится виртуальная машина, готовая к активации операционных систем и программ, а также к установке.

Выполните действия по созданию виртуальных машин с образами операционных систем и программ для работы компонента Sandbox для каждой виртуальной машины.

Активация операционных систем и программ для работы компонента Sandbox

- Чтобы активировать операционные системы и программы, необходимые для работы компонента Sandbox, выполните следующие действия:

1. В окне веб-интерфейса Sandbox выберите раздел **Virtual Machines**.
2. Если в списке **Not installed VMs** рядом с названием операционной системы отображается статус **Not activated**, нажмите на кнопку **Activate** в правой части строки.

Откроется окно ввода кодов активации операционной системы и программ, входящих в состав виртуальной машины для работы компонента Sandbox.

3. Введите коды активации и нажмите на кнопку **Apply**.

Например, если вы загрузили образ операционной системы Windows XP Professional, введите коды активации операционной системы Microsoft Windows XP Professional и Microsoft Office Professional 2003.

Операционная система и программы, входящие в состав виртуальной машины, будут активированы.

Статус рядом с названием операционной системы и программ изменится на **Ready to install**.

Достаточно активировать операционные системы и программы для работы компонента Sandbox один раз. Если вы будете переустанавливать виртуальные машины с ранее активированными операционными системами и программами, повторная активация не потребуется.

Рассчитывайте количество активаций при приобретении лицензий следующим образом:

- Количество активаций каждой из используемых версий Microsoft Windows должно быть равно максимальному количеству одновременно запускаемых виртуальных машин компонента Sandbox, деленному на 4.

32-разрядная MICROSOFT WINDOWS 7 PROFESSIONAL SERVICE PACK 1 и 64-разрядная MICROSOFT WINDOWS 7 PROFESSIONAL SERVICE PACK 1 лицензируются как одна версия Microsoft Windows.

- Количество активаций каждой из используемых версий Microsoft Office должно быть равно максимальному количеству одновременно запускаемых виртуальных машин компонента Sandbox.

Если вы увеличиваете количество виртуальных машин, вам нужно увеличить количество активаций.

Установка виртуальных машин с образами операционных систем и программ для работы компонента Sandbox

- ▶ Чтобы установить все готовые к установке виртуальные машины с образами операционных систем и программ для работы компонента Sandbox, выполните следующие действия:

1. В окне веб-интерфейса Sandbox выберите раздел **Virtual Machines**.
2. В левом нижнем углу списка **Not installed VMs** нажмите на кнопку **Install ready VMs**.

Виртуальные машины с операционными системами, рядом с названиями которых в списке **Not installed VMs** отображается статус **Ready to install**, будут установлены и отобразятся в списке в верхней части окна **Virtual Machines**.

Удаление всех виртуальных машин, ожидающих установки

- ▶ Чтобы удалить все виртуальные машины, ожидающие установки, выполните следующие действия:

1. В окне веб-интерфейса Sandbox выберите раздел **Virtual Machines**.
2. В левом нижнем углу списка **Not installed VMs** нажмите на кнопку **Delete all pending VMs**.

Виртуальные машины с операционными системами и программами для работы компонента Sandbox, ожидающие установки, будут удалены.

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, выполните следующие действия:

1. В окне веб-интерфейса Sandbox выберите раздел **Virtual Machines**.
2. В группе параметров **Guest VM settings** в поле **Max VMs** введите количество одновременно запускаемых виртуальных машин.
Вы можете ввести число от 1 до 200.
3. Нажмите на кнопку **Save**.

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, выполните следующие действия:

1. В окне веб-интерфейса Sandbox выберите раздел **Administration**.
2. В группе параметров **System Log** нажмите на кнопку **Download**.
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 программой.

Экспорт параметров Sandbox

► Чтобы экспортировать параметры системы Sandbox, выполните следующие действия:

1. В окне веб-интерфейса Sandbox выберите раздел **Administration**.
2. В группе параметров **Settings** нажмите на кнопку **Export**.
Откроется окно **Backup warning**, 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 **Backup**.

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 программы. 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, выполните следующие действия:

1. В окне веб-интерфейса Sandbox выберите раздел **Administration**.
2. В группе параметров **Settings** нажмите на кнопку **Import**.

Откроется окно **Restore warning**, 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 **Restore**.

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, выполните следующие действия:

1. В окне веб-интерфейса Sandbox выберите раздел **Administration**.
2. В группе параметров **Power** нажмите на кнопку **Restart**.
Откроется окно подтверждения перезагрузки сервера Sandbox.
3. Нажмите на кнопку **Yes**.

Сервер Sandbox перезагрузится. Через несколько минут вы сможете войти в систему.

Выключение сервера Sandbox

► Чтобы выключить сервер Sandbox, выполните следующие действия:

1. В окне веб-интерфейса Sandbox выберите раздел **Administration**.
2. В группе параметров **Power** нажмите на кнопку **Power off**.
Откроется окно подтверждения выключения сервера Sandbox.
3. Нажмите на кнопку **Yes**.

Сервер Sandbox выключится.

Изменение пароля учетной записи администратора Sandbox

► Чтобы изменить пароль учетной записи администратора Sandbox, выполните следующие действия:

1. В окне веб-интерфейса Sandbox выберите раздел **Administration**.
2. В группе параметров **Change password** отобразится имя учетной записи администратора Sandbox, которое вы задали при установке Sandbox (см. раздел "Шаг 3. Создание учетной записи администратора Sandbox" на стр. [60](#)) и поля для изменения пароля.
3. В поле **Current password** введите текущий пароль учетной записи администратора Sandbox.
4. В поле **New password** введите новый пароль учетной записи администратора Sandbox.
5. В поле **Confirm password** введите новый пароль учетной записи администратора Sandbox повторно.
6. Нажмите на кнопку **Change password**.

Пароль учетной записи администратора Sandbox будет изменен.

Начало установки компонентов Central Node и Sensor

Этот раздел представляет собой пошаговую инструкцию по установке компонентов Central Node и Sensor.

Выполняйте действия по установке на каждом сервере, на котором вы хотите установить компоненты Central Node и Sensor.

Количество запросов на авторизацию компонента Sensor на сервере Central Node не может превышать 50. По достижении этого ограничения Kaspersky Anti Targeted Attack Platform выводит уведомление пользователя на компьютере с компонентом Sensor. Новые запросы на авторизацию не отображаются на сервере Central Node.

В этом разделе

Шаг 1. Начало установки подготовленной среды для компонентов Central Node и Sensor	77
Шаг 2. Просмотр Лицензионного соглашения	77
Шаг 3. Установка подготовленной среды для компонентов Central Node и Sensor	78
Шаг 4. Начало установки компонентов Central Node и Sensor	78
Шаг 5. Просмотр Лицензионного соглашения	78
Шаг 6. Выбор диска для установки компонентов Central Node и Sensor	79
Шаг 7. Выбор роли сервера для установки компонентов Central Node и Sensor.....	79

Шаг 1. Начало установки подготовленной среды для компонентов Central Node и Sensor

► Чтобы приступить к установке подготовленной среды для компонентов Central Node и Sensor, выполните следующие действия:

1. Запустите образ диска с подготовленной средой для компонентов Central Node и Sensor.
Запустится мастер установки.
2. Нажмите на кнопку **ОК**.

Шаг 2. Просмотр Лицензионного соглашения

Для продолжения установки вам нужно просмотреть Лицензионное соглашение и принять его условия. Если условия Лицензионного соглашения не приняты, установка не выполняется.

► Чтобы принять условия Лицензионного соглашения, выполните следующие действия:

1. Выберите язык для просмотра Лицензионного соглашения в списке.

Например, если вы хотите просмотреть Лицензионное соглашение на английском языке, выберите **English**.

2. Нажмите на клавишу **ENTER**.

Откроется окно с текстом Лицензионного соглашения.

3. Ознакомьтесь с Лицензионным соглашением.
4. Если вы принимаете условия Лицензионного соглашения, нажмите на кнопку **I accept the terms**.

Мастер установки перейдет к следующему шагу.

Шаг 3. Установка подготовленной среды для компонентов Central Node и Sensor

На этом шаге выберите физический диск и установите подготовленную среду для компонентов Central Node и Sensor.

- ▶ *Чтобы выбрать диск и установить подготовленную среду, выполните следующие действия:*

1. В окне **Select device** в списке дисков выберите диск для установки подготовленной среды.
2. Нажмите на клавишу **ENTER**.

Сервер перезагрузится.

Подготовленная среда для компонентов Central Node и Sensor будет установлена на выбранный диск.

Шаг 4. Начало установки компонентов Central Node и Sensor

- ▶ *Чтобы приступить к установке компонентов Central Node и Sensor, выполните следующие действия:*

1. Запустите образ диска с компонентами Central Node и Sensor.

Запустится мастер установки.

2. Нажмите на кнопку **OK**.

Шаг 5. Просмотр Лицензионного соглашения

Для продолжения установки вам нужно просмотреть Лицензионное соглашение и принять его условия. Если условия Лицензионного соглашения не приняты, установка не выполняется.

- ▶ *Чтобы принять условия Лицензионного соглашения, выполните следующие действия:*

1. Выберите язык для просмотра Лицензионного соглашения в списке.

Например, если вы хотите просмотреть Лицензионное соглашение на английском языке, выберите **English**.

2. Нажмите на клавишу **ENTER**.
Откроется окно с текстом Лицензионного соглашения.
3. Ознакомьтесь с Лицензионным соглашением.
4. Если вы принимаете условия Лицензионного соглашения, нажмите на кнопку **I accept the terms**.

Мастер установки перейдет к следующему шагу.

Шаг 6. Выбор диска для установки компонентов Central Node и Sensor

► *Чтобы выбрать диск для установки компонентов Central Node и Sensor, выполните следующие действия:*

1. В окне **Select device** в списке дисков выберите диск, на который вы установили подготовленную среду для компонентов Central Node и Sensor.
2. Нажмите на клавишу **ENTER**.
Сервер перезагрузится.

Мастер установки перейдет к следующему шагу.

Шаг 7. Выбор роли сервера для установки компонентов Central Node и Sensor

Перед установкой компонентов Sensor и Central Node на сервере мастер установки программы предложит вам выбрать роль сервера – указать, какой именно компонент вы хотите установить на этот сервер.

► *Чтобы выбрать роль сервера, выполните следующие действия:*

3. В списке ролей сервера выберите один из следующих вариантов:
 - **Act as Central Node**, если вы хотите установить компонент Central Node и Sensor на этом сервере.
 - **Act as Sensor Only**, если вы хотите установить только компонент Sensor на этом сервере.
4. Нажмите на клавишу **ENTER**.
Откроется окно подтверждения выбора роли сервера.
5. Нажмите на кнопку **Confirm role**.

Мастер установки перейдет к следующему шагу установки программы в зависимости от выбранной вами роли сервера.

Установка и настройка компонентов Central Node и Sensor на одном сервере

Этот раздел представляет собой пошаговую инструкцию по установке и предварительной настройке компонентов Central Node и Sensor на одном сервере.

Если вы разворачиваете компонент Central Node в гипервизоре VMware ESXi™ и планируете, что компонент Central Node будет получать зеркалированный трафик от нескольких виртуальных сетей, вам нужно произвести предварительную настройку ESX-сервера, на котором вы хотите развернуть компонент Central Node.

► *Чтобы произвести предварительную настройку ESX-сервера, на котором вы хотите развернуть компонент Central Node, выполните следующие действия в гипервизоре VMware ESXi:*

1. Запустите программу VMware vSphere™ Client.
2. В списке ESX-серверов выберите ESX-сервер, предварительную настройку которого вы хотите произвести.
3. Нажатием правой кнопки мыши раскройте меню.
4. Выберите пункт меню **Configuration**.
Откроется окно изменения конфигурации ESX-сервера.
5. В разделе **Hardware** выберите пункт **Networking**.
Откроется окно изменения параметров.
6. На закладке **Ports** выберите раздел **VM Network**.
Откроется окно **VM Network Properties**.
7. На закладке **General** в списке **VLAN ID (Optional)** выберите значение **All**.
8. Нажмите на кнопку **Ok**.

Компонент Central Node сможет получать зеркалированный трафик от нескольких виртуальных сетей.

В этом разделе

Шаг 1. Создание учетной записи для работы в меню администратора и в консоли управления сервером.....	81
Шаг 2. Назначение имени хоста	82
Шаг 3. Первоначальное включение сетевого интерфейса	82
Шаг 4. Настройка сетевого маршрута для использования по умолчанию	82
Шаг 5. Настройка параметров DNS.....	83
Шаг 6. Настройка параметров соединения с прокси-сервером.....	85
Шаг 7. Установка часового пояса	86
Шаг 8. Настройка синхронизации времени с NTP-сервером	87
Шаг 9. Указание адреса сервера с компонентом Sandbox.....	88
Шаг 10. Создание учетной записи администратора веб-интерфейса	88
Шаг 11. Выделение диска для базы данных компонента Targeted Attack Analyzer	89
Шаг 12. Настройка получения зеркалированного трафика со SPAN-портов	89
Шаг 13. Настройка интеграции с прокси-сервером по протоколу ICAP	90
Шаг 14. Настройка интеграции с почтовым сервером по протоколу POP3	90
Шаг 15. Настройка интеграции с почтовым сервером по протоколу SMTP	92
Шаг 16. Просмотр Положения о KSN и настройка участия в KSN	93

Шаг 1. Создание учетной записи для работы в меню администратора и в консоли управления сервером

► Чтобы создать учетную запись администратора для работы в меню администратора и в консоли управления сервером, выполните следующие действия:

1. В поле **Username** введите имя пользователя учетной записи администратора.
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**.

Мастер установки перейдет к следующему шагу.

Шаг 2. Назначение имени хоста

► Чтобы назначить имя хоста программы для использования DNS-серверами, выполните следующие действия:

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 3. Первоначальное включение сетевого интерфейса

Необходимо включить сетевые интерфейсы для последующей настройки их параметров.

После первого включения сетевого интерфейса вы сможете отключать и включать каждый сетевой интерфейс в окне настройки сетевого интерфейса.

► Чтобы впервые включить сетевой интерфейс, выполните следующие действия:

1. В списке сетевых интерфейсов выберите сетевой интерфейс, который вы хотите включить.

2. Нажмите на клавишу **ENTER**.

Откроется окно подтверждения включения сетевого интерфейса.

3. Нажмите на кнопку **Yes**.

Сетевой интерфейс будет включен.

4. Выберите **Continue**.

5. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 4. Настройка сетевого маршрута для использования по умолчанию

На этом шаге настройте сетевой маршрут, который программа будет использовать по умолчанию. Вы можете настроить сетевой маршрут с помощью DHCP-сервера или настроить статический сетевой маршрут.

Настройка сетевого маршрута с помощью DHCP-сервера

► Чтобы настроить сетевой маршрут с помощью DHCP-сервера, выполните следующие действия:

1. В списке **Default route** выберите **Interface**.

2. Нажмите на клавишу **ENTER**.

Откроется список сетевых интерфейсов.

3. Выберите сетевой интерфейс, для которого вы хотите настроить сетевой маршрут.

4. Нажмите на клавишу **ENTER**.

Мастер установки вернется к окну настройки сетевого маршрута.

Напротив названия параметра **Gateway** отобразится значение **dhcp**.

5. Выберите **Continue**.

6. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Настройка статического сетевого маршрута

► *Чтобы настроить статический сетевой маршрут, выполните следующие действия:*

1. В списке **Default route** выберите **Interface**.

2. Нажмите на клавишу **ENTER**.

Откроется список сетевых интерфейсов.

3. Выберите сетевой интерфейс, для которого вы хотите настроить сетевой маршрут.

4. Нажмите на клавишу **ENTER**.

Мастер установки вернется к окну настройки сетевого маршрута.

5. Выберите параметр **Gateway**.

6. Нажмите на клавишу **ENTER**.

Откроется окно подтверждения настройки статического сетевого маршрута.

7. Нажмите на кнопку **Yes**.

Откроется окно ввода статического адреса шлюза.

8. В поле **Gateway** введите статический адрес шлюза.

9. Нажмите на кнопку **Ok**.

Мастер установки вернется к окну настройки сетевого маршрута.

Напротив названия параметра **Gateway** отобразится статический адрес шлюза, который вы назначили.

10. Выберите **Continue**.

11. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 5. Настройка параметров DNS

На этом шаге настройте параметры DNS для работы серверов с компонентами программы. Вы можете настроить назначение DNS-адресов с помощью DHCP-сервера или настроить назначение статических DNS-адресов.

В этом разделе

Назначение DNS-адресов с помощью DHCP-сервера.....	84
Назначение статических DNS-адресов.....	84

Назначение DNS-адресов с помощью DHCP-сервера

Вам может понадобиться использовать DHCP-сервер для назначения DNS-адресов, если вы настраиваете Kaspersky Anti Targeted Attack Platform в тестовом режиме.

► *Чтобы назначить DNS-адреса с помощью DHCP-сервера, выполните следующие действия:*

1. В окне **Obtain DNS addresses over DHCP** выберите имя вашего сетевого интерфейса.
2. Нажмите на клавишу **ENTER**.
Отобразится окно настройки параметров DNS.
3. Убедитесь, что параметры **Search list**, **Primary DNS**, **Secondary DNS** имеют значение **dhcp**.
4. Выберите **Continue**.
5. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Назначение статических DNS-адресов

Рекомендуется назначить статические DNS-адреса, если вы настраиваете Kaspersky Anti Targeted Attack Platform не в тестовом режиме.

► *Чтобы назначить статические DNS-адреса, выполните следующие действия:*

1. В окне **Obtain DNS addresses over DHCP** выберите **no**.
2. Нажмите на клавишу **ENTER**.
Отобразится окно настройки параметров DNS.
3. Выберите любой параметр.
Например, параметр **Search list**.
4. Нажмите на клавишу **ENTER**.
Отобразится окно ввода статических DNS-адресов.
5. В поле **Search list** введите DNS-суффикс, который вы хотите использовать в Kaspersky Anti Targeted Attack Platform.
Например, example.com.
6. В поле **Primary** введите IP-адрес основного DNS-сервера в формате IPv4.
7. В поле **Secondary** введите IP-адрес дополнительного DNS-сервера в формате IPv4.
8. Нажмите на кнопку **Ok**.

Отобразится окно настройки параметров DNS с установленными статическими параметрами DNS.

9. Проверьте правильность установленных параметров DNS.
10. Выберите **Continue**.
11. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 6. Настройка параметров соединения с прокси-сервером

На этом шаге включите или отключите использование прокси-сервера для обновления баз и подключения к службе KSN, настройте параметры соединения с прокси-сервером, а также включите или отключите использование прокси-сервера при подключении к локальным адресам сети вашей организации.

В этом разделе

Включение и отключение использования прокси-сервера	85
Настройка параметров соединения с прокси-сервером	85
Включение и отключение использования прокси-сервера при подключении к локальным адресам	86

Включение и отключение использования прокси-сервера

- ▶ *Чтобы включить или отключить использование прокси-сервера, выполните следующие действия:*

1. Выберите параметр **Enabled**.
2. Нажмите на клавишу **ENTER**.

Если использование прокси-сервера было отключено, оно включится. Напротив названия параметра **Enabled** отобразится значение **yes**.

Если использование прокси-сервера было включено, оно отключится. Напротив названия параметра **Enabled** отобразится значение **no**.

Перейдите к настройке параметров соединения с прокси-сервером в текущем окне.

Настройка параметров соединения с прокси-сервером

- ▶ *Чтобы настроить параметры соединения с прокси-сервером, выполните следующие действия:*

1. В окне **Select Action - Proxy** выберите любой параметр.
Например, выберите параметр **Host**.
2. Нажмите на клавишу **ENTER**.

Отобразится окно настройки параметров соединения с прокси-сервером.

3. В поле **Proxy URL** введите URL-адрес прокси-сервера, порт подключения, а также имя пользователя и пароль, если вы хотите использовать аутентификацию на прокси-сервере.

Вводите данные в формате `http://<имя пользователя прокси-сервера>:<пароль пользователя прокси-сервера>@<IP-адрес или URL-адрес прокси-сервера>:<порт подключения к прокси-серверу>`

Например, <http://admin:password@10.1.1.1:3128>

4. Нажмите на кнопку **Ok**.

Окно настройки параметров соединения с прокси-сервером закроется.

В окне **Select Action - Proxy** отобразятся значения параметров соединения с прокси-сервером.

Перейдите к включению или отключению использования прокси-сервера при подключении к локальным адресам сети вашей организации в текущем окне.

Если сервер обновлений баз находится внутри IT-инфраструктуры вашей организации или вы используете KPSN, отключите использование прокси-сервера при подключении к локальным адресам сети вашей организации.

Включение и отключение использования прокси-сервера при подключении к локальным адресам

- ▶ Чтобы включить или отключить использование прокси-сервера при подключении к локальным адресам сети вашей организации, выполните следующие действия:

1. Выберите параметр **Local addresses**.
2. Нажмите на клавишу **ENTER**.

Если использование прокси-сервера при подключении к локальным адресам было отключено, оно включится. Напротив названия параметра **Local addresses** отобразится значение **use proxy**.

Если использование прокси-сервера при подключении к локальным адресам было включено, оно отключится. Напротив названия параметра **Local addresses** отобразится значение **bypass**.

3. Выберите **Continue**.
4. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 7. Установка часового пояса

- ▶ Чтобы установить часовой пояс для *Kaspersky Anti Targeted Attack Platform*, выполните следующие действия:

1. В окне **Select Timezone - Select Country** выберите страну из списка.
Например, выберите **Russia**.

2. Нажмите на клавишу **ENTER**.
Отобразится список часовых поясов, доступных для выбранной страны.
3. Выберите часовой пояс.
4. Нажмите на клавишу **ENTER**.
Отобразится окно подтверждения выбора часового пояса.
5. Если часовой пояс выбран верно, нажмите на кнопку **Yes**.

Мастер установки перейдет к следующему шагу.

Шаг 8. Настройка синхронизации времени с NTP-сервером

На этом шаге вы можете настроить синхронизацию времени сервера с NTP-сервером.

NTP (Network Time Protocol – протокол сетевого времени) – сетевой протокол для синхронизации внутренних часов компьютера с сервером точного времени в интернете.

► *Чтобы отказаться от синхронизации времени с NTP-сервером, выполните следующие действия:*

1. В окне **Use NTP to set clock** нажмите на кнопку **No**.
Откроется окно **Set the system clock manually**.
2. Нажмите на одну из следующих кнопок:
 - **No**, если вы не хотите вручную настроить время.
Мастер установки программы сразу перейдет к следующему шагу.
 - **Yes**, если вы хотите вручную настроить время.
Откроется окно **Set the system clock**, в котором вы можете настроить время.
3. По окончании настройки времени выберите **Continue**.
4. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

► *Чтобы включить синхронизацию времени с NTP-сервером, выполните следующие действия:*

1. В окне **Configure NTP servers** выберите **New**.
Откроется окно **Add NTP server**.
2. В поле **NTP server** введите IP-адрес или URL-адрес NTP-сервера, с которым вы хотите настроить синхронизацию времени.
3. Нажмите на кнопку **Ok**.
Окно **Add NTP server** закроется.
Адрес NTP-сервера добавится в список NTP-серверов в окне **Configure NTP servers**.
4. Выберите **Continue**.

5. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 9. Указание адреса сервера с компонентом Sandbox

► *Чтобы указать адрес сервера, на котором вы установили компонент Sandbox, выполните следующие действия:*

1. В окне **Sandbox access** в поле **Sandbox server** введите IP-адрес или URL-адрес сервера, на котором вы установили компонент Sandbox.
2. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 10. Создание учетной записи администратора веб-интерфейса

► *Чтобы создать учетную запись администратора веб-интерфейса программы, выполните следующие действия:*

1. В поле **Username** введите имя пользователя учетной записи администратора веб-интерфейса программы.

По умолчанию используется имя пользователя Administrator.

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**.

Мастер установки перейдет к следующему шагу.

Шаг 11. 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 отказаться от выделения диска,*

в окне **Use separate disk for TA Analyzer database** нажмите на кнопку **No**.

Мастер установки перейдет к следующему шагу.

► *Чтобы выделить диск, выполните следующие действия:*

1. В окне **Use separate disk for TA Analyzer database** нажмите на кнопку **Yes**.

Откроется окно выбора дисков.

2. Выберите диск, который вы хотите выделить для базы данных компонента Targeted Attack Analyzer.

3. Нажмите на клавишу **ENTER**.

Сервер перезагрузится.

Мастер установки перейдет к следующему шагу.

Шаг 12. Настройка получения зеркалированного трафика со SPAN-портов

На этом шаге вы можете настроить получение зеркалированного трафика со SPAN-портов.

SPAN (Switch Port Analyzer) – технология зеркалирования трафика с одного порта на другой.

SPAN-порт – порт, с которого можно получить зеркалированный трафик.

► *Чтобы отказаться от получения зеркалированного трафика со SPAN-портов,*

в окне **Enable SPAN traffic processing** нажмите на кнопку **No**.

Мастер установки перейдет к следующему шагу.

► *Чтобы настроить получение зеркалированного трафика со SPAN-портов, выполните следующие действия:*

1. В окне **Enable SPAN traffic processing** нажмите на кнопку **Yes**.

Откроется окно выбора сетевых интерфейсов.

По умолчанию получение зеркалированного трафика со SPAN-портов всех интерфейсов отключено.

Справа от названия сетевого интерфейса отображается значение **skip**.

2. Выберите сетевой интерфейс, с которого вы хотите настроить получение зеркалированного трафика.

Не настраивайте получение зеркалированного трафика с управляющего сетевого интерфейса сервера с компонентом Central Node.

3. Нажмите на клавишу **ENTER**.

Получение зеркалированного трафика со SPAN-портов выбранного интерфейса включится. Справа от названия сетевого интерфейса отобразится значение **capture**.

4. Если вы хотите настроить получение зеркалированного трафика для других сетевых интерфейсов, повторите действия 2–3 для каждого из них.
5. Выберите **Continue**.
6. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 13. Настройка интеграции с прокси-сервером по протоколу ICAP

На этом шаге вы можете настроить интеграцию Kaspersky Anti Targeted Attack Platform с прокси-сервером, используемым в вашей организации, по протоколу ICAP.

- ▶ Чтобы отказаться от интеграции Kaspersky Anti Targeted Attack Platform с прокси-сервером, в окне **Enable ICAP processing** нажмите на кнопку **No**.

Мастер установки перейдет к следующему шагу.

- ▶ Чтобы включить интеграцию Kaspersky Anti Targeted Attack Platform с прокси-сервером, выполните следующие действия:

1. В окне **Enable ICAP processing** нажмите на кнопку **Yes**.

Откроется окно с URI-адресом сервера, на который вы устанавливаете компонент Central Node.

Используйте этот URI-адрес для настройки интеграции с Kaspersky Anti Targeted Attack Platform по протоколу ICAP на прокси-сервере, используемом в вашей организации.

2. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 14. Настройка интеграции с почтовым сервером по протоколу POP3

На этом шаге вы можете настроить интеграцию с почтовым сервером по протоколу POP3 после предварительной подготовки IT-инфраструктуры вашей организации (см. раздел "Подготовка IT-инфраструктуры к интеграции с почтовым сервером для приема сообщений по протоколу POP3" на

стр. [56](#)).

- ▶ Чтобы отказаться от интеграции с почтовым сервером по протоколу POP3, в окне **Enable POP3 processing** нажмите на кнопку **No**.

Мастер установки перейдет к следующему шагу.

- ▶ Чтобы настроить интеграцию с почтовым сервером по протоколу POP3, выполните следующие действия:

1. В окне **Enable POP3 processing** нажмите на кнопку **Yes**.

Откроется окно настройки интеграции с почтовым сервером по протоколу POP3.

2. Выберите параметр **Server**.

3. Нажмите на клавишу **ENTER**.

Откроется окно **POP3 server**.

4. В поле **Server** введите IP-адрес почтового сервера, с которым вы хотите настроить интеграцию.

5. Нажмите на кнопку **Ok**.

Мастер установки вернется к окну настройки интеграции с почтовым сервером по протоколу POP3.

6. Выберите параметр **Encrypted**.

7. Нажмите на клавишу **ENTER**.

- Если шифрованное соединение с почтовым сервером было отключено, оно включится. Напротив названия параметра **Encrypted** отобразится значение **yes**.
- Если шифрованное соединение с почтовым сервером было включено, оно отключится. Напротив названия параметра **Encrypted** отобразится значение **no**.

8. Выберите параметр **Username**.

9. Нажмите на клавишу **ENTER**.

Откроется окно **POP3 access**.

10. В поле **Username** введите имя учетной записи для доступа к почтовому серверу по протоколу POP3.

11. В поле **Password** введите пароль доступа к почтовому серверу.

12. Нажмите на кнопку **Ok**.

Мастер установки вернется к окну настройки интеграции с почтовым сервером по протоколу POP3.

13. Выберите параметр **Check interval**.

14. Нажмите на клавишу **ENTER**.

Откроется окно **Check interval**.

15. В поле **Check interval** введите частоту соединения с почтовым сервером в секундах.

16. Нажмите на кнопку **Ok**.

Мастер установки вернется к окну настройки интеграции с почтовым сервером по протоколу POP3.

17. Выберите **Continue**.

18. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 15. Настройка интеграции с почтовым сервером по протоколу SMTP

На этом шаге вы можете настроить интеграцию с почтовым сервером по протоколу SMTP после предварительной подготовки ИТ-инфраструктуры вашей организации (см. раздел "Подготовка ИТ-инфраструктуры к интеграции с почтовым сервером для отправки сообщений по протоколу SMTP" на стр. 57).

- ▶ Чтобы отказаться от интеграции с почтовым сервером по протоколу SMTP, в окне **Enable SMTP processing** нажмите на кнопку **No**.

Мастер установки перейдет к следующему шагу.

- ▶ Чтобы настроить интеграцию с почтовым сервером по протоколу SMTP, выполните следующие действия:
 1. В окне **Enable SMTP processing** нажмите на кнопку **Yes**.
Откроется окно настройки интеграции с почтовым сервером по протоколу SMTP.
 2. Выберите параметр **Clients**.
 3. Нажмите на клавишу **ENTER**.
Откроется окно **Configure Networks**.
 4. Выберите параметр **New**.
 5. Нажмите на клавишу **ENTER**.
 6. В поле **Network address** введите адрес почтового сервера, с которым Kaspersky Anti Targeted Attack Platform разрешено взаимодействовать по протоколу SMTP.
Если вы оставите адрес почтового сервера пустым, Kaspersky Anti Targeted Attack Platform будет принимать сообщения от всех серверов.
 7. Нажмите на кнопку **Ok**.
 8. Выберите параметр **Domains**.
 9. Нажмите на клавишу **ENTER**.
Откроется окно **Configure domains**.
 10. Выберите параметр **New**.
 11. Нажмите на клавишу **ENTER**.
 12. В поле **Domain** введите имя почтового домена или поддомена, на который администратор почтового сервера должен настроить отправку скрытой копии сообщений.
Если вы оставите имя почтового домена пустым, Kaspersky Anti Targeted Attack Platform будет принимать сообщения, отправленные на любые адреса электронной почты.
 13. Нажмите на кнопку **Ok**.
 14. Выберите параметр **TLS encryption**.

15. Нажмите на клавишу **ENTER**.

Откроется окно **Select TLS encryption level**.

16. Выберите один из следующих вариантов TLS-шифрования соединения с почтовым сервером по протоколу SMTP:

- **none**, если вы не хотите устанавливать TLS-шифрование соединения.
- **optional**, если вы хотите, чтобы сервер Kaspersky Anti Targeted Attack Platform поддерживал TLS-шифрование соединения.
- **mandatory**, если вы хотите, чтобы сервер Kaspersky Anti Targeted Attack Platform требовал TLS-шифрования соединения от почтового сервера.

17. Нажмите на клавишу **ENTER**.

18. Выберите параметр **Client certs**.

19. Нажмите на клавишу **ENTER**.

Откроется окно **Select TLS client certificates use**.

20. Выберите один из следующих вариантов проверки TLS-сертификата клиента при соединении с почтовым сервером по протоколу SMTP:

- **ignore**, если вы не хотите проверять TLS-сертификат клиента.
- **optional**, если вы хотите, чтобы сервер Kaspersky Anti Targeted Attack Platform поддерживал проверку TLS-сертификата клиента.
- **mandatory**, если вы хотите, чтобы сервер Kaspersky Anti Targeted Attack Platform требовал TLS-сертификат клиента.

21. Выберите параметр **Message size**.

22. Нажмите на клавишу **ENTER**.

Откроется окно **Message size limit**.

23. В поле **Message size limit** задайте максимальный размер принимаемого сообщения. Максимальный размер принимаемого сообщения не может быть больше 10 МБ.

24. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 16. Просмотр Положения о KSN и настройка участия в KSN

На этом шаге вы можете просмотреть Положение о KSN, принять его условия или отказаться участвовать в KSN.

Использование Kaspersky Security Network приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Kaspersky Private Security Network или отказаться от использования KSN. Для получения подробной информации см. *Руководство администратора Kaspersky Private Security Network*.

Участие в KSN

► Чтобы просмотреть Положение о KSN и принять его условия, выполните следующие действия:

1. Нажмите на кнопку **Yes**.

Откроется окно **Participation in Kaspersky Security Network**.

2. Выберите язык для просмотра Положения о KSN в списке.

Например, если вы хотите просмотреть Положение о KSN на английском языке, выберите **English**.

3. Нажмите на клавишу **ENTER**.

Откроется окно с текстом Положения о KSN.

4. Просмотрите Положение о KSN.

5. Нажмите на кнопку **I accept the terms**.

Сервер перезагрузится.

Установка компонентов Central Node и Sensor на одном сервере завершится.

Отказ от участия в KSN

► Чтобы отказаться от участия в KSN,

нажмите на кнопку **No**.

Сервер перезагрузится.

Установка компонентов Central Node и Sensor на одном сервере завершится.

Установка и настройка компонента Central Node на отдельном сервере

Этот раздел представляет собой пошаговую инструкцию по установке и предварительной настройке компонента Central Node на отдельном сервере.

Если вы разворачиваете компонент Central Node в гипервизоре VMware ESXi и планируете, что компонент Central Node будет получать зеркалированный трафик от нескольких виртуальных сетей, вам нужно произвести предварительную настройку ESX-сервера, на котором вы хотите развернуть компонент Central Node.

► *Чтобы произвести предварительную настройку ESX-сервера, на котором вы хотите развернуть компонент Central Node, выполните следующие действия в гипервизоре VMware ESXi:*

1. Запустите программу VMware vSphere Client.
2. В списке ESX-серверов выберите ESX-сервер, предварительную настройку которого вы хотите произвести.
3. Нажатием правой кнопки мыши раскройте меню.
4. Выберите пункт меню **Configuration**.
Откроется окно изменения конфигурации ESX-сервера.
5. В разделе **Hardware** выберите пункт **Networking**.
Откроется окно изменения параметров.
6. На закладке **Ports** выберите раздел **VM Network**.
Откроется окно **VM Network Properties**.
7. На закладке **General** в списке **VLAN ID (Optional)** выберите значение **All**.
8. Нажмите на кнопку **Ok**.

Компонент Central Node сможет получать зеркалированный трафик от нескольких виртуальных сетей.

В этом разделе

Шаг 1. Создание учетной записи для работы в меню администратора и в консоли управления сервером.....	96
Шаг 2. Назначение имени хоста	97
Шаг 3. Первоначальное включение сетевого интерфейса	97
Шаг 4. Настройка сетевого маршрута для использования по умолчанию	97
Шаг 5. Настройка параметров DNS.....	98
Шаг 6. Настройка параметров соединения с прокси-сервером.....	100
Шаг 7. Установка часового пояса	101
Шаг 8. Настройка синхронизации времени с NTP-сервером	102
Шаг 9. Указание адреса сервера с компонентом Sandbox.....	103
Шаг 10. Создание учетной записи администратора веб-интерфейса	103
Шаг 11. Выделение диска для базы данных компонента Targeted Attack Analyzer	103
Шаг 12. Просмотр Положения о KSN и настройка участия в KSN	104

Шаг 1. Создание учетной записи для работы в меню администратора и в консоли управления сервером

► Чтобы создать учетную запись администратора для работы в меню администратора и в консоли управления сервером, выполните следующие действия:

1. В поле **Username** введите имя пользователя учетной записи администратора.
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**.

Мастер установки перейдет к следующему шагу.

Шаг 2. Назначение имени хоста

► Чтобы назначить имя хоста программы для использования DNS-серверами, выполните следующие действия:

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 3. Первоначальное включение сетевого интерфейса

Необходимо включить сетевые интерфейсы для последующей настройки их параметров.

После первого включения сетевого интерфейса вы сможете отключать и включать каждый сетевой интерфейс в окне настройки сетевого интерфейса.

► Чтобы впервые включить сетевой интерфейс, выполните следующие действия:

1. В списке сетевых интерфейсов выберите сетевой интерфейс, который вы хотите включить.

2. Нажмите на клавишу **ENTER**.

Откроется окно подтверждения включения сетевого интерфейса.

3. Нажмите на кнопку **Yes**.

Сетевой интерфейс будет включен.

4. Выберите **Continue**.

5. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 4. Настройка сетевого маршрута для использования по умолчанию

На этом шаге настройте сетевой маршрут, который программа будет использовать по умолчанию. Вы можете настроить сетевой маршрут с помощью DHCP-сервера или настроить статический сетевой маршрут.

Настройка сетевого маршрута с помощью DHCP-сервера

► Чтобы настроить сетевой маршрут с помощью DHCP-сервера, выполните следующие действия:

1. В списке **Default route** выберите **Interface**.

2. Нажмите на клавишу **ENTER**.

Откроется список сетевых интерфейсов.

3. Выберите сетевой интерфейс, для которого вы хотите настроить сетевой маршрут.
4. Нажмите на клавишу **ENTER**.
Мастер установки вернется к окну настройки сетевого маршрута.
Напротив названия параметра **Gateway** отобразится значение **dhcp**.
5. Выберите **Continue**.
6. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Настройка статического сетевого маршрута

► *Чтобы настроить статический сетевой маршрут, выполните следующие действия:*

1. В списке **Default route** выберите **Interface**.
2. Нажмите на клавишу **ENTER**.
Откроется список сетевых интерфейсов.
3. Выберите сетевой интерфейс, для которого вы хотите настроить сетевой маршрут.
4. Нажмите на клавишу **ENTER**.
Мастер установки вернется к окну настройки сетевого маршрута.
5. Выберите параметр **Gateway**.
6. Нажмите на клавишу **ENTER**.
Откроется окно подтверждения настройки статического сетевого маршрута.
7. Нажмите на кнопку **Yes**.
Откроется окно ввода статического адреса шлюза.
8. В поле **Gateway** введите статический адрес шлюза.
9. Нажмите на кнопку **Ok**.
Мастер установки вернется к окну настройки сетевого маршрута.
Напротив названия параметра **Gateway** отобразится статический адрес шлюза, который вы назначили.
10. Выберите **Continue**.
11. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 5. Настройка параметров DNS

На этом шаге настройте параметры DNS для работы серверов с компонентами программы. Вы можете настроить назначение DNS-адресов с помощью DHCP-сервера или настроить назначение статических DNS-адресов.

В этом разделе

Назначение DNS-адресов с помощью DHCP-сервера.....	99
Назначение статических DNS-адресов.....	99

Назначение DNS-адресов с помощью DHCP-сервера

Вам может понадобиться использовать DHCP-сервер для назначения DNS-адресов, если вы настраиваете Kaspersky Anti Targeted Attack Platform в тестовом режиме.

► *Чтобы назначить DNS-адреса с помощью DHCP-сервера, выполните следующие действия:*

1. В окне **Obtain DNS addresses over DHCP** выберите имя вашего сетевого интерфейса.
2. Нажмите на клавишу **ENTER**.
Отобразится окно настройки параметров DNS.
3. Убедитесь, что параметры **Search list**, **Primary DNS**, **Secondary DNS** имеют значение **dhcp**.
4. Выберите **Continue**.
5. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Назначение статических DNS-адресов

Рекомендуется назначить статические DNS-адреса, если вы настраиваете Kaspersky Anti Targeted Attack Platform не в тестовом режиме.

► *Чтобы назначить статические DNS-адреса, выполните следующие действия:*

1. В окне **Obtain DNS addresses over DHCP** выберите **no**.
2. Нажмите на клавишу **ENTER**.
Отобразится окно настройки параметров DNS.
3. Выберите любой параметр.
Например, параметр **Search list**.
4. Нажмите на клавишу **ENTER**.
Отобразится окно ввода статических DNS-адресов.
5. В поле **Search list** введите DNS-суффикс, который вы хотите использовать в Kaspersky Anti Targeted Attack Platform.
Например, example.com.
6. В поле **Primary** введите IP-адрес основного DNS-сервера в формате IPv4.
7. В поле **Secondary** введите IP-адрес дополнительного DNS-сервера в формате IPv4.
8. Нажмите на кнопку **Ok**.

Отобразится окно настройки параметров DNS с установленными статическими параметрами DNS.

9. Проверьте правильность установленных параметров DNS.
10. Выберите **Continue**.
11. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 6. Настройка параметров соединения с прокси-сервером

На этом шаге включите или отключите использование прокси-сервера для обновления баз и подключения к службе KSN, настройте параметры соединения с прокси-сервером, а также включите или отключите использование прокси-сервера при подключении к локальным адресам сети вашей организации.

В этом разделе

Включение и отключение использования прокси-сервера	100
Настройка параметров соединения с прокси-сервером	100
Включение и отключение использования прокси-сервера при подключении к локальным адресам	101

Включение и отключение использования прокси-сервера

- ▶ *Чтобы включить или отключить использование прокси-сервера, выполните следующие действия:*

1. Выберите параметр **Enabled**.
2. Нажмите на клавишу **ENTER**.

Если использование прокси-сервера было отключено, оно включится. Напротив названия параметра **Enabled** отобразится значение **yes**.

Если использование прокси-сервера было включено, оно отключится. Напротив названия параметра **Enabled** отобразится значение **no**.

Перейдите к настройке параметров соединения с прокси-сервером в текущем окне.

Настройка параметров соединения с прокси-сервером

- ▶ *Чтобы настроить параметры соединения с прокси-сервером, выполните следующие действия:*

1. В окне **Select Action - Proxy** выберите любой параметр.
Например, выберите параметр **Host**.
2. Нажмите на клавишу **ENTER**.

Отобразится окно настройки параметров соединения с прокси-сервером.

3. В поле **Proxy URL** введите URL-адрес прокси-сервера, порт подключения, а также имя пользователя и пароль, если вы хотите использовать аутентификацию на прокси-сервере.

Вводите данные в формате `http://<имя пользователя прокси-сервера>:<пароль пользователя прокси-сервера>@<IP-адрес или URL-адрес прокси-сервера>:<порт подключения к прокси-серверу>`

Например, <http://admin:password@10.1.1.1:3128>

4. Нажмите на кнопку **Ok**.

Окно настройки параметров соединения с прокси-сервером закрывается.

В окне **Select Action - Proxy** отобразятся значения параметров соединения с прокси-сервером.

Перейдите к включению или отключению использования прокси-сервера при подключении к локальным адресам сети вашей организации в текущем окне.

Если сервер обновлений баз находится внутри IT-инфраструктуры вашей организации или вы используете KPSN, отключите использование прокси-сервера при подключении к локальным адресам сети вашей организации.

Включение и отключение использования прокси-сервера при подключении к локальным адресам

- Чтобы включить или отключить использование прокси-сервера при подключении к локальным адресам сети вашей организации, выполните следующие действия:

1. Выберите параметр **Local addresses**.
2. Нажмите на клавишу **ENTER**.

Если использование прокси-сервера при подключении к локальным адресам было отключено, оно включится. Напротив названия параметра **Local addresses** отобразится значение **use proxy**.

Если использование прокси-сервера при подключении к локальным адресам было включено, оно отключится. Напротив названия параметра **Local addresses** отобразится значение **bypass**.

3. Выберите **Continue**.
4. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 7. Установка часового пояса

- Чтобы установить часовой пояс для Kaspersky Anti Targeted Attack Platform, выполните следующие действия:

1. В окне **Select Timezone - Select Country** выберите страну из списка.

Например, выберите **Russia**.

2. Нажмите на клавишу **ENTER**.

Отобразится список часовых поясов, доступных для выбранной страны.

3. Выберите часовой пояс.

4. Нажмите на клавишу **ENTER**.
Отобразится окно подтверждения выбора часового пояса.
5. Если часовой пояс выбран верно, нажмите на кнопку **Yes**.

Мастер установки перейдет к следующему шагу.

Шаг 8. Настройка синхронизации времени с NTP-сервером

На этом шаге вы можете настроить синхронизацию времени сервера с NTP-сервером.

NTP (Network Time Protocol – протокол сетевого времени) – сетевой протокол для синхронизации внутренних часов компьютера с сервером точного времени в интернете.

► *Чтобы отказаться от синхронизации времени с NTP-сервером, выполните следующие действия:*

1. В окне **Use NTP to set clock** нажмите на кнопку **No**.
Откроется окно **Set the system clock manually**.
2. Нажмите на одну из следующих кнопок:
 - **No**, если вы не хотите вручную настроить время.
Мастер установки программы сразу перейдет к следующему шагу.
 - **Yes**, если вы хотите вручную настроить время.
Откроется окно **Set the system clock**, в котором вы можете настроить время.
3. По окончании настройки времени выберите **Continue**.
4. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

► *Чтобы включить синхронизацию времени с NTP-сервером, выполните следующие действия:*

1. В окне **Configure NTP servers** выберите **New**.
Откроется окно **Add NTP server**.
2. В поле **NTP server** введите IP-адрес или URL-адрес NTP-сервера, с которым вы хотите настроить синхронизацию времени.
3. Нажмите на кнопку **Ok**.
Окно **Add NTP server** закроется.
Адрес NTP-сервера добавится в список NTP-серверов в окне **Configure NTP servers**.
4. Выберите **Continue**.
5. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 9. Указание адреса сервера с компонентом Sandbox

► Чтобы указать адрес сервера, на котором вы установили компонент Sandbox, выполните следующие действия:

1. В окне **Sandbox access** в поле **Sandbox server** введите IP-адрес или URL-адрес сервера, на котором вы установили компонент Sandbox.
2. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 10. Создание учетной записи администратора веб-интерфейса

► Чтобы создать учетную запись администратора веб-интерфейса программы, выполните следующие действия:

1. В поле **Username** введите имя пользователя учетной записи администратора веб-интерфейса программы.

По умолчанию используется имя пользователя Administrator.

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**.

Мастер установки перейдет к следующему шагу.

Шаг 11. 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 отказаться от выделения диска,*

в окне **Use separate disk for TA Analyzer database** нажмите на кнопку **No**.

Мастер установки перейдет к следующему шагу.

► *Чтобы выделить диск, выполните следующие действия:*

1. В окне **Use separate disk for TA Analyzer database** нажмите на кнопку **Yes**.

Откроется окно выбора дисков.

2. Выберите диск, который вы хотите выделить для базы данных компонента Targeted Attack Analyzer.

3. Нажмите на клавишу **ENTER**.

Сервер перезагрузится.

Мастер установки перейдет к следующему шагу.

Шаг 12. Просмотр Положения о KSN и настройка участия в KSN

На этом шаге вы можете просмотреть Положение о KSN, принять его условия или отказаться участвовать в KSN.

Использование Kaspersky Security Network приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Kaspersky Private Security Network или отказаться от использования KSN. Для получения подробной информации см. *Руководство администратора Kaspersky Private Security Network*.

Участие в KSN

► *Чтобы просмотреть Положение о KSN и принять его условия, выполните следующие действия:*

1. Нажмите на кнопку **Yes**.

Откроется окно **Participation in Kaspersky Security Network**.

2. Выберите язык для просмотра Положения о KSN в списке.

Например, если вы хотите просмотреть Положение о KSN на английском языке, выберите **English**.

3. Нажмите на клавишу **ENTER**.

Откроется окно с текстом Положения о KSN.

4. Просмотрите Положение о KSN.

5. Нажмите на кнопку **I accept the terms**.

Сервер перезагрузится.

Установка компонентов Central Node и Sensor на одном сервере завершится.

Отказ от участия в KSN

► *Чтобы отказаться от участия в KSN,*

нажмите на кнопку **No**.

Сервер перезагрузится.

Установка компонентов Central Node и Sensor на одном сервере завершится.

Установка и настройка компонента Sensor на отдельном сервере

Этот раздел представляет собой пошаговую инструкцию по установке и предварительной настройке компонента Sensor на отдельном сервере.

В этом разделе

Шаг 1. Создание учетной записи для работы в меню администратора и в консоли управления сервером.....	106
Шаг 2. Назначение имени хоста	107
Шаг 3. Первоначальное включение сетевого интерфейса	107
Шаг 4. Настройка сетевого маршрута для использования по умолчанию	108
Шаг 5. Настройка параметров DNS.....	109
Шаг 6. Настройка параметров соединения с прокси-сервером.....	110
Шаг 7. Установка часового пояса	111
Шаг 8. Настройка синхронизации времени с NTP-сервером	112
Шаг 9. Указание адреса сервера с компонентом Central Node.....	113
Шаг 10. Настройка получения зеркалированного трафика со SPAN-портов	113
Шаг 11. Настройка интеграции с прокси-сервером по протоколу ICAP	114
Шаг 12. Настройка интеграции с почтовым сервером по протоколу POP3	114
Шаг 13. Настройка интеграции с почтовым сервером по протоколу SMTP	115
Шаг 14. Просмотр Положения о KSN и настройка участия в KSN	117

Шаг 1. Создание учетной записи для работы в меню администратора и в консоли управления сервером

► Чтобы создать учетную запись администратора для работы в меню администратора и в консоли управления сервером, выполните следующие действия:

1. В поле **Username** введите имя пользователя учетной записи администратора.
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**.

Мастер установки перейдет к следующему шагу.

Шаг 2. Назначение имени хоста

► *Чтобы назначить имя хоста программы для использования DNS-серверами, выполните следующие действия:*

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 3. Первоначальное включение сетевого интерфейса

Необходимо включить сетевые интерфейсы для последующей настройки их параметров.

После первого включения сетевого интерфейса вы сможете отключать и включать каждый сетевой интерфейс в окне настройки сетевого интерфейса.

► *Чтобы впервые включить сетевой интерфейс, выполните следующие действия:*

1. В списке сетевых интерфейсов выберите сетевой интерфейс, который вы хотите включить.
2. Нажмите на клавишу **ENTER**.
Откроется окно подтверждения включения сетевого интерфейса.
3. Нажмите на кнопку **Yes**.
Сетевой интерфейс будет включен.
4. Выберите **Continue**.
5. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 4. Настройка сетевого маршрута для использования по умолчанию

На этом шаге настройте сетевой маршрут, который программа будет использовать по умолчанию. Вы можете настроить сетевой маршрут с помощью DHCP-сервера или настроить статический сетевой маршрут.

Настройка сетевого маршрута с помощью DHCP-сервера

► *Чтобы настроить сетевой маршрут с помощью DHCP-сервера, выполните следующие действия:*

1. В списке **Default route** выберите **Interface**.
2. Нажмите на клавишу **ENTER**.
Откроется список сетевых интерфейсов.
3. Выберите сетевой интерфейс, для которого вы хотите настроить сетевой маршрут.
4. Нажмите на клавишу **ENTER**.
Мастер установки вернется к окну настройки сетевого маршрута.
Напротив названия параметра **Gateway** отобразится значение **dhcp**.
5. Выберите **Continue**.
6. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Настройка статического сетевого маршрута

► *Чтобы настроить статический сетевой маршрут, выполните следующие действия:*

1. В списке **Default route** выберите **Interface**.
2. Нажмите на клавишу **ENTER**.
Откроется список сетевых интерфейсов.
3. Выберите сетевой интерфейс, для которого вы хотите настроить сетевой маршрут.
4. Нажмите на клавишу **ENTER**.
Мастер установки вернется к окну настройки сетевого маршрута.
5. Выберите параметр **Gateway**.
6. Нажмите на клавишу **ENTER**.
Откроется окно подтверждения настройки статического сетевого маршрута.
7. Нажмите на кнопку **Yes**.
Откроется окно ввода статического адреса шлюза.
8. В поле **Gateway** введите статический адрес шлюза.
9. Нажмите на кнопку **Ok**.

Мастер установки вернется к окну настройки сетевого маршрута.

Напротив названия параметра **Gateway** отобразится статический адрес шлюза, который вы назначили.

10. Выберите **Continue**.

11. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 5. Настройка параметров DNS

На этом шаге настройте параметры DNS для работы серверов с компонентами программы. Вы можете настроить назначение DNS-адресов с помощью DHCP-сервера или настроить назначение статических DNS-адресов.

В этом разделе

Назначение DNS-адресов с помощью DHCP-сервера.....	109
Назначение статических DNS-адресов.....	109

Назначение DNS-адресов с помощью DHCP-сервера

Вам может понадобиться использовать DHCP-сервер для назначения DNS-адресов, если вы настраиваете Kaspersky Anti Targeted Attack Platform в тестовом режиме.

► *Чтобы назначить DNS-адреса с помощью DHCP-сервера, выполните следующие действия:*

1. В окне **Obtain DNS addresses over DHCP** выберите имя вашего сетевого интерфейса.
2. Нажмите на клавишу **ENTER**.
Отобразится окно настройки параметров DNS.
3. Убедитесь, что параметры **Search list**, **Primary DNS**, **Secondary DNS** имеют значение **dhcp**.
4. Выберите **Continue**.
5. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Назначение статических DNS-адресов

Рекомендуется назначить статические DNS-адреса, если вы настраиваете Kaspersky Anti Targeted Attack Platform не в тестовом режиме.

► *Чтобы назначить статические DNS-адреса, выполните следующие действия:*

1. В окне **Obtain DNS addresses over DHCP** выберите **no**.
2. Нажмите на клавишу **ENTER**.

- Отобразится окно настройки параметров DNS.
3. Выберите любой параметр.
Например, параметр **Search list**.
 4. Нажмите на клавишу **ENTER**.
Отобразится окно ввода статических DNS-адресов.
 5. В поле **Search list** введите DNS-суффикс, который вы хотите использовать в Kaspersky Anti Targeted Attack Platform.
Например, example.com.
 6. В поле **Primary** введите IP-адрес основного DNS-сервера в формате IPv4.
 7. В поле **Secondary** введите IP-адрес дополнительного DNS-сервера в формате IPv4.
 8. Нажмите на кнопку **Ok**.
Отобразится окно настройки параметров DNS с установленными статическими параметрами DNS.
 9. Проверьте правильность установленных параметров DNS.
 10. Выберите **Continue**.
 11. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 6. Настройка параметров соединения с прокси-сервером

На этом шаге включите или отключите использование прокси-сервера для обновления баз и подключения к службе KSN, настройте параметры соединения с прокси-сервером, а также включите или отключите использование прокси-сервера при подключении к локальным адресам сети вашей организации.

В этом разделе

Включение и отключение использования прокси-сервера при подключении к локальным адресам	110
Настройка параметров соединения с прокси-сервером	111

Включение и отключение использования прокси-сервера при подключении к локальным адресам

- *Чтобы включить или отключить использование прокси-сервера при подключении к локальным адресам сети вашей организации, выполните следующие действия:*

1. Выберите параметр **Local addresses**.
2. Нажмите на клавишу **ENTER**.

Если использование прокси-сервера при подключении к локальным адресам было отключено, оно включится. Напротив названия параметра **Local addresses** отобразится значение **use proxy**.

Если использование прокси-сервера при подключении к локальным адресам было включено, оно отключится. Напротив названия параметра **Local addresses** отобразится значение **bypass**.

3. Выберите **Continue**.
4. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Настройка параметров соединения с прокси-сервером

► Чтобы настроить параметры соединения с прокси-сервером, выполните следующие действия:

1. В окне **Select Action - Proxy** выберите любой параметр.
Например, выберите параметр **Host**.
2. Нажмите на клавишу **ENTER**.
Отобразится окно настройки параметров соединения с прокси-сервером.
3. В поле **Proxy URL** введите URL-адрес прокси-сервера, порт подключения, а также имя пользователя и пароль, если вы хотите использовать аутентификацию на прокси-сервере.

Вводите данные в формате `http://<имя пользователя прокси-сервера>:<пароль пользователя прокси-сервера>@<IP-адрес или URL-адрес прокси-сервера>:<порт подключения к прокси-серверу>`

Например, <http://admin:password@10.1.1.1:3128>

4. Нажмите на кнопку **Ok**.
Окно настройки параметров соединения с прокси-сервером закроется.

В окне **Select Action - Proxy** отобразятся значения параметров соединения с прокси-сервером.

Перейдите к включению или отключению использования прокси-сервера при подключении к локальным адресам сети вашей организации в текущем окне.

Если сервер обновлений баз находится внутри IT-инфраструктуры вашей организации или вы используете KPSN, отключите использование прокси-сервера при подключении к локальным адресам сети вашей организации.

Шаг 7. Установка часового пояса

► Чтобы установить часовой пояс для *Kaspersky Anti Targeted Attack Platform*, выполните следующие действия:

1. В окне **Select Timezone - Select Country** выберите страну из списка.
Например, выберите **Russia**.
2. Нажмите на клавишу **ENTER**.
Отобразится список часовых поясов, доступных для выбранной страны.
3. Выберите часовой пояс.

4. Нажмите на клавишу **ENTER**.
Отобразится окно подтверждения выбора часового пояса.
5. Если часовой пояс выбран верно, нажмите на кнопку **Yes**.

Мастер установки перейдет к следующему шагу.

Шаг 8. Настройка синхронизации времени с NTP-сервером

На этом шаге вы можете настроить синхронизацию времени сервера с NTP-сервером.

NTP (Network Time Protocol – протокол сетевого времени) – сетевой протокол для синхронизации внутренних часов компьютера с сервером точного времени в интернете.

► *Чтобы отказаться от синхронизации времени с NTP-сервером, выполните следующие действия:*

1. В окне **Use NTP to set clock** нажмите на кнопку **No**.
Откроется окно **Set the system clock manually**.
2. Нажмите на одну из следующих кнопок:
 - **No**, если вы не хотите вручную настроить время.
Мастер установки программы сразу перейдет к следующему шагу.
 - **Yes**, если вы хотите вручную настроить время.
Откроется окно **Set the system clock**, в котором вы можете настроить время.
3. По окончании настройки времени выберите **Continue**.
4. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

► *Чтобы включить синхронизацию времени с NTP-сервером, выполните следующие действия:*

1. В окне **Configure NTP servers** выберите **New**.
Откроется окно **Add NTP server**.
2. В поле **NTP server** введите IP-адрес или URL-адрес NTP-сервера, с которым вы хотите настроить синхронизацию времени.
3. Нажмите на кнопку **Ok**.
Окно **Add NTP server** закроется.
Адрес NTP-сервера добавится в список NTP-серверов в окне **Configure NTP servers**.
4. Выберите **Continue**.
5. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 9. Указание адреса сервера с компонентом Central Node

► Чтобы указать адрес сервера, на котором вы установили компонент Central Node, выполните следующие действия:

1. В окне **Connection to Central Node** в поле **Central Node** введите IP-адрес или URL-адрес сервера, на котором вы установили компонент Central Node.
2. Нажмите на кнопку **Ok**.

Мастер установки подключится к серверу с компонентом Central Node и 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.

SPAN-порт – порт, с которого можно получить зеркалированный трафик.

► Чтобы отказаться от получения зеркалированного трафика со SPAN-портов,

в окне **Enable SPAN traffic processing** нажмите на кнопку **No**.

Мастер установки перейдет к следующему шагу.

► Чтобы настроить получение зеркалированного трафика со SPAN-портов, выполните следующие действия:

1. В окне **Enable SPAN traffic processing** нажмите на кнопку **Yes**.

Откроется окно выбора сетевых интерфейсов.

По умолчанию получение зеркалированного трафика со SPAN-портов всех сетевых интерфейсов отключено. Справа от названия сетевого интерфейса отображается значение **skip**.

2. Выберите сетевой интерфейс, с которого вы хотите настроить получение зеркалированного трафика.

Не настраивайте получение зеркалированного трафика с управляющего сетевого интерфейса сервера с компонентом Central Node.

3. Нажмите на клавишу **ENTER**.

Получение зеркалированного трафика со SPAN-портов выбранного сетевого интерфейса включится. Справа от названия сетевого интерфейса отобразится значение **capture**.

4. Если вы хотите настроить получение зеркалированного трафика для других сетевых интерфейсов, повторите действия 2–3 для каждого из них.
5. Выберите **Continue**.
6. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 11. Настройка интеграции с прокси-сервером по протоколу ICAP

На этом шаге вы можете настроить интеграцию Kaspersky Anti Targeted Attack Platform с прокси-сервером, используемым в вашей организации, по протоколу ICAP.

- ▶ *Чтобы отказаться от интеграции Kaspersky Anti Targeted Attack Platform с прокси-сервером,*
в окне **Enable ICAP processing** нажмите на кнопку **No**.

Мастер установки перейдет к следующему шагу.

- ▶ *Чтобы включить интеграцию Kaspersky Anti Targeted Attack Platform с прокси-сервером,*
выполните следующие действия:
 1. В окне **Enable ICAP processing** нажмите на кнопку **Yes**.
Откроется окно с URI-адресом сервера, на который вы устанавливаете компонент Central Node.
Используйте этот URI-адрес для настройки интеграции с Kaspersky Anti Targeted Attack Platform по протоколу ICAP на прокси-сервере, который используется в вашей организации.
 2. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 12. Настройка интеграции с почтовым сервером по протоколу POP3

На этом шаге вы можете настроить интеграцию с почтовым сервером по протоколу POP3 после предварительной подготовки ИТ-инфраструктуры вашей организации (см. раздел "Подготовка ИТ-инфраструктуры к интеграции с почтовым сервером для приема сообщений по протоколу POP3" на стр. [56](#)).

- ▶ *Чтобы отказаться от интеграции с почтовым сервером по протоколу POP3,*
в окне **Enable POP3 processing** нажмите на кнопку **No**.

Мастер установки перейдет к следующему шагу.

- ▶ *Чтобы настроить интеграцию с почтовым сервером по протоколу POP3, выполните следующие действия:*
 1. В окне **Enable POP3 processing** нажмите на кнопку **Yes**.
Откроется окно настройки интеграции с почтовым сервером по протоколу POP3.
 2. Выберите параметр **Server**.
 3. Нажмите на клавишу **ENTER**.
Откроется окно **POP3 server**.
 4. В поле **Server** введите IP-адрес почтового сервера, с которым вы хотите настроить интеграцию.

5. Нажмите на кнопку **Ok**.
Мастер установки вернется к окну настройки интеграции с почтовым сервером по протоколу POP3.
6. Выберите параметр **Encrypted**.
7. Нажмите на клавишу **ENTER**.
 - Если шифрованное соединение с почтовым сервером было отключено, оно включится. Напротив названия параметра **Encrypted** отобразится значение **yes**.
 - Если шифрованное соединение с почтовым сервером было включено, оно отключится. Напротив названия параметра **Encrypted** отобразится значение **no**.
8. Выберите параметр **Username**.
9. Нажмите на клавишу **ENTER**.
Откроется окно **POP3 access**.
10. В поле **Username** введите имя учетной записи для доступа к почтовому серверу по протоколу POP3.
11. В поле **Password** введите пароль доступа к почтовому серверу.
12. Нажмите на кнопку **Ok**.
Мастер установки вернется к окну настройки интеграции с почтовым сервером по протоколу POP3.
13. Выберите параметр **Check interval**.
14. Нажмите на клавишу **ENTER**.
Откроется окно **Check interval**.
15. В поле **Check interval** введите частоту соединения с почтовым сервером в секундах.
16. Нажмите на кнопку **Ok**.
Мастер установки вернется к окну настройки интеграции с почтовым сервером по протоколу POP3.
17. Выберите **Continue**.
18. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 13. Настройка интеграции с почтовым сервером по протоколу SMTP

На этом шаге вы можете настроить интеграцию с почтовым сервером по протоколу SMTP после предварительной подготовки ИТ-инфраструктуры вашей организации (см. раздел "Подготовка ИТ-инфраструктуры к интеграции с почтовым сервером для отправки сообщений по протоколу SMTP" на стр. [57](#)).

- ▶ *Чтобы отказаться от интеграции с почтовым сервером по протоколу SMTP,*
в окне **Enable SMTP processing** нажмите на кнопку **No**.

Мастер установки перейдет к следующему шагу.

- ▶ *Чтобы настроить интеграцию с почтовым сервером по протоколу SMTP, выполните*

следующие действия:

1. В окне **Enable SMTP processing** нажмите на кнопку **Yes**.
Откроется окно настройки интеграции с почтовым сервером по протоколу SMTP.
2. Выберите параметр **Clients**.
3. Нажмите на клавишу **ENTER**.
Откроется окно **Configure Networks**.
4. Выберите параметр **New**.
5. Нажмите на клавишу **ENTER**.
6. В поле **Network address** введите адрес почтового сервера, с которым Kaspersky Anti Targeted Attack Platform разрешено взаимодействовать по протоколу SMTP.
Если вы оставите адрес почтового сервера пустым, Kaspersky Anti Targeted Attack Platform будет принимать сообщения от всех серверов.
7. Нажмите на кнопку **Ok**.
8. Выберите параметр **Domains**.
9. Нажмите на клавишу **ENTER**.
Откроется окно **Configure domains**.
10. Выберите параметр **New**.
11. Нажмите на клавишу **ENTER**.
12. В поле **Domain** введите имя почтового домена или поддомена, на который администратор почтового сервера должен настроить отправку скрытой копии сообщений.
Если вы оставите имя почтового домена пустым, Kaspersky Anti Targeted Attack Platform будет принимать сообщения, отправленные на любые адреса электронной почты.
13. Нажмите на кнопку **Ok**.
14. Выберите параметр **TLS encryption**.
15. Нажмите на клавишу **ENTER**.
Откроется окно **Select TLS encryption level**.
16. Выберите один из следующих вариантов TLS-шифрования соединения с почтовым сервером по протоколу SMTP:
 - **none**, если вы не хотите устанавливать TLS-шифрование соединения.
 - **optional**, если вы хотите, чтобы сервер Kaspersky Anti Targeted Attack Platform поддерживал TLS-шифрование соединения.
 - **mandatory**, если вы хотите, чтобы сервер Kaspersky Anti Targeted Attack Platform требовал TLS-шифрования соединения от почтового сервера.
17. Нажмите на клавишу **ENTER**.
18. Выберите параметр **Client certs**.
19. Нажмите на клавишу **ENTER**.
Откроется окно **Select TLS client certificates use**.
20. Выберите один из следующих вариантов проверки TLS-сертификата клиента при соединении с

почтовым сервером по протоколу SMTP:

- **ignore**, если вы не хотите проверять TLS-сертификат клиента.
- **optional**, если вы хотите, чтобы сервер Kaspersky Anti Targeted Attack Platform поддерживал проверку TLS-сертификата клиента.
- **mandatory**, если вы хотите, чтобы сервер Kaspersky Anti Targeted Attack Platform требовал TLS-сертификат клиента.

21. Выберите параметр **Message size**.

22. Нажмите на клавишу **ENTER**.

Откроется окно **Message size limit**.

23. В поле **Message size limit** задайте максимальный размер принимаемого сообщения. Максимальный размер принимаемого сообщения не может быть больше 10 МБ.

24. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 14. Просмотр Положения о KSN и настройка участия в KSN

На этом шаге вы можете просмотреть Положение о KSN, принять его условия или отказаться участвовать в KSN.

Использование Kaspersky Security Network приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Kaspersky Private Security Network или отказаться от использования KSN. Для получения подробной информации см. *Руководство администратора Kaspersky Private Security Network*.

Участие в KSN

► Чтобы просмотреть Положение о KSN и принять его условия, выполните следующие действия:

1. Нажмите на кнопку **Yes**.

Откроется окно **Participation in Kaspersky Security Network**.

2. Выберите язык для просмотра Положения о KSN в списке.

Например, если вы хотите просмотреть Положение о KSN на английском языке, выберите **English**.

3. Нажмите на клавишу **ENTER**.

Откроется окно с текстом Положения о KSN.

4. Просмотрите Положение о KSN.

5. Нажмите на кнопку **I accept the terms**.

Сервер перезагрузится.

Установка компонентов Central Node и Sensor на одном сервере завершится.

Отказ от участия в KSN

► Чтобы отказаться от участия в KSN,

нажмите на кнопку **№**.

Сервер перезагрузится.

Установка компонентов Central Node и Sensor на одном сервере завершится.

Настройка перенаправления трафика с компонентов Endpoint Sensors на компонент Sensor

Вы можете использовать сервер с компонентом Sensor в качестве прокси-сервера при обмене данными между компонентами Endpoint Sensors 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.
- Максимальное количество компьютеров с компонентом Endpoint Sensors составляет 1000 шт.
- 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.

Выполняйте действия по усилению безопасности SSL-соединения сервера с компонентом Sensor с сервером Central Node аналогично действиям с компонентом Endpoint Sensors и компонентом Central Node в следующем порядке:

1. Используйте сертификат, автоматически созданный в процессе установки программы, созданный на сервере с компонентом Sensor вручную (см. стр. [124](#)) или созданный самостоятельно и загруженный на сервер с компонентом Sensor (см. стр. [125](#)).
2. Подготовьте SSL-сертификат и загрузите его в Active Directory® (см. стр. [126](#)).

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 настройке параметров компонента Endpoint Sensors (см. раздел "Создание установочного пакета Endpoint Sensors" на стр. [129](#)) вместо IP-адреса Central Node вы указали IP-адрес компонента Sensor.

В этом разделе

Включение и отключение перенаправления трафика с компонентов Endpoint Sensors	119
Авторизация компонента Sensor на сервере с компонентом Central Node	120

Включение и отключение перенаправления трафика с компонентов Endpoint Sensors

- Чтобы включить или отключить использование компонента Sensor в качестве прокси-сервера при обмене данными между компонентами Endpoint Sensors и компонентом Central Node, выполните следующие действия в меню администратора сервера с

компонентом *Sensor* (см. раздел "Начало работы в меню администратора программы" на стр. [141](#)):

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**.
10. В открывшемся окне **Update source** выполните одно из следующих действий:
 - Если вы хотите использовать сервер с компонентом Central Node в качестве источника обновления баз программы, нажмите на кнопку **Yes**.
 - Если вы не хотите использовать сервер с компонентом Central Node в качестве источника обновления баз программы, нажмите на кнопку **No**.
11. Если вы хотите использовать компонент *Sensor* в качестве прокси-сервера, в открывшемся окне **Enable Proxy to Central Node** нажмите на кнопку **Yes**.
Использование компонента *Sensor* в качестве прокси-сервера будет включено после подтверждения авторизации на сервере с компонентом Central Node.
12. Если вы уже используете компонент *Sensor* в качестве прокси-сервера и хотите отключить его, в открывшемся окне **Proxy to Central Node** 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 с компонентом 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 программы" на стр. [141](#)):

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.

Установка и удаление компонента Endpoint Sensors

Этот раздел представляет собой инструкцию по установке и удалению компонента Endpoint Sensors.

Если вы установите программу Kaspersky Endpoint Security на компьютер с компонентом Endpoint Sensors, компонент Endpoint Sensors будет удален независимо от того, включен ли компонент Endpoint Sensors в состав программы Kaspersky Endpoint Security или нет.

В этом разделе

Установка компонента Endpoint Sensors	122
Подготовка SSL-соединения к обмену данными между компонентами Endpoint Sensors и Central Node	123
Удаление компонента Endpoint Sensors	128

Установка компонента Endpoint Sensors

Для установки компонента Endpoint Sensors ваша учетная запись должна обладать правами локального администратора.

Перед установкой новой версии компонента Endpoint Sensors убедитесь, что на локальном компьютере не установлена предыдущая версия этого компонента.

► Чтобы установить компонент Endpoint Sensors на компьютеры, с которых Kaspersky Anti Targeted Attack Platform получает и обрабатывает данные, выполните следующие действия:

1. Загрузите установочный файл компонента Endpoint Sensors на компьютер любым доступным способом.
2. Запустите на компьютере приложение для работы в командной строке.
3. В командной строке введите следующую команду:

```
msiexec /i "<путь к установочному файлу компонента Endpoint Sensors с указанием имени файла и расширения msi>" /qn /l*v <путь к журналу установки>\install.log SERVER=<адрес сервера с компонентом Central Node> acceptEULA=1
```

Если вы используете компонент Sensor в качестве прокси-сервера, вместо IP-адреса или FQDN-имени Central Node укажите IP-адрес или FQDN-имя сервера с компонентом Sensor.

4. Нажмите на клавишу **ENTER**.

Установка компонента Endpoint Sensors завершится.

Вы также можете установить компонент Endpoint Sensors с помощью утилиты Orca.exe компании Microsoft или удаленно, как объект групповой политики Microsoft Windows. Подробнее об этих способах установки см. в документации компании Microsoft.

Подготовка SSL-соединения к обмену данными между компонентами Endpoint Sensors и Central Node

Компонент Endpoint Sensors наблюдает за процессами, открытыми сетевыми соединениями и изменяемыми файлами на компьютерах, на которых он установлен, и отправляет данные наблюдения на сервер с компонентом Central Node. По результатам проверки этих данных компонентом Central Node компонент Endpoint Sensors также может отправить файлы, дампы и карты памяти, связанные с обнаруженными событиями, на сервер с компонентом Central Node.

Чтобы компонент Endpoint Sensors мог отправлять файлы, дампы и карты памяти на сервер с компонентом Central Node, вам нужно усилить безопасность SSL-соединения компонента Endpoint Sensors с сервером Central Node.

Вы можете усилить безопасность SSL-соединения компьютеров с компонентом Endpoint Sensors с сервером Central Node при соблюдении следующих условий конфигурации локальной сети вашей организации:

- В локальной сети вашей организации развернуты доменные службы Active Directory.
- Компьютеры, на которых установлен компонент Endpoint Sensors, подключены к Active Directory.

Выполняйте действия по усилению безопасности SSL-соединения компьютеров с компонентом Endpoint Sensors с сервером Central Node в следующем порядке:

1. Скачайте SSL-сертификат с сервера с компонентом Central Node (см. стр. [124](#)).

Вы можете скачать сертификат, автоматически созданный на сервере с компонентом Central Node в процессе установки программы, созданный на сервере с компонентом Central Node вручную (см. стр. [124](#)) или созданный самостоятельно и загруженный на сервер с компонентом Central Node (см. стр. [125](#)).

2. Подготовьте SSL-сертификат и загрузите его в Active Directory (см. стр. [126](#)).

В этом разделе

Скачивание SSL-сертификата с сервера с компонентом Central Node	124
Создание SSL-сертификата на сервере с компонентом Central Node	124
Загрузка самостоятельно подготовленного SSL-сертификата на сервер с компонентом Central Node	125
Подготовка и загрузка SSL-сертификата в Active Directory.....	126

Скачивание SSL-сертификата с сервера с компонентом Central Node

Вы можете скачать SSL-сертификат с сервера с компонентом Central Node на любой компьютер, имеющий доступ к серверу с компонентом Central Node, 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 SSL-сертификат.

► Чтобы скачать SSL-сертификат с сервера с компонентом Central Node 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 Central Node>:ssl/kata.crt .`
2. На приглашение ввести пароль введите пароль администратора для работы в меню администратора сервера с компонентом Central Node, заданный при установке компонента Central Node (см. стр. [152](#)).

SSL-сертификат будет загружен с сервера с компонентом Central Node в текущую директорию.

Создание SSL-сертификата на сервере с компонентом Central Node

► Чтобы создать SSL-сертификат на сервере с компонентом Central Node, выполните следующие действия в меню администратора сервера с компонентом Central Node (см. раздел "Начало работы в меню администратора программы" на стр. [141](#)):

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 SSL-сертификата на сервер с компонентом Central Node

Вы можете самостоятельно подготовить SSL-сертификат и загрузить его на сервер с компонентом Central Node 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 SSL-сертификат.

Файл SSL-сертификата, предназначенный для загрузки на сервер с компонентом Central Node, 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 SSL-сертификатов к импорту см. в документации Open SSL.

► *Чтобы загрузить самостоятельно подготовленный SSL-сертификат на сервер с компонентом Central Node 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 Central Node>:`
2. На приглашение ввести пароль введите пароль администратора для работы в меню администратора сервера с компонентом Central Node, заданный при установке компонента Central Node (см. стр. [152](#)).

SSL-сертификат будет загружен на сервер с компонентом Central Node.

► *Чтобы применить загруженный SSL-сертификат на сервере с компонентом Central Node, выполните следующие действия в меню администратора сервера с компонентом Central Node (см. раздел "Начало работы в меню администратора программы" на стр. [141](#)):*

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.

Подготовка и загрузка SSL-сертификата в Active Directory

► Чтобы подготовить и загрузить SSL-сертификат в Active Directory, выполните следующие действия для каждого сервера с компонентом Central Node:

1. Выберите контейнер Active Directory для размещения сертификата. Компонент Endpoint Sensors поддерживает поиск объекта serviceConnectionPoint в следующих расположениях (в порядке очередности поиска):
 - `ldap://CN=<Active Directory Site, в котором находится компьютер с компонентом Endpoint Sensors>,CN=Sites,<configurationPartition>`
 - `ldap://CN=Services, <раздел конфигурации Active Directory>`

Публиковать сертификат в контейнере Sites рекомендуется, если для какого-либо из Active Directory Site развернут отдельный компонент Central Node.

2. В выбранном контейнере создайте объект типа serviceConnectionPoint.
3. Откройте SSL-сертификат сервера с компонентом Central Node в формате PEM в текстовом редакторе и выполните следующие действия:
 - a. Удалите строки BEGIN CERTIFICATE и END CERTIFICATE.
 - b. Удалите все переносы строк.
4. Заполните атрибуты serviceConnectionPoint следующим образом:
 - keywords содержит строку-идентификатор 013D90F9-517B-486D-A7E8-888439D1DD61.
 - serviceDNSName в точности совпадает с адресом сервера Central Node, указанным при установке

компонента Endpoint Sensors.

Если в качестве адреса при установке задан IP-адрес, атрибут должен содержать тот же IP-адрес. Если в качестве адреса при установке задано FQDN-имя сервера, атрибут должен содержать то же FQDN-имя сервера.

- `serviceBindingInformation` содержит SSL-сертификат сервера с компонентом Central Node в формате PEM в одну строку.

Компонент Endpoint Sensors ищет объект `serviceConnectionPoint` последовательно сначала в контейнере Sites, затем в контейнере Services. Используется первый найденный объект, у которого атрибут `keywords` содержит уникальный идентификатор, а атрибут `serviceDnsName` в точности совпадает с адресом сервера Central Node, заданным при установке компонента Endpoint Sensors.

Если в одном и том же контейнере Active Directory располагаются два и более объекта `serviceConnectionPoint`, у которых атрибут `keywords` содержит уникальный идентификатор, а значения `serviceDnsName` совпадают, компонент Endpoint Sensors будет иметь ограниченную функциональность.

Если компонент Endpoint Sensors не может декодировать значение атрибута `serviceBindingInformation` в бинарный формат или если значение атрибута – пустая строка, компонент Endpoint Sensors будет иметь ограниченную функциональность.

Удаление компонента Endpoint Sensors

Для удаления компонента Endpoint Sensors с компьютера локальной сети организации ваша учетная запись должна обладать правами локального администратора.

Вы можете удалить компонент Endpoint Sensors средствами операционной системы Microsoft Windows, установленной на компьютере локальной сети организации. Процедура удаления зависит от версии операционной системы. Подробнее об удалении программ средствами операционной системы Microsoft Windows смотрите в документации компании Microsoft.

При удалении компонента Endpoint Sensors удаляются следующие данные:

- Все данные, накопленные в процессе работы компонента Endpoint Sensors на компьютере.
- Конфигурационный файл из системной папки Program Data, подпапки Kaspersky Lab\Anti-APT Agent 3.1.
- Ветка реестра HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Endpoint Sensor 3.1\protected (для 32-разрядной операционной системы), HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Endpoint Sensor 3.1 (для 64-разрядной операционной системы) и все хранящиеся в ней ключи.

После удаления компонента Endpoint Sensors необходимо перезагрузить компьютер, на котором он был установлен.

Управление компонентами Endpoint Sensors в консоли администрирования Kaspersky Security Center

Вы можете устанавливать, удалять и удаленно управлять компонентами Endpoint Sensors из Консоли администрирования Kaspersky Security Center (далее также "консоль KSC").

Подробную информацию о работе в консоли KSC см. в *Справке Kaspersky Security Center*.

Если у вас установлен Endpoint Sensors в составе Kaspersky Endpoint Security (далее также "KES"), вам не нужно создавать установочный пакет, устанавливать или удалять компонент Endpoint Sensors.

Если вы установите программу Kaspersky Endpoint Security на компьютер с компонентом Endpoint Sensors, компонент Endpoint Sensors будет удален независимо от того, включен ли компонент Endpoint Sensors в состав программы Kaspersky Endpoint Security или нет.

Вы можете получить подробную информацию об установке компонента Endpoint Sensors в Kaspersky Endpoint Security из *Руководства администратора Kaspersky Endpoint Security*.

В этом разделе

Создание установочного пакета Endpoint Sensors	129
Удаленная установка компонента Endpoint Sensors	131
Удаленное изменение параметров компонента Endpoint Sensors	132
Удаленная деинсталляция компонента Endpoint Sensors	134
Удаленный запуск и остановка компонента Endpoint Sensors.....	135
Создание политики для удаленного управления компонентом Endpoint Sensors	135
Изменение параметров политики для удаленного управления компонентом Endpoint Sensors	136

Создание установочного пакета Endpoint Sensors

Для создания установочного пакета используйте дистрибутив компонента Endpoint Sensors (файл с расширением msi, входящий в инсталляционный комплект).

Если у вас установлен компонент Endpoint Sensors в составе KES, вам не нужно дополнительно создавать установочный пакет и устанавливать или удалять компонент Endpoint Sensors. Вы можете получить подробную информацию об установке компонента Endpoint Sensors в Kaspersky Endpoint Security из *Руководства администратора Kaspersky Endpoint Security*.

- Чтобы создать установочный пакет для удаленной установки компонента *Endpoint Sensors*, выполните следующие действия:

1. Откройте консоль KSC.
2. Выберите нужный Сервер администрирования.
3. В дереве консоли KSC в разделе с дополнительными параметрами выберите подраздел с установочными пакетами.
4. Запустите создание установочного пакета.

Откроется окно мастера создания установочного пакета.

5. Если вы используете программу Kaspersky Security Center 10 SP3, выполните следующие действия:
 - a. В окне мастера создания установочного пакета выберите установочный пакет программы "Лаборатории Касперского".

Не рекомендуется выбирать создание установочного пакета сторонней программы, так как в этом случае некоторые функции удаленного управления компонентом *Endpoint Sensors* будут недоступны.

- b. Укажите путь к файлу в формате KUD и имя нового установочного пакета.
 - c. Ознакомьтесь с Лицензионным соглашением на этот компонент.

Внимательно прочитайте Лицензионное соглашение. Если вы согласны со всеми его пунктами, примите условия Лицензионного соглашения.

После этого создание установочного пакета будет продолжено. В процессе создания установочного пакета в программу Kaspersky Security Center будет установлен плагин для управления компонентом *Endpoint Sensors*, если вы не установили его ранее.

- d. Укажите адрес и порт сервера с компонентом Central Node, а также статус самозащиты.

Если вы используете компонент *Sensor* в качестве прокси-сервера, вместо IP-адреса или FQDN-имени Central Node укажите IP-адрес или FQDN-имя сервера с компонентом *Sensor*.

Значения по умолчанию: порт 443, адрес сервера не задан, самозащита включена.

Самозащита запускает механизм защиты компонента *Endpoint Sensors* от изменения или удаления собственных файлов на диске, процессов в памяти и записей в системном реестре. Изменить статус самозащиты компонента *Endpoint Sensors* в дальнейшем можно только при переустановке компонента.

6. Если вы используете программу Kaspersky Security Center 10 SP2 MR1 или Kaspersky Security Center 10 SP2, в окне мастера создания установочного пакета выберите создание установочного пакета сторонней программы и укажите следующие параметры в командной строке:

- SELFDEFENSE=On/Off – статус самозащиты.

По умолчанию самозащита включена.

Самозащита запускает механизм защиты компонента *Endpoint Sensors* от изменения или удаления собственных файлов на диске, процессов в памяти и записей в системном реестре.

Изменить статус самозащиты компонента Endpoint Sensors в дальнейшем можно только при переустановке компонента.

- SERVER=<адрес сервера> – адрес сервера с компонентом Central Node.

Если вы используете компонент Sensor в качестве прокси-сервера, вместо IP-адреса или FQDN-имени Central Node укажите IP-адрес или FQDN-имя сервера с компонентом Sensor.

По умолчанию адрес сервера не задан.

- acceptEULA=1 – принятие условий Лицензионного соглашения.

Вы можете ознакомиться с условиями Лицензионного соглашения, прочитав документ license.txt. Этот документ включен в инсталляционный комплект программы. Если вы согласны со всеми пунктами Лицензионного соглашения, примите условия Лицензионного соглашения.

- MESSAGEQUEUEPRINTMESSAGESTOLOG=1 – запись событий в журнал на сервере с компонентом Central Node.

Необязательный параметр.

Постоянное использование записи событий в журнал приводит к быстрому заполнению свободного места на диске. Используйте запись событий в журнал только в случае необходимости.

Также вы можете указать следующие параметры записи событий в журнал:

- TRACELEVEL=500, если вы хотите записывать в журнал только ошибки.
- TRACELEVEL=800, если вы хотите использовать запись событий в журнал в режиме отладки.

О настройке дополнительных параметров вы можете узнать, обратившись в Службу технической поддержки.

После завершения работы мастера созданный установочный пакет будет отображаться в рабочей области папки с установочными пакетами.

Удаленная установка компонента Endpoint Sensors

Если у вас установлен компонент Endpoint Sensors в составе KES, вам не нужно дополнительно создавать установочный пакет и устанавливать или удалять компонент Endpoint Sensors. Вы можете получить подробную информацию об установке компонента Endpoint Sensors в Kaspersky Endpoint Security из *Руководства администратора Kaspersky Endpoint Security*.

Перед установкой новой версии компонента Endpoint Sensors убедитесь, что на локальном компьютере не установлена предыдущая версия этого компонента.

Вы можете удаленно установить компонент Endpoint Sensors на компьютер с помощью программы Kaspersky Security Center 10 SP3, Kaspersky Security Center 10 SP2 MR1 или Kaspersky Security Center 10 SP2.

Вы можете получить подробную информацию об установке компонента Endpoint Sensors в Kaspersky Endpoint Security из *Руководства администратора Kaspersky Endpoint Security*.

► *Чтобы удаленно установить компонент Endpoint Sensors на компьютеры локальной сети организации, выполните следующие действия:*

1. Откройте консоль KSC.
2. Выберите нужный Сервер администрирования.
3. В дереве консоли KSC выберите раздел с задачами.
4. В рабочей области выберите создание задачи.
Запустится мастер создания задачи.
5. В мастере создания задачи выберите создание задачи удаленной установки приложения.
6. Выберите группу администрирования или отдельные компьютеры, на которые вы хотите установить компонент Endpoint Sensors.
7. Оставьте без изменений значения параметров по умолчанию.

В результате работы мастера создания задачи будет создана задача удаленной установки. Созданная задача разместится в папке с задачами или добавится к задачам группы администрирования, для которой она была создана.

Удаленное изменение параметров компонента Endpoint Sensors

Вы можете удаленно изменить параметры компонента Endpoint Sensors, переустановив его на компьютерах локальной сети организации.

► *Чтобы удаленно изменить параметры компонента Endpoint Sensors на компьютерах локальной сети организации, выполните следующие действия:*

1. Откройте консоль KSC.
2. Выберите нужный Сервер администрирования.
3. В дереве консоли KSC в разделе с дополнительными параметрами выберите подраздел с установочными пакетами.
4. Запустите создание установочного пакета.
Откроется окно мастера создания установочного пакета.
5. Если вы используете программу Kaspersky Security Center 10 SP3, выполните следующие действия:
 - a. В окне мастера создания установочного пакета выберите установочный пакет программы "Лаборатории Касперского".

b. Укажите путь к файлу в формате KUD и имя нового установочного пакета.

c. Ознакомьтесь с Лицензионным соглашением на этот компонент.

Внимательно прочитайте Лицензионное соглашение. Если вы согласны со всеми его пунктами, примите условия Лицензионного соглашения.

После этого создание установочного пакета будет продолжено. В процессе создания установочного пакета в программу Kaspersky Security Center будет установлен плагин для управления компонентом Endpoint Sensors, если вы не установили его ранее.

d. Укажите адрес и порт сервера с компонентом Central Node, а также статус самозащиты.

Если вы используете компонент Sensor в качестве прокси-сервера, вместо IP-адреса или FQDN-имени Central Node укажите IP-адрес или FQDN-имя сервера с компонентом Sensor.

Значения по умолчанию: порт 443, адрес сервера не задан, самозащита включена.

Самозащита запускает механизм защиты компонента Endpoint Sensors от изменения или удаления собственных файлов на диске, процессов в памяти и записей в системном реестре. Изменить статус самозащиты компонента Endpoint Sensors в дальнейшем можно только при переустановке компонента.

6. Если вы используете программу Kaspersky Security Center 10 SP2 MR1 или Kaspersky Security Center 10 SP2, в окне мастера создания установочного пакета выберите создание установочного пакета сторонней программы и укажите следующие параметры в командной строке:

- SELFDEFENSE=On/Off – статус самозащиты.

По умолчанию самозащита включена.

Самозащита запускает механизм защиты компонента Endpoint Sensors от изменения или удаления собственных файлов на диске, процессов в памяти и записей в системном реестре. Изменить статус самозащиты компонента Endpoint Sensors в дальнейшем можно только при переустановке компонента.

- SERVER=<адрес сервера> – адрес сервера с компонентом Central Node.

Если вы используете компонент Sensor в качестве прокси-сервера, вместо IP-адреса или FQDN-имени Central Node укажите IP-адрес или FQDN-имя сервера с компонентом Sensor.

По умолчанию адрес сервера не задан.

- acceptEULA=1 – принятие условий Лицензионного соглашения.

Внимательно прочитайте Лицензионное соглашение. Если вы согласны со всеми его пунктами, примите условия Лицензионного соглашения.

- MESSAGEQUEUEPRINTMESSAGESTOLOG=1 – запись событий в журнал на сервере с компонентом Central Node.

Необязательный параметр.

Постоянное использование записи событий в журнал приводит к быстрому заполнению свободного места на диске. Используйте запись событий в журнал только в случае необходимости.

Также вы можете указать следующие параметры записи событий в журнал:

- TRACELEVEL=500, если вы хотите записывать в журнал только ошибки.
- TRACELEVEL=800, если вы хотите использовать запись событий в журнал в режиме отладки.

О настройке дополнительных параметров вы можете узнать, обратившись в Службу технической поддержки.

7. В рабочей области выберите установочный пакет компонента Endpoint Sensors.
8. В блоке работы с выбранным объектом запустите установку программы.
Запустится мастер удаленной установки.
9. Выберите компьютеры, на которые вы хотите установить компонент Endpoint Sensors.
Вы можете выбрать группу администрирования или отдельные устройства.
10. Оставьте без изменений значения параметров по умолчанию.

В результате работы мастера будет создана и запущена задача удаленной установки компонента Endpoint Sensors с новыми значениями параметров. Созданная задача разместится в папке с задачами или добавится к задачам группы администрирования, для которой она была создана.

Удаленная деинсталляция компонента Endpoint Sensors

Если у вас установлен компонент Endpoint Sensors в составе KES, вам не нужно дополнительно создавать установочный пакет и устанавливать или удалять компонент Endpoint Sensors. Вы можете получить подробную информацию об установке компонента Endpoint Sensors в Kaspersky Endpoint Security из *Руководства администратора Kaspersky Endpoint Security*.

Вы можете удаленно деинсталлировать компонент Endpoint Sensors с компьютера с помощью программы Kaspersky Security Center 10 SP3. Удаленная деинсталляция компонента Endpoint Sensors с компьютера с помощью программ Kaspersky Security Center 10 SP2 MR1 или Kaspersky Security Center 10 SP2 не поддерживается.

- ▶ Чтобы удаленно деинсталлировать компонент Endpoint Sensors на компьютерах локальной сети организации, выполните следующие действия:
 1. Откройте консоль KSC.
 2. Выберите нужный Сервер администрирования.
 3. В дереве консоли KSC выберите папку с задачами.

4. Запустите процесс создания задачи.
Откроется окно мастера создания задачи.
5. Выберите задачу удаленной деинсталляции.
6. В списке программ Kaspersky Security Center выберите компонент Endpoint Sensors.
7. Выберите группу администрирования или набор устройств, с которых вы хотите удалить компонент Endpoint Sensors.
8. Укажите имя задачи и время запуска.

Созданная задача отображается в рабочей области папки с задачами. В результате выполнения задачи удаленной деинсталляции компонент Endpoint Sensors будет удален с выбранных устройств.

Удаленный запуск и остановка компонента Endpoint Sensors

Вы можете временно отключить компонент Endpoint Sensors, если он мешает работе пользователя, а затем включить его. Не рекомендуется отключать компонент надолго, так как это снижает безопасность локальной сети организации.

► *Чтобы запустить или остановить компонент Endpoint Sensors на компьютере локальной сети организации, выполните следующие действия:*

1. Откройте консоль KSC.
2. Выберите нужный Сервер администрирования.
3. В дереве консоли KSC выберите устройство, на котором вы хотите остановить или запустить компонент Endpoint Sensors.
4. С помощью контекстного меню перейдите в окно свойств компонента.
5. Если вы хотите остановить или запустить компонент Endpoint Sensors, использующийся в составе KES, выберите закладку с задачами.
6. Если вы хотите остановить или запустить компонент Endpoint Sensors, не входящий в состав KES, выберите закладку с приложениями.
7. На открывшейся закладке выберите компонент Endpoint Sensors.
8. Остановите или запустите компонент Endpoint Sensors.

После остановки компонент Endpoint Sensors прекратит наблюдение за процессами, открытыми сетевыми соединениями и изменяемыми файлами, а также отправку данных наблюдения на сервер с компонентом Central Node.

Создание политики для удаленного управления компонентом Endpoint Sensors

Вы можете создать политику для удаленного управления компонентом Endpoint Sensors на компьютере с помощью программы Kaspersky Security Center 10 SP3.

Если у вас установлен компонент Endpoint Sensors в составе KES, вам не нужно дополнительно создавать

политику.

Вы можете получить подробную информацию об установке компонента Endpoint Sensors в Kaspersky Endpoint Security из *Руководства администратора Kaspersky Endpoint Security*.

Для работы с политиками в программе Kaspersky Security Center должен быть установлен плагин управления компонентом Endpoint Sensors. Подробную информацию об установке плагина управления в Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

► Чтобы создать политику для удаленного управления компонентом Endpoint Sensors, выполните следующие действия:

1. Откройте консоль KSC.
2. Выберите нужный Сервер администрирования.
3. В дереве консоли KSC выберите раздел с политиками.
4. Запустите мастер создания политики.
Откроется окно мастера создания политики.
5. Укажите имя политики.
6. Укажите адрес и порт сервера с компонентом Central Node.

Если вы используете компонент Sensor в качестве прокси-сервера, вместо IP-адреса или FQDN-имени Central Node укажите IP-адрес или FQDN-имя сервера с компонентом Sensor.

Значения по умолчанию: порт 443, адрес сервера не задан.

7. Выберите группу компьютеров, к которой будет применена политика.
8. Сделайте новую политику активной.

После завершения работы мастера будет создана новая политика. Список всех политик отображается в папке политик дерева консоли KSC.

Изменение параметров политики для удаленного управления компонентом Endpoint Sensors

Вы можете изменить параметры политики для удаленного управления компонентом Endpoint Sensors на компьютере с помощью программы Kaspersky Security Center 10 SP3.

► Чтобы изменить параметры политики для удаленного управления компонентом Endpoint Sensors, выполните следующие действия:

1. Откройте консоль KSC.
2. Выберите нужный Сервер администрирования.
3. В дереве консоли KSC в разделе с политиками выберите политику, параметры которой вы хотите изменить.

4. С помощью контекстного меню перейдите в окно свойств политики.
5. Внесите необходимые изменения.

Вы можете изменить:

- параметры отображения компонентов Endpoint Sensors разных типов в журнале состояний;
- время хранения компонентов Endpoint Sensors разных типов в журнале состояний;
- адрес и порт сервера с компонентом Central Node.

Если вы используете компонент Sensor в качестве прокси-сервера, вместо IP-адреса или FQDN-имени Central Node укажите IP-адрес или FQDN-имя сервера с компонентом Sensor.

6. Примените изменения.

Изменения политики будут сохранены.

Получение данных от компонента Endpoint Sensors в консоли администрирования Kaspersky Security Center

Вы можете получать данные о состоянии компонента Endpoint Sensors из Консоли администрирования Kaspersky Security Center.

Подробную информацию о работе в консоли KSC см. в *Справке Kaspersky Security Center*.

В этом разделе

Создание выборки компьютеров по наличию на них или свойствам компонентов Endpoint Sensors [138](#)

Получение данных о состоянии компонента Endpoint Sensors на определенном компьютере [140](#)

Создание выборки компьютеров по наличию на них или свойствам компонентов Endpoint Sensors

► Чтобы создать выборку компьютеров по свойствам компонентов Endpoint Sensors или наличию на компьютерах компонентов Endpoint Sensors, выполните следующие действия:

1. Откройте консоль KSC.
2. Выберите нужный Сервер администрирования.
3. В дереве консоли KSC в разделе выбора устройств создайте новую выборку.
4. В свойствах выборки добавьте условие, созданное по умолчанию.
5. Откройте свойства нового условия.
6. Дополните условие по умолчанию в соответствии с желаемым результатом с помощью тегов. Также вы можете переходить в другие разделы для совершения дополнительных действий по поиску необходимой информации о компонентах Endpoint Sensors.

Например, если вы хотите получить список компьютеров, на которых компонент Endpoint Sensors остановлен, включите в условие по умолчанию регулярное выражение `KATA:server address*` и статус компонента Endpoint Sensors `Stopped` в разделе статусов компонентов.

Таблица 2. Параметры создания выборки компьютеров с компонентом Endpoint Sensors

Список компьютеров, на которых...	Регулярное выражение	Необходимое действие	Дополнительные действия
...установлен компонент Endpoint Sensors.	<code>KATA:*</code>	Включить	Нет значения.
...не установлен компонент Endpoint Sensors.	<code>KATA:*</code>	Исключить	Нет значения.

Список компьютеров, на которых...	Регулярное выражение	Необходимое действие	Дополнительные действия
...установлен компонент Endpoint Sensors, настроенный на соединение с любым компонентом Central Node.	<code>KATA:server address*</code>	Включить	Нет значения.
...установлен компонент Endpoint Sensors, настроенный на соединение с определенным компонентом Central Node.	<code>KATA:server address:<имя сервера>:443</code>	Включить	Нет значения.
...установлен компонент Endpoint Sensors определенной версии.	Нет значения	Нет значения	В новом условии в разделе с названиями программ выберите компонент Endpoint Sensors и укажите номер версии.
...установлен компонент Endpoint Sensors в составе KES определенной версии.	<code>KATA:agent version:<номер версии></code>	Включить	Нет значения.
...установлена программа KES, но отсутствует Endpoint Sensors в составе KES.	<code>KATA:*</code>	Исключить	В разделе с названиями программ выберите Kaspersky Endpoint Security.
...компонент Endpoint Sensors в составе KES установлен, но не включен.	<code>KATA:agent version*</code>	Включить	Нет значения.
	<code>KATA:server address*</code>	Исключить	Нет значения.
...остановлен компонент Endpoint Sensors.	<code>KATA:server address*</code>	Включить	В разделе статусов компонентов добавьте в условие статус компонента Endpoint Sensors: Stopped.
...установлен компонент Endpoint Sensors, но отсутствует соединение с компонентом Central Node.	Нет значения	Нет значения	В разделе статусов компонентов добавьте в условие статус компонента Endpoint Sensors: Connection to server is failed.
			В разделе статусов компонентов добавьте в условие статус Kaspersky Endpoint Security 11: Connection to server is failed.

Список компьютеров, на которых...	Регулярное выражение	Необходимое действие	Дополнительные действия
...компонент Endpoint Sensors установлен, но не выполняет задачи.	Нет значения	Нет значения	В разделе статусов компонентов добавьте в условие статус компонента Endpoint Sensors: Tasks don't work.
			В разделе статусов компонентов добавьте в условие статус Kaspersky Endpoint Security 11: Tasks don't work.
...отключена самозащита компонента Endpoint Sensors.	Нет значения	Нет значения	В разделе описания статусов компонентов выберите значение статус компонента Endpoint Sensors: Self-defense is off.

Получение данных о состоянии компонента Endpoint Sensors на определенном компьютере

► Чтобы получить данные о состоянии компонента Endpoint Sensors на определенном компьютере, выполните следующие действия:

1. Откройте консоль KSC.
2. Выберите нужный Сервер администрирования.
3. В дереве консоли KSC в разделе с управляемыми устройствами выберите нужный вам компьютер.
В рабочей области отобразятся данные о текущем состоянии компонента Endpoint Sensors на этом компьютере.
4. Выберите закладку с событиями в свойствах компьютера.
Откроется журнал событий. События, связанные с работой компонента Endpoint Sensors, содержат строку "Endpoint Sensor" в графе задач.

Начало работы с программой

Этот раздел содержит информацию о том, как начать работу с программой в веб-интерфейсе, в меню администратора и в режиме Technical Support Mode.

В этом разделе

Начало работы в веб-интерфейсе программы	141
Начало работы в меню администратора программы	141
Начало работы с программой в режиме Technical Support Mode.....	142

Начало работы в веб-интерфейсе программы

Веб-интерфейс Kaspersky Anti Targeted Attack Platform расположен на сервере с компонентом Central Node.

Веб-интерфейс Kaspersky Anti Targeted Attack Platform защищен от *CSRF-атак* (см. стр. [332](#)) и работает только в том случае, если браузер пользователя веб-интерфейса программы 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.

► Чтобы начать работу в веб-интерфейсе, выполните следующие действия:

1. В браузере на любом компьютере, на котором разрешен доступ к серверу Central Node, введите IP-адрес сервера с компонентом Central Node.

Откроется окно ввода учетных данных пользователя Kaspersky Anti Targeted Attack Platform.

2. Введите имя пользователя и пароль доступа к веб-интерфейсу программы, которые вы задали на этапе установки и настройки компонента Central Node.

Откроется страница **Dashboard** веб-интерфейса программы.

Вы можете начать работу в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.

Начало работы в меню администратора программы

Вы можете работать с параметрами каждого из компонентов программы Sensor, Central Node и Sandbox в меню администратора в консоли управления каждого сервера, на котором установлен компонент программы.

- Чтобы начать работу в меню администратора компонента Sandbox, Sensor или Central Node в консоли управления сервером с компонентом Sandbox, Sensor или Central Node, выполните следующие действия:
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 программы.
Отобразится меню администратора компонента программы.
- Вы можете начать работу в меню администратора компонента программы.

Начало работы с программой в режиме Technical Support Mode

Вы можете работать с компонентами программы 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 программе и всем данным (в том числе персональным), которые в ней хранятся.

Режим Technical Support Mode позволяет управлять конфигурационными файлами программы. В частности, он позволяет отключить шифрование данных, передаваемых между серверами с компонентами программы, чтобы данные передавались 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 программы.

Не рекомендуется выполнять действия с Kaspersky Anti Targeted Attack Platform в режиме Technical Support Mode без консультации или указания сотрудников Службы технической поддержки.

- Чтобы начать работу с программой в режиме Technical Support Mode на сервере с компонентом Sandbox, Sensor или Central Node, выполните следующие действия:
1. Войдите в консоль управления того сервера, с которым вы хотите работать в режиме Technical Support Mode, по протоколу SSH или через терминал.
 2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке программы.

Отобразится меню администратора программы.

3. В меню администратора программы выберите режим **Technical Support Mode**.

4. Нажмите на клавишу **ENTER**.

Отобразится окно подтверждения входа в режим Technical Support Mode.

5. Если вы действительно хотите выполнять действия с программой в режиме Technical Support Mode, выберите **Yes** и нажмите на клавишу **ENTER**.

Отобразится окно работы с программой в режиме Technical Support Mode.

Вы можете начать работу с программой в режиме Technical Support Mode.

Настройка получения данных из KSN

В этом разделе содержится информация о том, как просмотреть Положение о KSN, а также настроить получение данных модулем KSN из службы KSN. Модуль KSN входит в состав компонентов Central Node и Sensor. Выполняйте действия по настройке получения данных из службы KSN на всех серверах с компонентами Central Node и Sensor.

Использование Kaspersky Security Network приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Kaspersky Private Security Network или отказаться от использования KSN. Для получения подробной информации см. *Руководство администратора Kaspersky Private Security Network*.

В этом разделе

Просмотр Положения о KSN.....	144
Настройка участия в KSN.....	145
Отказ от участия в KSN.....	145

Просмотр Положения о KSN

► Чтобы просмотреть Положение о KSN, выполните следующие действия в меню администратора любого сервера с компонентом Central Node или Sensor (см. стр. [141](#)):

1. В главном окне меню администратора выберите пункт **Legal information**.
 2. Нажмите на клавишу **ENTER**.
Откроется следующее окно меню администратора.
 3. Выберите пункт **Show KSN statement**.
 4. Нажмите на клавишу **ENTER**.
Откроется следующее окно меню администратора.
 5. Выберите язык для просмотра Положения о KSN в списке.
Например, если вы хотите просмотреть Положение о KSN на английском языке, выберите **English**.
 6. Нажмите на клавишу **ENTER**.
Откроется окно с текстом Положения о KSN.
 7. Просмотрите Положение о KSN.
 8. Нажмите на кнопку **Ok**.
- Вы вернетесь к главному окну меню администратора программы.

Настройка участия в KSN

Использование Kaspersky Security Network приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Kaspersky Private Security Network или отказаться от использования KSN. Для получения подробной информации см. *Руководство администратора Kaspersky Private Security Network*.

- Чтобы согласиться участвовать в KSN, выполните следующие действия в меню администратора каждого сервера с компонентами Sensor и Central Node (см. стр. [141](#)):
1. В главном окне меню администратора выберите пункт **Program settings**.
 2. Нажмите на клавишу **ENTER**.
Откроется следующее окно меню администратора.
 3. Выберите пункт **Configure KSN services**.
 4. Нажмите на клавишу **ENTER**.
Откроется следующее окно меню администратора.
 5. Выберите пункт **KSN**.
 6. Нажмите на клавишу **ENTER**.
Откроется следующее окно меню администратора.
 7. Нажмите на кнопку **Yes**.
Откроется следующее окно меню администратора.
 8. Выберите язык для просмотра Положения о KSN в появившемся списке.
Например, если вы хотите просмотреть Положение о KSN на английском языке, выберите **English**.
 9. Нажмите на клавишу **ENTER**.
Откроется окно меню администратора с текстом Положения о KSN.
 10. Просмотрите Положение о KSN.
 11. Нажмите на кнопку **I accept the terms**.
Вы будете участвовать в KSN.

Отказ от участия в KSN

- Чтобы отказаться от участия в KSN, если участие в KSN было настроено ранее, выполните следующие действия в меню администратора каждого сервера с компонентами Sensor и Central Node (см. стр. [141](#)):
1. В главном окне меню администратора выберите пункт **Program settings**.
 2. Нажмите на клавишу **ENTER**.
Откроется следующее окно меню администратора.
 3. Выберите пункт **Configure KSN services**.

4. Нажмите на клавишу **ENTER**.
Откроется следующее окно меню администратора.
5. Выберите пункт **KSN**.
6. Нажмите на клавишу **ENTER**.
Параметр KSN примет значение **No**.
Вы откажетесь от участия в KSN.

Настройка получения данных из KPSN

В этом разделе содержится информация о том, как настроить получение данных модулем KSN из KPSN (см. раздел "Компонент Sensor" на стр. [49](#)).

Вы можете настроить получение данных модулем KSN из KPSN (см. раздел "Компонент Sensor" на стр. [49](#)), если вы не хотите участвовать в KSN. Подробнее смотрите в документации к KPSN.

Модуль KSN входит в состав компонентов Central Node и Sensor. Выполняйте действия по настройке получения данных из KPSN на всех серверах с компонентами Central Node и Sensor.

В этом разделе

Подготовка серверов к использованию KPSN	147
Настройка использования KPSN	148

Подготовка серверов к использованию KPSN

► *Перед настройкой использования KPSN выполните следующие действия для каждого сервера с компонентами Sensor и Central Node (см. стр. [141](#)):*

1. Загрузите файлы `kc_private.xml`, `kh_private.xml` и `ksncli_private.dat` на жесткий диск компьютера, с которого вы можете подключиться к серверам с компонентами Sensor и Central Node, любым доступным способом.

О том, как получить эти файлы, смотрите в документации к KPSN.

2. Скопируйте файлы на сервер с компонентом Sensor.
3. Введите команды:

```
cd <директория, в которую вы загрузили файлы>
```

```
scp kc_private.xml kh_private.xml ksncli_private.dat admin@<IP-адрес сервера с компонентом Sensor>:
```

4. Введите пароль учетной записи `admin`, который вы задали при установке компонента Sensor.
5. Скопируйте файлы на сервер с компонентом Central Node.

6. Введите команды:

```
cd <директория, в которую вы загрузили файлы>
```

```
scp kc_private.xml kh_private.xml ksncli_private.dat admin@<IP-адрес сервера с компонентом Central Node>:
```

7. Введите пароль учетной записи `admin`, который вы задали при установке компонента Central Node.

Вы подготовите серверы к настройке использования KPSN.

Если вы хотите обновить файлы `kc_private.xml`, `kh_private.xml` и `ksncli_private.dat`, которые уже загружены на серверы с компонентами Sensor и Central Node, загрузите их повторно на каждый из этих серверов.

Настройка использования KPSN

► Чтобы настроить использование KPSN, выполните следующие действия в меню администратора каждого сервера с компонентами Sensor и Central Node (см. стр. [141](#)):

1. В главном окне меню администратора выберите пункт **Program settings**.

2. Нажмите на клавишу **ENTER**.

Откроется следующее окно меню администратора.

3. Выберите пункт **Configure KSN services**.

4. Нажмите на клавишу **ENTER**.

Откроется следующее окно меню администратора.

5. Выберите пункт **KPSN**.

6. Нажмите на клавишу **ENTER**.

Откроется следующее окно меню администратора.

Если вы подготовили серверы к использованию KPSN, вы увидите `found` напротив каждого из файлов KPSN.

7. Нажмите на кнопку **Continue**.

Откроется окно подтверждения использования KPSN вместо KSN.

8. Нажмите на кнопку **Enable**.

Вы вернетесь к окну начала настройки использования KSN и KPSN.

9. Нажмите на кнопку **Go Back**.

Вы вернетесь к главному окну меню администратора программы.

Модуль KSN будет получать данные из KPSN.

Управление учетными записями администраторов и пользователей программы

Этот раздел содержит информацию об управлении учетными записями администраторов и пользователей программы.

В этом разделе

Об учетных записях администраторов и пользователей программы	149
Создание учетной записи администратора для работы в меню администратора и в консоли серверов с компонентами программы	152
Создание учетной записи администратора веб-интерфейса при установке программы	153
Создание учетной записи администратора или пользователя веб-интерфейса программы.....	154
Включение и отключение учетной записи администратора или пользователя веб-интерфейса программы	155
Изменение пароля доступа к веб-интерфейсу программы учетной записи Administrator	155
Изменение пароля доступа к веб-интерфейсу программы учетной записи администратора или пользователя.....	156
Изменение пароля учетной записи администратора Sandbox	157

Об учетных записях администраторов и пользователей программы

В Kaspersky Anti Targeted Attack Platform предусмотрены учетные записи для серверов со следующими компонентами:

- **Sensor.** Учетная запись администратора для работы в меню администратора программы 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 программы, 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 программы и в консоли управления сервером (в режиме Technical Support Mode).
По умолчанию используется учетная запись admin.
 - Учетная запись администратора веб-интерфейса программы.
По умолчанию используется учетная запись Administrator.

- Учетные записи пользователей веб-интерфейса программы **Старший сотрудник службы безопасности и Сотрудник службы безопасности**.

Все учетные записи администратора создаются при установке программы. Данные каждой из этих учетных записей хранятся на том сервере с компонентом программы, к которому она относится.

Учетная запись администратора для работы в консоли управления сервером обладает неограниченными правами на управление сервером с компонентом программы, к которому она относится (правами суперпользователя). Под этой учетной записью вы можете выключить или перезагрузить сервер, а также изменить параметры программы 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 необходимо обеспечить безопасность серверов самостоятельно. Администратор несет ответственность за доступ к данным, хранящимся на серверах.

Учетная запись администратора веб-интерфейса программы **Administrator** создается при установке компонентов программы. В дальнейшем вы можете сами создавать учетные записи **Администратор** в веб-интерфейсе программы.

Учетная запись администратора программы предназначена для сотрудников вашей организации, в чьи обязанности входит управление Kaspersky Anti Targeted Attack Platform через веб-интерфейс программы. Под этой учетной записью вы можете создавать (см. стр. [154](#)), включать и отключать (см. стр. [155](#)) учетные записи пользователей программы, а также настраивать показатели активности Endpoint Sensors (см. стр. [284](#)).

Учетные записи пользователей веб-интерфейса программы **Старший сотрудник службы безопасности и Сотрудник службы безопасности** предназначены для сотрудников вашей организации, в чьи обязанности входит работа с событиями и задачами (см. стр. [233](#)) Kaspersky Anti Targeted Attack Platform в веб-интерфейсе программы.

Под учетной записью с ролью **Администратор** или **Старший сотрудник службы безопасности** вы можете добавлять, включать и отключать учетные записи пользователей программы, а также изменять пароли учетных записей администраторов и пользователей программы.

Таблица 3. Права доступа к веб-интерфейсу администраторов и пользователей программы

Раздел	Администратор	Старший сотрудник службы безопасности	Сотрудник службы безопасности
Мониторинг	Только графики из раздела Общая информация .	Неограниченный доступ	Все графики, кроме графиков событий группы VIP. Нет возможности перейти по ссылке на графике в раздел Обнаружения .

Раздел	Администратор	Старший сотрудник службы безопасности	Сотрудник службы безопасности
Обнаружения	Нет доступа.	Неограниченный доступ	Полный доступ ко всем обнаружениям, кроме обнаружений группы VIP; ограниченный доступ к обнаружениям группы VIP. Нет возможности экспортировать обнаружения.
Поиск угроз	Нет доступа.	Неограниченный доступ	Полный доступ ко всем событиям, в которых нет хостов из обнаружений группы VIP.
Задачи	Нет доступа.	Неограниченный доступ	Полный доступ ко всем задачам, в которых нет хостов из обнаружений группы VIP.
Политики	Нет доступа.	Неограниченный доступ	Доступ на чтение.
ИОС-проверка	Нет доступа.	Неограниченный доступ	Доступ на чтение.
Хранилище	Нет доступа.	Неограниченный доступ	Доступ только к файлам, задачи по которым созданы этим пользователем.
Endpoint Sensors	Доступ к просмотру таблиц компьютеров с компонентом Endpoint Sensors, ограничения по просмотру данных из задач и политик.	Неограниченный доступ	Доступ к просмотру таблиц компьютеров с компонентом Endpoint Sensors, ограничения по просмотру данных из задач и политик.
Отчеты	Нет доступа.	Неограниченный доступ	Нет доступа.
Параметры: Пользователи	Неограниченный доступ.	Неограниченный доступ	Нет доступа.
Параметры: YARA-правила	Нет доступа.	Неограниченный доступ	Доступ только на экспорт правил.
Параметры: Белый список	Нет доступа.	Неограниченный доступ	Доступ на чтение и экспорт.

Раздел	Администратор	Старший сотрудник службы безопасности	Сотрудник службы безопасности
Параметры: Группа VIP	Нет доступа.	Неограниченный доступ	Доступ на чтение.
Параметры: Интеграции	Неограниченный доступ.	Неограниченный доступ	Доступ ограничен.
Параметры: Endpoint Sensors	Неограниченный доступ.	Неограниченный доступ	Неограниченный доступ.
Параметры: Лицензия	Неограниченный доступ.	Неограниченный доступ	Доступ на чтение.
Параметры: Отправка уведомлений	Нет доступа.	Неограниченный доступ	Нет доступа.

Создание учетной записи администратора для работы в меню администратора и в консоли серверов с компонентами программы

Вы можете создать учетную запись администратора для работы в меню администратора и в консоли серверов с компонентами программы во время установки этих компонентов.

► Чтобы создать учетную запись, выполните следующие действия в окне создания учетной записи администратора в меню администратора программы (см. стр. [141](#)) того сервера, для которого вы хотите создать учетную запись:

1. В поле **Username** введите имя пользователя учетной записи администратора.
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.

Нажмите на кнопку **Ok**.

См. также


Управление учетными записями администраторов и пользователей программы	149
Об учетных записях администраторов и пользователей программы	149
Создание учетной записи администратора веб-интерфейса при установке программы	153
Создание учетной записи администратора или пользователя веб-интерфейса программы.....	154
Включение и отключение учетной записи администратора или пользователя веб-интерфейса программы	155
Изменение пароля доступа к веб-интерфейсу программы учетной записи Administrator	155
Изменение пароля доступа к веб-интерфейсу программы учетной записи администратора или пользователя.....	156
Изменение пароля учетной записи администратора Sandbox	157
Шаг 3. Создание учетной записи администратора Sandbox	60
Шаг 1. Создание учетной записи для работы в меню администратора и в консоли управления сервером.....	81

Создание учетной записи администратора веб-интерфейса при установке программы

- Чтобы создать учетную запись администратора веб-интерфейса программы, выполните следующие действия в окне создания учетной записи администратора веб-интерфейса в меню администратора программы (см. стр. [141](#)) сервера с компонентом Central Node:
1. В поле **Username** введите имя пользователя учетной записи администратора веб-интерфейса программы.
По умолчанию используется имя пользователя Administrator.
 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**.

Создание учетной записи администратора или пользователя веб-интерфейса программы

► Чтобы создать учетную запись администратора или пользователя веб-интерфейса программы, выполните следующие действия:

1. Войдите в веб-интерфейс программы под учетной записью администратора или старшего сотрудника службы безопасности.
2. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Пользователи**.
3. Нажмите на кнопку **Добавить**.
Откроется окно **Добавить**.
4. В раскрывающемся списке **Роль** выберите роль пользователя, учетную запись которого вы хотите создать. Вы можете выбрать одну из следующих ролей:
 - **Администратор**.
 - **Старший сотрудник службы безопасности**.
 - **Сотрудник службы безопасности**.
5. 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 и дефис (-);
 - должно начинаться с буквы (A-Z или a-z).
6. 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.
7. В поле **Подтвердите пароль** повторно введите пароль доступа пользователя к веб-интерфейсу.
8. Если вы хотите включить учетную запись пользователя, установите флажок **Включить учетную запись**.


Если учетная запись пользователя веб-интерфейса программы включена, доступ пользователя к веб-интерфейсу программы разрешен. Если учетная запись отключена, доступ пользователя к веб-интерфейсу программы запрещен. Правами на включение и отключение учетных записей пользователей обладают только учетные записи администратора и старшего сотрудника службы безопасности.

9. Нажмите на кнопку **Создать**.

Учетная запись администратора или пользователя веб-интерфейса программы будет создана.

Включение и отключение учетной записи администратора или пользователя веб-интерфейса программы

- Чтобы включить или отключить учетную запись администратора или пользователя веб-интерфейса программы, выполните следующие действия:

1. Войдите в веб-интерфейс программы под учетной записью администратора или старшего сотрудника службы безопасности.
2. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Пользователи**.
3. В списке учетных записей выберите учетную запись администратора или пользователя, которую вы хотите включить или отключить.
4. Выполните одно из следующих действий:
 - 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 подтверждение действия.

5. Нажмите на кнопку **Да**.

Состояние учетной записи администратора или пользователя веб-интерфейса программы будет изменено.

Изменение пароля доступа к веб-интерфейсу программы учетной записи Administrator

- Чтобы изменить пароль доступа к веб-интерфейсу программы учетной записи Administrator, выполните следующие действия:

1. Войдите в веб-интерфейс программы под учетной записью Administrator.
2. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в списке действий выберите **Изменить пароль**

Откроется окно **Изменить пароль**.

3. В поле **Старый пароль** введите текущий пароль доступа к веб-интерфейсу программы.
4. В поле **Новый пароль** введите новый пароль доступа к веб-интерфейсу программы.

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.

5. В поле **Подтвердите пароль** повторно введите новый пароль.
6. Нажмите на кнопку **Изменить пароль**.

Пароль доступа к веб-интерфейсу программы учетной записи Administrator будет изменен.

Изменение пароля доступа к веб-интерфейсу программы учетной записи администратора или пользователя

► *Чтобы изменить пароль доступа к веб-интерфейсу программы учетной записи администратора или пользователя, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью администратора или старшего сотрудника службы безопасности.
2. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Пользователи**.
3. В списке учетных записей выберите учетную запись администратора или пользователя, пароль которой вы хотите изменить.
4. По ссылке **Изменить пароль** откройте окно изменения пароля.
5. В поле **Новый пароль** введите новый пароль доступа к веб-интерфейсу программы.

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 **Применить**.
- Пароль доступа к веб-интерфейсу программы учетной записи администратора или пользователя веб-интерфейса будет изменен.

Изменение пароля учетной записи администратора Sandbox

► *Чтобы изменить пароль учетной записи администратора Sandbox, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Administration**.
2. В группе параметров **Change password** отобразится имя учетной записи администратора Sandbox, которое вы задали при установке Sandbox (см. раздел "Шаг 3. Создание учетной записи администратора Sandbox" на стр. [60](#)) и поля для изменения пароля.
3. В поле **Current password** введите текущий пароль учетной записи администратора Sandbox.
4. В поле **New password** введите новый пароль учетной записи администратора Sandbox.
5. В поле **Confirm password** введите новый пароль учетной записи администратора Sandbox повторно.
6. Нажмите на кнопку **Change password**.

Пароль учетной записи администратора Sandbox будет изменен.

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 программы (см. стр. [175](#));
- записи о работоспособности компонентов в журнале Kaspersky Anti Targeted Attack Platform (см. стр. [158](#)).

В этом разделе

О журналах Kaspersky Anti Targeted Attack Platform	158
Просмотр журнала работоспособности сервера с компонентом Central Node	158
Просмотр журнала работоспособности сервера с компонентом Sandbox	159
Просмотр журнала аудита безопасности сервера с компонентом Central Node	160
Просмотр журнала аудита безопасности сервера с компонентом Sandbox	160

О журналах Kaspersky Anti Targeted Attack Platform

Во время работы Kaspersky Anti Targeted Attack Platform возникают различного рода события. Они отражают изменения состояния программы. Для того, чтобы администратор программы мог самостоятельно проанализировать ход работы программы 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 программы в журналах.

В журналах содержится, например, следующая информация:

- о запуске программы;
- о входе в систему каждого пользователя;
- о состоянии работы серверов с компонентами программы;
- 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 окно **Kaspersky Anti Targeted Attack Platform**.
2. В списке параметров программы выберите **System Administration**.
3. Нажмите на клавишу **ENTER**.
Откроется окно **Select action**.
4. В списке действий выберите **View system logs**.
5. Нажмите на клавишу **ENTER**.
Откроется окно со списком дальнейших действий.
6. В списке действий выберите **View subdirectory kaspersky**.
7. Нажмите на клавишу **ENTER**.
Откроется окно со списком директорий.
8. В списке директорий выберите **View subdirectory 'apt-monitor'**.
9. Нажмите на клавишу **ENTER**.
Откроется окно со списком журналов директории **apt-monitor**.
10. В списке журналов выберите **View file 'apt-monitor.log'**.
11. Нажмите на клавишу **ENTER**.

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

► Чтобы просмотреть журнал аудита безопасности сервера с компонентом Central Node, выполните следующие действия:

1. Подключитесь к серверу с компонентом Central Node по протоколу SSH под учетной записью администратора.

Откроется окно **Kaspersky Anti Targeted Attack Platform**.

2. В списке параметров программы выберите **System Administration**.

3. Нажмите на клавишу **ENTER**.

Откроется окно **Select action**.

4. В списке действий выберите **View system logs**.

5. Нажмите на клавишу **ENTER**.

Откроется окно со списком дальнейших действий.

6. В списке действий выберите **View subdirectory kaspersky**.

7. Нажмите на клавишу **ENTER**.

Откроется окно со списком директорий.

8. В списке директорий выберите **View subdirectory 'apt-monitor'**.

9. Нажмите на клавишу **ENTER**.

Откроется окно со списком журналов директории **apt-monitor**.

10. В списке журналов выберите **View file 'apt-monitor.log'**.

11. Нажмите на клавишу **ENTER**.

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, 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 less /var/log/kaspersky/sandbox/checker/checker.log
```

Вы сможете просмотреть журнал аудита безопасности сервера с компонентом Sandbox.

Проверка целостности файлов Kaspersky Anti Targeted Attack Platform

Вы можете проверить целостность файлов Kaspersky Anti Targeted Attack Platform с помощью скрипта `verify_files`. Скрипт `verify_files`, эталонные файлы с контрольной суммой файлов компонентов Sensor и Central Node, а также с контрольной суммой файлов компонента Sandbox входят в инсталляционный комплект программы.

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 компонентов Sensor и Central Node.

Проверка целостности файлов компонента Sandbox выполняется на сервере с компонентом Sandbox с использованием эталонного файла с контрольной суммой файлов компонента Sandbox.

► *Чтобы проверить целостность файлов компонентов Sensor и Central Node, выполните следующие действия:*

1. Войдите в режим Technical Support Mode сервера с компонентом Sensor или Central Node.
2. Создайте файл с контрольной суммой файлов. Выполните команду:

```
sudo /opt/kaspersky/apt-cert/libexec/verify_files
```

3. Получите контрольную сумму файлов в директории `/tmp/MD5SUM`.
4. Сравните контрольную сумму файлов в эталонном файле и в созданном файле MD5SUM. Выполните команду:

```
sudo /opt/kaspersky/apt-cert/libexec/verify_files /var/opt/kaspersky/  
apt/MD5SUM /tmp/MD5SUM
```

► *Чтобы проверить целостность файлов компонента Sandbox, выполните следующие действия:*

1. Войдите в режим Technical Support Mode сервера с компонентом Sandbox.
2. Создайте файл с контрольной суммой файлов. Выполните команду:

```
sudo /opt/kaspersky/apt-cert/libexec/verify_files
```

3. Получите контрольную сумму файлов в директории /tmp/MD5SUM.
4. Сравните контрольную сумму файлов в эталонном файле и в созданном файле MD5SUM. Выполните команду:

```
sudo /opt/kaspersky/apt-cert/libexec/verify_files /var/opt/kaspersky/  
apt/MD5SUM /tmp/MD5SUM
```

Проверка целостности значений параметров Kaspersky Anti Targeted Attack Platform

Вы можете проверить целостность значений параметров Kaspersky Anti Targeted Attack Platform с помощью скрипта `verify_settings`. Скрипт `verify_settings` входит в инсталляционный комплект программы.

Вы можете проверить целостность значений параметров Kaspersky Anti Targeted Attack Platform на каждом из серверов с компонентами программы Sensor, Central Node и Sandbox. Для проверки целостности значений параметров компонентов программы используется эталонный файл со значениями параметров компонентов программы. Вам необходимо создать эталонный файл со значениями параметров компонентов программы после того, как вы зададите значения всех параметров программы.

► *Чтобы создать эталонный файл со значениями параметров компонентов программы, выполните следующие действия:*

1. Войдите в режим Technical Support Mode сервера с тем компонентом Kaspersky Anti Targeted Attack Platform, целостность значений параметров которого вы хотите проверить.
2. Создайте файл со значениями параметров компонента программы. Выполните команду:

```
# /opt/kaspersky/apt-cert/libexec/verify_settings
```

Эталонный файл со значениями параметров компонента программы будет создан в директории `tmp/SETTINGS`.

3. Переименуйте созданный эталонный файл. Например, вы можете назвать файл `SETTINGS.<дата создания файла в формате DDMMYY>`. Выполните команду:

```
# cp /tmp/SETTINGS /tmp/SETTINGS.<дата создания файла в формате DDMMYY>
```

► *Чтобы проверить целостность значений параметров компонентов программы, выполните следующие действия:*

1. Войдите в режим Technical Support Mode сервера с тем компонентом Kaspersky Anti Targeted Attack Platform, целостность значений параметров которого вы хотите проверить.
2. Сравните эталонный файл с текущими значениями параметров компонента программы. Выполните команду:

```
# /opt/kaspersky/apt-cert/libexec/verify_settings /tmp/SETTINGS.<дата создания файла в формате DDMMYY>
```

Например, если вы переименовывали файл `SETTINGS` в `SETTINGS.010119`, выполните команду:

```
# /opt/kaspersky/apt-cert/libexec/verify_settings /tmp/SETTINGS.010119
```

Ограничение размера проверяемых файлов

Вы можете установить ограничение на размер файлов, отправляемых на проверку на сервер с компонентом Central Node.

- *Чтобы установить ограничение на размер проверяемых файлов, выполните следующие действия:*
1. Подключитесь к серверу с компонентом Central Node по протоколу SSH под учетной записью администратора.
Откроется окно **Kaspersky Anti Targeted Attack Platform**.
 2. В списке параметров программы выберите **Program settings**.
 3. Нажмите на клавишу **ENTER**.
Откроется окно **Select action**.
 4. В списке действий выберите **Configure object processing**.
Откроется окно **Configure file size limit**.
 5. Выберите параметр **File size limit**.
 6. Нажатием клавиш ← и → выберите одно из предложенных значений максимального размера файлов.
 7. Выберите **Go back**.
 8. Нажмите на клавишу **ENTER**.
Служба перезагрузится.

Ограничение размера проверяемых файлов будет установлено.

Мониторинг работы программы

Вы можете осуществлять мониторинг работы программы с помощью графиков в разделе **Мониторинг** окна веб-интерфейса программы. Вы можете настроить схему расположения графиков в рабочей области окна веб-интерфейса программы, добавлять, удалять, перемещать графики, настраивать масштаб графиков и выбирать период отображения данных.

В этом разделе

О графиках и схемах расположения графиков	165
Создание новой схемы расположения графиков	166
Добавление графика на текущую схему расположения графиков	167
Перемещение графика на текущей схеме расположения графиков	167
Перемещение графика и создание новой схемы расположения графиков	168
Удаление графика с текущей схемы расположения графиков	168
Удаление графика и создание новой схемы расположения графиков	169
Выбор схемы расположения графиков из списка	169
Назначение схемы расположения графиков для использования по умолчанию	169
Переименование схемы расположения графиков	170
Удаление схемы расположения графиков	170
Сохранение схемы расположения графиков в PDF	170
Настройка периода отображения данных на графиках	171
Настройка размера отображения графиков на текущей схеме расположения графиков	172
Настройка размера отображения графиков и создание новой схемы расположения графиков	172
Основные принципы работы с графиками типа "Топ 10"	173
Основные принципы работы с графиками типа "Обнаружения"	173
Работа с графиками типа "Общая информация"	175

О графиках и схемах расположения графиков

С помощью графиков вы можете осуществлять мониторинг работы программы. Например, работоспособности модулей и компонентов программы, обработки данных, событий, обновления баз модулей и компонентов программы.

Схема расположения графиков – вид рабочей области окна веб-интерфейса программы в разделе **Мониторинг**. Вы можете добавлять, удалять и перемещать графики на схеме расположения графиков, а также настраивать масштаб графиков.


В окне веб-интерфейса программы в разделе **Мониторинг** отображаются следующие графики:

- **Обнаружения:**
 - **Вектор атаки.** Отображение обнаруженных объектов по направлению атаки.

- **Важность.** 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».
- **Состояние.** Отображение состояния обнаружения в зависимости от того, какой пользователь Kaspersky Anti Targeted Attack Platform его обрабатывает и от того, обработано это обнаружение или нет.
- **Технологии.** Отображение названий модулей или компонентов программы, сделавших обнаружение.
- **VIP по степени важности.** Отображение важности обнаружений группы VIP в соответствии с тем, какое влияние они могут оказать на безопасность компьютера или локальной сети организации, по опыту «Лаборатории Касперского».
- **Общая информация:**
 - **Работоспособность системы.** Отображение работоспособности компонентов программы и сведений об обработке данных.
 - **Статус компонентов.** Отображение работоспособности компонентов программы и состояния обновления баз.
 - **Очереди.** Отображение сведений о количестве и объеме объектов, ожидающих проверки модулями и компонентами программы.
 - **Время обработки в Sandbox.** Отображение среднего времени, за которое были получены результаты проверки объектов компонентом Sandbox.
 - **Обработка данных.** Отображение состояния обработки трафика компонентом Sensor.
- **Топ 10:**
 - **Домены.** 10 доменов, наиболее часто встречающихся в обнаружениях.
 - **Адреса получателей.** 10 получателей сообщений электронной почты, наиболее часто встречающихся в обнаружениях.
 - **IP.** 10 IP-адресов, наиболее часто встречающихся в обнаружениях.
 - **Адреса отправителей.** 10 отправителей сообщений электронной почты, наиболее часто встречающихся в обнаружениях.

Создание новой схемы расположения графиков

► Чтобы создать новую схему расположения графиков, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку .
3. В раскрывающемся списке выберите **Создать схему**.
4. В поле **Название схемы** введите имя новой схемы расположения графиков.
5. Если вы хотите добавить графики на новую схему расположения графиков, нажмите на кнопку **Графики** и выполните следующие действия:
 - a. В появившемся окне **Управление графиками** включите переключатели рядом с графиками, которые вы хотите добавить.

- b. Нажмите на кнопку .

Выбранные графики будут добавлены в рабочую область окна веб-интерфейса программы.


6. Нажмите на кнопку **Сохранить**.

Новая схема расположения графиков будет добавлена в список схем расположения графиков в разделе **Мониторинг**.

Добавление графика на текущую схему расположения графиков

- *Чтобы добавить график на текущую схему расположения графиков, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.

2. В верхней части окна нажмите на кнопку .

3. В раскрывающемся списке выберите **Изменить**.

4. Нажмите на кнопку **Графики**.

5. В появившемся окне **Управление графиками** включите переключатель рядом с графиком, который вы хотите добавить.

6. Нажмите на кнопку .

Выбранный график будет добавлен в рабочую область окна веб-интерфейса программы.


7. Нажмите на кнопку **Сохранить**.

График будет добавлен на текущую схему расположения графиков.

Перемещение графика на текущей схеме расположения графиков

- *Чтобы переместить график на текущей схеме расположения графиков, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.

2. В верхней части окна нажмите на кнопку .

3. В раскрывающемся списке выберите **Изменить**.

4. Выберите график, который вы хотите переместить на схеме расположения графиков.

5. Нажав и удерживая левую клавишу мыши на верхней части графика, перетащите график на другое место схемы расположения графиков.

6. Нажмите на кнопку **Сохранить**.

Текущая схема расположения графиков сохранится.

Перемещение графика и создание новой схемы расположения графиков

► Чтобы переместить график и создать новую схему расположения графиков, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.

2. В верхней части окна нажмите на кнопку .

3. В раскрывающемся списке выберите **Изменить**.

4. Выберите график, который вы хотите переместить на схеме расположения графиков.

5. Нажав и удерживая левую клавишу мыши на верхней части графика, перетащите график на другое место схемы расположения графиков.

6. В поле **Название схемы** введите имя новой схемы расположения графиков.

7. Нажмите на кнопку **Сохранить**.

Новая схема расположения графиков будет добавлена в список схем расположения графиков в разделе **Мониторинг**.

Удаление графика с текущей схемы расположения графиков

► Чтобы удалить график с текущей схемы расположения графиков, выполните следующие действия:

1. В окне веб-интерфейса программы 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 графика, который вы хотите удалить со схемы расположения графиков.

График будет удален из рабочей области окна веб-интерфейса программы.

5. Нажмите на кнопку **Сохранить**.

График будет удален с текущей схемы расположения графиков.

Удаление графика и создание новой схемы расположения графиков

► Чтобы удалить график и создать новую схему расположения графиков, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.

2. В верхней части окна нажмите на кнопку .

3. В раскрывающемся списке выберите **Изменить**.

4. Нажмите на значок **X** в правом верхнем углу графика, который вы хотите удалить со схемы расположения графиков.

График будет удален из рабочей области окна веб-интерфейса программы.

5. В поле **Название схемы** введите имя новой схемы расположения графиков.

6. Нажмите на кнопку **Сохранить**.

Новая схема расположения графиков будет добавлена в список схем расположения графиков в разделе **Мониторинг**.

Выбор схемы расположения графиков из списка

► Чтобы выбрать схему расположения графиков из списка схем расположения графиков, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.

2. В правом верхнем углу окна веб-интерфейса программы раскройте список схем расположения графиков.

3. Выберите нужную схему расположения графиков.

4. Нажмите на левую клавишу мыши.

Выбранная схема расположения графиков отобразится в рабочей области окна веб-интерфейса программы.

Назначение схемы расположения графиков для использования по умолчанию

► Чтобы назначить схему расположения графиков для использования по умолчанию, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.

2. В правом верхнем углу окна веб-интерфейса программы раскройте список схем расположения графиков.

3. Выберите схему расположения графиков, которую вы хотите назначить для использования по

умолчанию.


4. Нажмите на значок ☆ слева от названия схемы расположения графиков.

Выбранная схема расположения графиков будет отмечена значком ★ и будет использоваться по умолчанию.

Переименование схемы расположения графиков

- Чтобы переименовать схему расположения графиков, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса программы в списке схем расположения графиков выберите схему расположения графиков, которую вы хотите переименовать.

3. В верхней части окна нажмите на кнопку .

4. В раскрывающемся списке выберите **Изменить**.
5. В поле **Название схемы** введите новое имя схемы расположения графиков.
6. Нажмите на кнопку **Сохранить**.

Схема расположения графиков будет переименована.

Удаление схемы расположения графиков

- Чтобы удалить схему расположения графиков, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса программы в списке схем расположения графиков выберите схему расположения графиков, которую вы хотите удалить.
3. Наведите курсор мыши на название схемы расположения графиков, которую вы хотите удалить.
4. Нажмите на значок ✕ справа от названия схемы расположения графиков.
Отобразится подтверждение удаления схемы расположения графиков.
5. Нажмите на кнопку **Удалить**.


Схема расположения графиков будет удалена.

Сохранение схемы расположения графиков в PDF

- Чтобы сохранить схему расположения графиков в PDF, выполните следующие действия:

1. В окне веб-интерфейса программы 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 **Сохранение в PDF** в раскрывающемся списке **Ориентация** выберите ориентацию страницы.
5. Нажмите на кнопку **Скачать**.
Схема расположения графиков в формате PDF 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 Kaspersky Anti Targeted Attack Platform.
6. Нажмите на кнопку **Заккрыть** в нижней части окна **Сохранение в PDF**.
Окно **Сохранение в PDF** закрывается.

Настройка периода отображения данных на графиках

Вы можете настроить отображение данных на графиках за следующие периоды:

- **День.**
- **Неделя.**
- **Месяц.**

► *Чтобы настроить отображение данных на графиках за сутки (с 00:00 до 23:59), выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса программы в раскрывающемся списке периодов отображения данных выберите **День**.
3. В календаре справа от названия периода **День** выберите дату, за которую вы хотите, чтобы на графиках отображались данные.

На всех графиках страницы **Мониторинг** отобразятся данные за выбранный вами период.

► *Чтобы настроить отображение данных на графиках за неделю (с понедельника по воскресенье), выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса программы в раскрывающемся списке периодов отображения данных выберите **Неделя**.
3. В календаре справа от названия периода **Неделя** выберите неделю, за которую вы хотите, чтобы на графиках отображались данные.


На всех графиках страницы **Мониторинг** отобразятся данные за выбранный вами период.

- ▶ Чтобы настроить отображение данных на графиках за месяц (календарный месяц), выполните следующие действия:



1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса программы в раскрывающемся списке периодов отображения данных выберите **Месяц**.
3. В календаре справа от названия периода **Месяц** выберите месяц, за который вы хотите, чтобы на графиках отображались данные.

На всех графиках страницы **Мониторинг** отобразятся данные за выбранный вами период.

Настройка размера отображения графиков на текущей схеме расположения графиков

Вы можете настроить размер отображения некоторых графиков. В правом верхнем углу графиков, размер отображения которых можно настроить, есть значок .

- ▶ Чтобы настроить размер отображения графиков на текущей схеме расположения графиков, выполните следующие действия:


1. В окне веб-интерфейса программы 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 графика.
5. В раскрывшемся списке выберите один из следующих размеров отображения графика:
 - 1x1.
 - 2x1.
 - 3x1.

Размер отображения выбранного графика изменится.

6. Повторите действия для всех графиков, размер отображения которых вы хотите изменить.
7. Нажмите на кнопку **Сохранить**.



Текущая схема расположения графиков нужного размера сохранится.

Настройка размера отображения графиков и создание новой схемы расположения графиков

Вы можете настроить размер отображения некоторых графиков. В правом верхнем углу графиков, размер отображения которых можно настроить, есть значок .

- ▶ Чтобы настроить размер отображения графиков и создать новую схему расположения

графиков, выполните следующие действия:

1. В окне веб-интерфейса программы 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 графика.
5. В раскрывшемся списке выберите один из следующих размеров отображения графика:
 - 1x1.
 - 2x1.
 - 3x1.
 Размер отображения выбранного графика изменится.
6. Повторите действия для всех графиков, размер отображения которых вы хотите изменить.
7. В поле **Название схемы** введите имя новой схемы расположения графиков.
8. Нажмите на кнопку **Сохранить**.

Новая схема расположения графиков нужного размера будет добавлена в список схем расположения графиков в разделе **Мониторинг**.

Основные принципы работы с графиками типа "Топ 10"

В разделе **Мониторинг** окна веб-интерфейса программы отображаются следующие графики типа **Топ 10**:

- **Топ 10 доменов.** 10 доменов, наиболее часто встречающихся в обнаружениях.
- **Топ 10 адресов получателей.** 10 получателей сообщений электронной почты, наиболее часто встречающихся в обнаружениях.
- **Топ 10 IP-адресов.** 10 IP-адресов, наиболее часто встречающихся в обнаружениях.
- **Топ 10 адресов отправителей.** 10 отправителей сообщений электронной почты, наиболее часто встречающихся в обнаружениях.

В левой части каждого графика перечислены домены, адреса получателей, IP-адреса и адреса отправителей сообщений. В правой части каждого графика отображается количество раз, которое Kaspersky Anti Targeted Attack Platform обнаружила их за выбранный период отображения данных на графиках.

По ссылке с именем каждого домена, адреса получателя, IP-адреса и адреса отправителя сообщений можно перейти на закладку **Обнаружения** веб-интерфейса программы и просмотреть обнаружения, связанные с этим доменом, адресом получателя, IP-адресом и адресом отправителя сообщений. При этом обнаружения будут отфильтрованы по данному домену, адресу получателя, IP-адресу или адресу отправителя сообщений.

Основные принципы работы с графиками типа "Обнаружения"

В разделе **Мониторинг** окна веб-интерфейса программы отображаются следующие графики типа

Обнаружения:

- **Обнаружения по вектору атаки.** Отображение обнаруженных объектов по направлению атаки.
- **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».
- **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 программы, сделавших обнаружение.
- **Обнаружения группы VIP по степени важности.** Отображение важности обнаружений группы VIP в соответствии с тем, какое влияние они могут оказать на безопасность компьютера или локальной сети организации, по опыту «Лаборатории Касперского».

Для всех графиков типа **Обнаружения** можно настроить размер отображения.

В левой части каждого графика отображается легенда графика по цветам, которыми данные отображены на самих графиках.

Пример:

На графике **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 графике **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 графиках.

По ссылке с типом каждого обнаружения можно перейти в раздел **Обнаружения** веб-интерфейса программы и просмотреть все обнаружения этого типа. При этом обнаружения будут отфильтрованы по данному типу.

Пример:

На графике **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 графиках.

По ссылке **Файлы из почты** откроется закладка **Обнаружения** и отобразятся все обнаружения, связанные с обнаружением файлов в почтовом трафике за выбранный период отображения данных на графиках. Данные будут отфильтрованы по следующим параметрам: **Время**, **Тип объекта=FILE** и **Источник данных=MAIL**.

В правой части каждого графика отображаются секторы данных на кольцевых диаграммах и столбцы данных на линейных диаграммах. На вертикальной оси отображается количество событий, на горизонтальной оси отображаются дата и время обнаружения. Вы можете изменить период отображения данных на графиках.

При наведении курсора мыши на каждый сектор данных отображается количество обнаружений, подсчитанных по данному сектору.

При наведении курсора мыши на каждый столбец данных отображается количество обнаружений, подсчитанных за период, представленный этим столбцом.

Работа с графиками типа "Общая информация"

В разделе **Мониторинг** окна веб-интерфейса программы отображаются следующие графики типа **Общая информация**:

- **Работоспособность системы.** Отображение работоспособности компонентов программы и сведений об обработке данных.
- **Статус компонентов.** Отображение работоспособности компонентов программы и состояния обновления баз.
- **Очереди.** Отображение сведений о количестве и объеме объектов, ожидающих проверки модулями и компонентами программы.
- **Время обработки в Sandbox.** Отображение среднего времени, за которое были получены результаты проверки объектов компонентом Sandbox.
- **Обработка данных.** Отображение состояния обработки трафика компонентом Sensor.

Вы можете изменить период отображения данных на графиках (см. раздел "Настройка периода отображения данных на графиках" на стр. [171](#)).

Мониторинг работоспособности модулей и компонентов программы

На графике **Статус компонентов** вы можете оценить статус работы следующих модулей и компонентов программы:

- **RS Engine.**
- **YARA.**
- **Sandbox.**
- **IDS** – на всех серверах, на которых работает компонент.
- **Anti-Malware Engine.**
- **Targeted Attack Analyzer.**
- **IOC**
 - **IOC в базе Событий.**
 - **IOC на Endpoint Sensors.**
- **Обновление баз** – на всех серверах, на которых работает программа.

- **URL Reputation (KSN)** – на всех серверах, на которых работает модуль.
- **Карантин.**

На графике **Статус компонентов** отображается следующая информация:

- Если модули и компоненты работают без сбоев, рядом с названием модуля или компонента отображается значок ✓.
- Если обнаружены проблемы с работой модулей и компонентов программы, рядом с названием модуля или компонента отображается значок ○.

Вы также можете оценить состояние обновления баз модулей и компонентов программы **Обновление баз**. Отображается следующая информация:

- Если базы модулей и компонентов программы в актуальном состоянии, рядом с именем сервера, на котором установлены модули и компоненты программы, отображается значок ✓.
- Если базы одного или нескольких компонентов программы не обновлялись в течение 24 часов, рядом с именем сервера, на котором установлены модули и компоненты программы, отображается значок ○.

На графике **Работоспособность системы** вы можете оценить работоспособность компонентов программы и статус обработки данных.

В разделе **Статус компонентов** графика отображается следующая информация:

- Количество модулей и компонентов, работающих без сбоев (для модулей IDS и KSN – если модули исправно работают на всех серверах, на которых они установлены) отображается со статусом **Без ошибок** и значком ■.
- Количество модулей и компонентов, у которых работоспособность нарушена (для модулей IDS и KSN – если работоспособность нарушена хотя бы на одном сервере из тех, на которых они установлены) отображается со статусом **С ошибкой** и значком ■.
- Количество модулей и компонентов, которые не установлены или отключены (например, в Kaspersky Anti Targeted Attack Platform не загружены YARA-правила) отображается со статусом **С ошибкой** и значком ■.

По ссылке с названием каждого статуса можно перейти на график **Статус компонентов**.

В разделе **Обработка данных** графика отображается следующая информация:

- Если данные с серверов с компонентом Sensor и с сервера или виртуальной машины с программой Kaspersky Secure Mail Gateway поступают без сбоев, справа от названия компонента **Sensors** отображается значок ✓.
- Если ожидание объектов в очереди на проверку модулями и компонентами программы не превышает максимально допустимое время, справа от названия **Очереди** отображается значок ✓.
- Если обнаружены проблемы с поступлением данных с серверов с компонентом Sensor или с сервера или виртуальной машины с программой Kaspersky Secure Mail Gateway, справа от названия компонента **Sensors** отображается значок ✗.
- Если обнаружено превышение максимально допустимого времени ожидания объектов в очереди на проверку модулями и компонентами программы, справа от названия **Очереди** отображается значок ✗.

Нажатие левой клавиши мыши на название **Sensors** или **Очереди** позволяет раскрыть окно со списком всех серверов с компонентом Sensor и всех очередей на проверку объектов модулями и компонентами

программы.

По ссылке с именем каждого сервера с компонентом Sensor открываются графики **Обработка данных**.

По ссылке с именем каждой очереди на проверку объектов модулями и компонентами программы открываются графики **Очереди**.

На круговой диаграмме графика отображается следующая информация:

- Во внешней области круга отображается работоспособность компонентов программы.
 - Если все модули и компоненты работают без сбоев, внешняя область круга окрашена в зеленый цвет.
 - При наличии проблем в работе модулей и компонентов программы, внешняя область круга окрашена в красный цвет.

Нажатие левой клавиши мыши на внешнюю область круга позволяет перейти на график **Статус компонентов**.

- Во внутренней области круга отображается статус обработки данных.
 - Если данные с серверов с компонентом Sensor и с сервера или виртуальной машины с программой Kaspersky Secure Mail Gateway поступают без сбоев и ожидание объектов в очереди на проверку модулями и компонентами программы не превышает максимально допустимое время, внутренняя часть круга окрашена в зеленый цвет.
 - Если обнаружены проблемы с поступлением данных с серверов с компонентом Sensor или с сервера или виртуальной машины с программой Kaspersky Secure Mail Gateway или превышение максимально допустимого времени ожидания объектов в очереди на проверку модулями и компонентами программы, внутренняя часть круга окрашена в красный цвет и помечена знаком



Нажатие левой клавиши мыши на внутреннюю область круга позволяет раскрыть окно со списком всех серверов с компонентом Sensor и всех очередей на проверку объектов модулями и компонентами программы.

По ссылке с именем каждого сервера с компонентом Sensor открываются графики **Обработка данных**. По ссылке с именем каждой очереди на проверку объектов модулями и компонентами программы открываются графики **Очереди**.

В случае обнаружения проблем в работоспособности модулей и компонентов программы, которые вы не можете решить самостоятельно, рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Способы получения технической поддержки" на стр. [330](#)).

Мониторинг приема и обработки входящих данных

На графике **Обработка данных** вы можете оценить статус обработки данных, поступающих от компонента Sensor (см. раздел "Компонент Sensor" на стр. [49](#)) на сервер с компонентом Central Node (см. раздел "Компонент Central Node" на стр. [50](#)), и отследить ошибки обработки данных.

Вы можете выбрать Sensor, поступление данных с которого вы хотите оценить, в раскрывающемся списке

справа от названия графика **Обработка данных**.

Вы можете выбрать тип отображения данных в раскрывающемся списке справа от списка Sensor:

- **Текущая загрузка** – 5 минут до текущего момента.
- **Пользовательский диапазон**. В этом случае вы также можете настроить период отображения данных на графиках.

В левой части каждого графика отображается легенда графика по цветам, которыми данные отображены на самих графиках.

Если выбран тип отображения данных **Текущая загрузка**, справа от легенды отображается средняя скорость обработки данных за последние 5 минут.

Пример:

На графике **Обработка данных**, где выбраны Sensor типа (**SPAN**) и тип отображения данных **Текущая загрузка**, отображается скорость обработки данных зеркалированного трафика локальной сети, поступающих от компонента Sensor (см. раздел "Компонент Sensor" на стр. 49) на сервер с компонентом Central Node (см. раздел "Компонент Central Node" на стр. 50) в определенное время.

Отображаются следующие данные:

- **Трафик** – скорость поступления трафика на сервер с компонентом Central Node зеленым цветом.
- **Файлы** – скорость обработки файлов серым цветом.
- **URL-адреса** – скорость обработки URL-адресов синим цветом.
- **Ошибки обработки** – ошибки обработки данных вертикальными линиями красного цвета.

При наведении курсора мыши на график появляется всплывающее окно, в котором отображается скорость обработки данных в определенное время.

Если выбран тип отображения данных **Пользовательский диапазон**, справа от легенды отображается средняя скорость поступления трафика на сервер с компонентом Central Node и количество обработанных объектов за выбранный период.

Пример:

На графике **Обработка данных**, где выбраны Sensor типа (**SMTP**) и тип отображения данных **Пользовательский диапазон** с настроенным периодом отображения данных **Месяц**, отображается скорость поступления почтового трафика по протоколу SMTP 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.
- **Файлы** – количество извлеченных файлов серым цветом.
- **URL-адреса** – количество извлеченных URL-адресов синим цветом.
- **Ошибки обработки** – ошибки обработки данных вертикальными линиями красного цвета.

При наведении курсора мыши на график появляется всплывающее окно, в котором отображается скорость поступления трафика на сервер с компонентом Central Node и количество обработанных объектов в определенное время.

Мониторинг обработки данных модулями и компонентами программы

На графике **Очереди** вы можете оценить статус обработки данных модулями программы **YARA**, **AM Engine**, **Risk Score**, компонентом **Sandbox** и отследить ошибки обработки данных.

Вы можете выбрать тип отображения данных в раскрывающемся списке справа от названия графика **Очереди**:

- **Текущая загрузка** – 5 минут до текущего момента.
- **Выбранный период**. В этом случае вы также можете настроить период отображения данных на графиках (см. раздел "Настройка периода отображения данных на графиках" на стр. [171](#)).

В левой части графика отображается легенда графика по цветам, которыми данные отображены на самом графике.

На графике **Очереди** отображаются следующие данные:

- **Количество сообщений** и **Объем данных**, обработанных модулями и компонентами программы:
 - **YARA** – синим цветом.
 - **Sandbox** – фиолетовым цветом.
 - **AM Engine** – зеленым цветом.
 - **RS Engine** – оранжевым цветом.
- **Ошибки обработки** – ошибки обработки данных вертикальными линиями красного цвета.

При наведении курсора мыши на график появляется всплывающее окно, в котором отображается статус обработки данных модулями программы **YARA**, **AM Engine**, **RS Engine** и компонентом **Sandbox**, а также ошибки обработки данных в определенное время.

На графике **Время обработки в Sandbox** 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 период.

Пример:

Если настроен период отображения данных на графиках **Месяц**, на графике **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 "Архитектура программы" на стр. [49](#)) и распределив по этим серверам данные, предназначенные для обработки.

Таблица 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 с виртуальной машины или сервера с программой Kaspersky Secure Mail Gateway, если она используется в вашей организации.
- данных о запущенных процессах, открытых сетевых соединениях и изменяемых файлах, полученных от отдельных компьютеров, которые входят в IT-инфраструктуру организации и работают под управлением операционной системы Microsoft Windows.

Kaspersky Anti Targeted Attack Platform отображает обнаруженные признаки целевых атак и вторжений в IT-инфраструктуру организации в виде таблицы обнаружений.




Таблица обнаружений находится в разделе **Обнаружения**, на закладке **Все** окна веб-интерфейса программы.

Также в разделе **Обнаружения** на закладке **Комплексные** находится таблица комплексных обнаружений. *Комплексное обнаружение* – обнаружение, при котором одна или несколько технологий программы опубликовали несколько результатов проверки, связанных друг с другом.

В таблице обнаружений содержится следующая информация:

1.  – принадлежность обнаружения группе с особыми правами доступа. Например, обнаружения группы VIP недоступны для просмотра пользователями программы **Сотрудник службы безопасности**.
2. **Время** – время, в которое программа выполнила обнаружение.
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 программа обнаружила 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 программы, выполнивших обнаружение.

В графе **Технологии** могут быть указаны следующие модули и компоненты программы:

- **(YARA) YARA.**
- **(SB) Sandbox.**
- **(URL) URL Reputation.**
- **(IDS) Intrusion Detection System.**
- **(AM) AM Engine.**
- **(TAA) Targeted Attack Analyzer.**
- **(IOC-DB) IOC в базе Событий.**
- **(IOC-ES) IOC на Endpoint Sensors.**

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:

- **Новых** – новые обнаружения.
- **В обработке** – обнаружения, которые один из пользователей Kaspersky Anti Targeted Attack Platform уже обрабатывает.
- **Обработано** – обнаружения, отмеченные пользователем Kaspersky Anti Targeted Attack Platform как обработанные.
- **Повторная проверка** – обнаружения, выполненные в результате повторной проверки объекта.

Кроме того, в этой графе отображается имя пользователя, которому назначено данное обнаружение. Например, Administrator.

Если информация в графах 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.**
- Имя файла:
 - **Завершить процесс.**
 - **Удалить файл.**
 - **Получить файл.**
 - **Отправить файл в Карантин.**
 - **Найти в базе Событий.**

- Хеш MD5:
 - **Найти на Kaspersky Threat Intelligence Portal.**
 - **Запретить запуск этого файла.**
 - **Найти файл в Хранилище.**
 - **Найти в базе Событий.**
- Хеш SHA256:
 - **Запретить запуск этого файла.**
 - **Найти файл в Хранилище.**
 - **Найти в базе Событий.**
 - **Найти на virustotal.com.**
- IP-адрес: **Найти на Kaspersky Threat Intelligence Portal.**
- Имя хоста или IP-адрес:
 - **Завершить процесс.**
 - **Удалить файл.**
 - **Получить файл.**
 - **Отправить файл в Карантин.**
 - **Выполнить программу.**
 - **Найти в базе Событий.**

Фильтрация и поиск обнаружений


Вы можете отфильтровать обнаружения для отображения в таблице обнаружений по одной или нескольким графам таблицы или выполнить поиск обнаружений по некоторым графам 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. Фильтры сохраняются на том компьютере, на котором пользователь Kaspersky Anti Targeted Attack Platform открывает веб-интерфейс программы.


В этом разделе

Фильтрация обнаружений по принадлежности группе	184
Фильтрация и поиск обнаружений по времени	185
Фильтрация обнаружений по степени важности	185
Фильтрация и поиск обнаружений по категориям обнаруженных объектов	186
Фильтрация и поиск обнаружений по полученной информации	187
Фильтрация и поиск обнаружений по адресу источника	187
Фильтрация и поиск обнаружений по названиям модулей и компонентов программы	188
Фильтрация и поиск обнаружений по состоянию их обработки пользователем	189
Быстрое создание фильтра обнаружений	190
Сохранение фильтра обнаружений	190
Изменение имени фильтра обнаружений	191
Создание фильтра обнаружений на основе существующего фильтра	191
Сброс фильтра обнаружений	192
Удаление фильтра обнаружений	192

Фильтрация обнаружений по принадлежности группе

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю  – принадлежность обнаружения группе обнаружений с особыми правами доступа. Например, обнаружения группы VIP недоступны для просмотра пользователями программы **Сотрудник службы безопасности**.

► *Чтобы отфильтровать обнаружения по принадлежности к группе, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.
Откроется таблица обнаружений.
2. По значку  откройте окно настройки фильтрации обнаружений.
3. Настройте фильтрацию обнаружений:
 - Если вы хотите, чтобы в таблице обнаружений отображались только обнаружения,

принадлежащие определенной группе, установите флажок рядом с названием этой группы.

Например, если вы хотите, чтобы в таблице обнаружений отображались только обнаружения группы VIP, установите флажок рядом с названием группы **VIP**.

- Если вы хотите, чтобы в таблице обнаружений отображались только обнаружения, не принадлежащие никаким группам, установите флажок рядом с названием **Остальные**.

Если ни одно из значений не выбрано, в таблице отображаются все обнаружения независимо от их принадлежности группе.

4. Нажмите на кнопку **Применить**.

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 **Время** – время, в которое произошло обнаружение.

- *Чтобы отфильтровать или найти обнаружения по времени, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

Откроется таблица обнаружений.

2. По ссылке **Время создания** / **Время обновления** раскройте список периодов отображения обнаружений.

3. В списке **Время** выберите один из следующих периодов отображения обнаружений:

- **Все**, если вы хотите, чтобы программа отображала в таблице все обнаружения.
- **Прошедший час**, если вы хотите, чтобы программа отображала в таблице обнаружения, произошедшие за последний час.
- **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице обнаружения, произошедшие за последний день.
- **Пользовательский диапазон**, если вы хотите, чтобы программа отображала 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, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.
Откроется таблица обнаружений.
2. По значку  откройте окно настройки фильтрации обнаружений.
3. Выберите одну или несколько из следующих степеней важности обнаружений:
 - **Высокая** – обнаружение высокой степени важности.
 - **Средняя** – обнаружение средней степени важности.
 - **Низкая** – обнаружение низкой 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 программа отображала в таблице обнаружения файлов, зараженных определенным вирусом, вы можете задать фильтр по названию этого вируса.

► *Чтобы отфильтровать или найти обнаружения по категориям обнаруженных объектов, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.
Откроется таблица обнаружений.
2. По ссылке **Обнаружено** откройте окно настройки фильтрации обнаружений.
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.

В этом поле вы также можете осуществлять поиск обнаружений типа **Aggregated alert** – комплексное обнаружение, при котором одна или несколько технологий программы опубликовали несколько результатов проверки, связанных друг с другом.

5. 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, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.
Откроется таблица обнаружений.
2. По ссылке **Сведения** откройте окно настройки фильтрации обнаружений.
3. В раскрывающемся списке **Сведения** выберите один из следующих критериев поиска:
 - **Сведения**. Поиск будет осуществляться по всем сведениям об обнаруженном объекте.
 - **ID**.
 - **Имя файла**.
 - **Тип файла**.
 - **MD5**.
 - **SHA256**.
 - **URL**.
 - **Домен**.
 - **User Agent**.
 - **Тема**.
 - **HTTP-статус**.
 - **Источник данных**.
 - **Тип объекта**.
4. В 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. 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.

► *Чтобы отфильтровать или найти обнаружения по адресу источника, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.
Откроется таблица обнаружений.
 2. По ссылке **Адрес источника** откройте окно настройки фильтрации обнаружений.
 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. Нажмите на кнопку **Применить**.
- В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по названиям модулей и компонентов программы

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 названиям модулей и компонентов программы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.
Откроется таблица обнаружений.
2. По ссылке **Технологии** откройте окно настройки фильтрации обнаружений по названиям модулей и компонентов программы.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации обнаружений:
 - **Содержит**, если вы хотите, чтобы программа отображала обнаружения, выполненные модулем или компонентом программы, который вы укажете.
 - **Не содержит**, если вы хотите, чтобы программа скрывала обнаружения, выполненные модулем или компонентом программы, который вы укажете.
 - **Равняется**, если вы хотите, чтобы программа отображала обнаружения, выполненные модулем или компонентом программы, который вы укажете.
 - **Не равняется**, если вы хотите, чтобы программа скрывала обнаружения, выполненные модулем или компонентом программы, который вы укажете.
4. В раскрывающемся списке справа от выбранного вами оператора фильтрации обнаружений выберите название модуля или компонента программы, по которому вы хотите отфильтровать обнаружения:

- (YARA) YARA.
- (SB) Sandbox.
- (URL) URL Reputation.
- (IDS) Intrusion Detection System.
- (AM) AM Engine.
- (TAA) Targeted Attack Analyzer.
- (IOC-DB) IOC в базе Событий.
- (IOC-ES) IOC на Endpoint Sensors.

Например, если вы хотите, чтобы программа отобразила в списке обнаружения, выполненные компонентом Sandbox, выберите оператор фильтрации **Содержит** и название компонента **(SB) Sandbox**.



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**.

Окно настройки фильтрации обнаружений по названиям модулей и компонентов программы закроется.

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, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.
Откроется таблица обнаружений.
2. По ссылке **Состояние** раскройте список вариантов обнаружений в зависимости от состояния их обработки пользователем Kaspersky Anti Targeted Attack Platform.
3. Выберите одно из следующих значений:
 - **Новых**, если вы хотите, чтобы программа отображала новые обнаружения, которые ни один из пользователей еще не начал обрабатывать.
 - **В обработке**, если вы хотите, чтобы программа отображала обнаружения, которые один из пользователей Kaspersky Anti Targeted Attack Platform уже обрабатывает.
 - **Обработано**, если вы хотите, чтобы программа отображала обнаружения, отмеченные пользователем Kaspersky Anti Targeted Attack Platform как обработанные.
 - **Повторная проверка**, если вы хотите, чтобы программа отображала обнаружения, произошедшие в результате повторной проверки.

4. В поле **Имя пользователя** введите имя пользователя, если вы хотите найти обнаружения, назначенные определенному пользователю **Старший сотрудник службы безопасности** или **Сотрудник службы безопасности**.
5. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Быстрое создание фильтра обнаружений

► *Чтобы быстро создать фильтр обнаружений, выполните следующие действия:*

1. В окне веб-интерфейса программы 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 графы 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.

Сохранение фильтра обнаружений



► *Чтобы сохранить фильтр обнаружений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.
Откроется таблица обнаружений.
2. Выполните фильтрацию обнаружений по интересующим вас показателям.
3. Нажмите на кнопку **Фильтры** в правом верхнем углу окна веб-интерфейса программы.
Откроется список действий над фильтрами.
4. В списке действий над фильтрами выберите **Сохранить текущий фильтр**.

Фильтр сохранится в списке фильтров обнаружений в правом верхнем углу окна веб-интерфейса программы.

Изменение имени фильтра обнаружений

► Чтобы изменить имя фильтра обнаружений, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.
Откроется таблица обнаружений.
2. Раскройте список фильтров обнаружений **Фильтры**.
3. Наведите курсор мыши на фильтр, имя которого вы хотите изменить.
4. Нажмите на кнопку  справа от имени фильтра.
5. Внесите необходимые изменения в поле редактирования имени фильтра.
6. Нажмите на кнопку  справа от поля редактирования имени фильтра.


Новое имя фильтра отобразится в списке фильтров обнаружений в правом верхнем углу окна веб-интерфейса программы.

Создание фильтра обнаружений на основе существующего фильтра

► Чтобы создать фильтр событий на основе существующего фильтра, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.
Откроется таблица событий, обнаруженных программой.
2. Раскройте список фильтров событий **Сохраненные фильтры**.
3. Выберите фильтр, который вы хотите изменить.
4. Если вы хотите добавить условия фильтрации в изменяемый фильтр, выполните действия по быстрому добавлению условий фильтрации в изменяемый фильтр:
 - a. Наведите курсор мыши на ссылку с тем значением графы таблицы, которое вы хотите добавить в качестве условия фильтрации.
 - b. Нажмите на левую клавишу мыши.
Откроется список действий над значением.
 - c. В открытом 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.

Если вы хотите добавить несколько условий фильтрации в изменяемый фильтр, выполните действия по быстрому добавлению каждого из условий фильтрации.

5. Если вы хотите удалить условия фильтрации из изменяемого фильтра, нажмите на кнопку  справа от заголовка графы с выбранным условием фильтрации.
6. Нажмите на кнопку **Фильтры** в правом верхнем углу окна веб-интерфейса программы.

Откроется список действий над фильтрами.

7. В списке действий над фильтрами выберите **Сохранить текущий фильтр**.


Фильтр сохранится в списке фильтров обнаружений в правом верхнем углу окна веб-интерфейса программы.

Сброс фильтра обнаружений

- ▶ *Чтобы сбросить фильтр обнаружений по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

Откроется таблица обнаружений.

2. Нажмите на кнопку  справа от того заголовка графы 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.

Удаление фильтра обнаружений


- ▶ *Чтобы удалить фильтр обнаружений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

Откроется таблица обнаружений.

2. Нажмите на кнопку **Фильтры** в правом верхнем углу окна веб-интерфейса программы.

Откроется список действий над фильтрами.

3. Нажмите на кнопку  справа от названия фильтра, который вы хотите удалить.

Фильтр будет удален из списка фильтров обнаружений.

Просмотр обнаружений

В веб-интерфейсе программы 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. Программа обнаружила 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. Программа обнаружила этот файл в 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. Программа обнаружила 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. Программа обнаружила эту сетевую активность в зеркалированном трафике локальной сети организации.
- На компьютере локальной сети организации были запущены процессы. Программа обнаружила эти процессы модулем Endpoint Sensors, установленным на отдельные компьютеры, входящие в IT-инфраструктуру организации и работающие под управлением операционной системы Microsoft Windows.

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 при попадании в операционные системы Windows XP SP3, 32-разрядную Windows 7 и 64-разрядную Windows 7, выполненного компонентом Sandbox;
- результаты эвристического анализа поведения исполняемого файла формата APK в операционной системе Android, выполненного ядром Risk Score.

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 исследования сетевой активности компьютера, выполненного модулем Targeted Attack Analyzer;
- результаты проверки интернет-трафика на наличие признаков вторжения в IT-инфраструктуру организации по предустановленным правилам, выполненной модулем Intrusion Detection System (IDS).

Если обнаружены процессы, запущенные на компьютере локальной сети организации, на котором установлен компонент Endpoint Sensors, в веб-интерфейсе программы может отображаться следующая информация:

- общая информация об обнаружении и процессах, запущенных на этом компьютере;
- результаты исследования сетевой активности компьютера, выполненного модулем Targeted Attack Analyzer.

В этом разделе

Просмотр информации об обнаружении	194
Общая информация об обнаружении	195
Информация в блоке Информация об объекте	195
Информация в блоке Информация об обнаружении	196
Информация в блоке Сетевое событие	196
Информация в блоке Результаты проверки	197
Информация в блоке Удаленные хосты	198
Информация о сетевой активности компьютера в блоке Процессы	198
Информация в блоке Данные учетной записи пользователя	199
Информация в блоке Модули, загруженные процессом	199
Информация в блоке История изменения обнаружения	200
Отправка данных об обнаружении	200

Просмотр информации об обнаружении

► Чтобы просмотреть информацию об обнаружении, выполните следующие действия:

1. В окне веб-интерфейса программы 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

В заголовке окна с информацией об обнаружении отображается идентификатор обнаружения.

В верхней части окна с информацией об обнаружении может отображаться следующая общая информация об обнаружении:

- **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".
- **Состояние** – состояние обнаружения в зависимости от того, обработал пользователь Kaspersky Anti Targeted Attack Platform это обнаружение или нет.
- **Назначено** – имя пользователя, которому назначено данное обнаружение.
- **Хост** – доменное имя компьютера, на котором произошло обнаружение.
- **Источник данных** – источник данных. Например, SMTP Sensor или SPAN Sensor.

Информация в блоке Информация об объекте

В блоке **Информация об объекте** может отображаться следующая информация об обнаруженном файле:

- **Объект** – имя файла.
По ссылке **Скачать** рядом с именем файла вы можете 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.
- **Тип объекта** – тип файла. Например, ExecutableWin32.
- **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 Kaspersky Threat Intelligence Portal.**
 - **Скопировать значение в буфер.**
 - **Найти в базе Событий.**
 - **Запретить запуск этого файла.**
- **SHA256** – SHA256-хеш файла.
По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - **Найти на virustotal.com.**
 - **Скопировать значение в буфер.**
 - **Найти в базе Событий.**
 - **Запретить запуск этого файла.**
- **Скачать артефакт IDS** – Файл, содержащий результат анализа сетевых данных обнаруженного объекта. По ссылке рядом с названием параметра **Скачать артефакт IDS** вы можете загрузить файл


на жесткий диск вашего компьютера. Файл загружается в формате PCAP (Packet Capture).

Файл подписан – автор сертификата, в котором содержится цифровая подпись к обнаруженному файлу.

- **Сообщение от** – адрес электронной почты, с которого было отправлено сообщение, содержащее файл.
- **Получатели сообщения** – один или несколько адресов электронной почты, на которые было отправлено сообщение, содержащее файл.
- **Тема сообщения** – тема сообщения.
- **Заголовки сообщения** – 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:

-  – 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 программа обнаружила 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 или Post.
- **URL** – обнаруженный URL-адрес.
- **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.
- **Запрос/Ответ** – длина запроса и ответа.

Информация в блоке Сетевое событие

В блоке **Сетевое событие** может отображаться следующая информация о ссылке на веб-сайт, открытой на компьютере:

- **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.
- **User Agent** – 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.
- **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.

- **Имя пользователя** – имя учетной записи пользователя компьютера, на котором была открыта ссылка на веб-сайт, был загружен файл или была предпринята попытка загрузки файла.

Информация в блоке Результаты проверки

В блоке **Результаты проверки** могут отображаться следующие результаты проверки обнаружения:

- Названия модулей или компонентов программы, выполнивших обнаружение.
- Результаты проверки обнаружений модулями и компонентами программы.
- Результаты эвристического анализа поведения файла в операционной системе Android, выполненного модулем Risk Score.
- Результаты исследования поведения файла в операционной системе Windows XP SP3, выполненного компонентом Sandbox.
- Результаты исследования поведения файла в 32-разрядной операционной системе Windows 7, выполненного компонентом Sandbox.
- Результаты исследования поведения файла в 64-разрядной операционной системе Windows 7, выполненного компонентом Sandbox.
- **Обнаружено** – одна или несколько категорий обнаруженного объекта. Например, может отображаться название вируса Virus.Win32.Chiton.i.
- **Размер файла** – размер файла.
- **MD5** – MD5-хеш файла.
- **Подписано** – автор сертификата, в котором содержится цифровая подпись к обнаруженному файлу.
- **Активность** – действия файла внутри операционной системы. По ссылке **Активность** отобразится список действий файла.
- **Журнал HTTP-активности** – журнал HTTP-активности файла. Содержит следующую информацию:
 - **IP назначения** – IP-адрес, на который файл пытается перейти из операционной системы.
 - **Запрос** – метод HTTP-запроса, например, GET или POST.
 - **URL** – URL-адрес ссылки на веб-сайт, которую файл пытается открыть из операционной системы.
- **Журнал DNS-активности** – журнал DNS-активности файла. Содержит следующую информацию:
 - **Запрос** – имя и тип DNS-запроса.
 - **Ответ** – имя, тип ответа от DNS-сервера, а также имя хоста или IP-адрес компьютера, с которого был получен ответ.
- **Скачать полный журнал** – журнал исследования поведения файла в каждой операционной системе.
- **YARA** – категория обнаруженного файла в YARA-правилах (например, может отображаться название категории susp_fake_Microsoft_signer).
- **Intrusion Detection System** – категория обнаруженного объекта по базе Intrusion Detection System. Например, может отображаться категория Bot.AridViper.UDP.C&C.
- **Anti-Malware Engine** – категория обнаруженного объекта по антивирусной базе. Например, может

отображаться название вируса Virus.Win32.Chiton.i.

- Версии баз модулей и компонентов Kaspersky Anti Targeted Attack Platform, выполнивших обнаружение.
- Дата и время последнего обновления баз.
- **Скачать полный журнал** – журнал исследования поведения файла в каждой операционной системе.
- **Скачать сведения об отладке** – подробный журнал исследования поведения файла во всех операционных системах. По ссылке рядом с названием параметра **Скачать сведения об отладке** вы можете загрузить файл на жесткий диск вашего компьютера.

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 1 ТБ. По достижении этого ограничения программа удаляет журналы исследования поведения файлов, созданные раньше остальных, и заменяет их новыми журналами.

Информация в блоке Удаленные хосты

В блоке **Удаленные хосты** отображается список хостов, с которыми связана обнаруженная сетевая активность. По ссылке с именем хоста вы можете раскрыть блок информации о сетевой активности, связанной с этим хостом.

Отобразится следующая информация:

- IP-адрес или доменное имя компьютера, с которым связывался компьютер локальной сети организации.
- **Регистратор** – название организации – регистратора доменов, которая зарегистрировала этот домен.
- **Информация о домене** – подробная информация о домене.
- **Популярность в мире** – популярность домена в мире.
- **Обнаружено в локальной сети** – дата и время обнаружения хоста Kaspersky Anti Targeted Attack Platform.
- **Подключенные компьютеры** – количество компьютеров локальной сети организации, связывающихся с обнаруженным доменом.

Информация о сетевой активности компьютера в блоке Процессы

В блоке **Процессы** отображается список процессов, с которыми связана обнаруженная сетевая активность. По ссылке с путем к процессу вы можете раскрыть блок информации об этом процессе.

Отобразится следующая информация:

- **Путь к файлу** – путь к файлу процесса.

- **Название программы** – название программы, запустившей процесс.
- **Описание файла** – дополнительная информация об обнаруженном файле.
- **Размер файла** – размер обнаруженного файла.
- **Версия файла** – версия обнаруженного файла.
- **MD5** – MD5-хеш файла.
- **SHA256** – SHA256-хеш файла.
- **Поставщик** – компания, выпустившая программу, к которой относится процесс.
- **Версия программы** – версия программы.
- **Подписано** – автор сертификата, в котором содержится цифровая подпись к обнаруженному файлу.
- **Подпись действительна** – дата истечения срока действия сертификата.
- **Обнаружено в локальной сети** – дата и время обнаружения процесса в локальной сети.
- **Обнаружено на компьютерах** – количество раз, которое этот процесс был обнаружен в локальной сети.
- **Компьютеров с подобной активностью** – количество компьютеров, на которых был обнаружен подобный процесс.
- **Популярность файла в мире** – популярность файла, запустившего процесс, в мире.
- **Популярность пути в мире** – популярность пути, по которому был загружен процесс, в мире.

Информация в блоке Данные учетной записи пользователя

В блоке **Данные учетной записи пользователя** отображается информация об учетной записи пользователя компьютера, на котором была обнаружена сетевая активность.

Отображается следующая информация:

- **Тип учетной записи** – тип учетной записи. Например, Administrator.
- **Тип входа** – тип входа в компьютер.
- **Обнаружен в сети** – дата и время, когда сетевая активность была впервые обнаружена в локальной сети.
- **Обнаружен на компьютере** – дата и время, когда активность была впервые обнаружена на компьютере.
- **Используется на компьютерах** – количество компьютеров, на которых была обнаружена аналогичная сетевая активность.

Информация в блоке Модули, загруженные процессом

В блоке **Модули, загруженные процессом** отображается информация о модулях, загруженных процессом, с которым связана обнаруженная сетевая активность. Например, процессом может быть загружена библиотека dll. По ссылке с путем к модулю вы можете раскрыть блок информации об этом процессе.

Отобразится следующая информация:

- **Название программы** – имя файла, загруженного процессом.
- **Описание файла** – дополнительная информация об обнаруженном файле.
- **Размер файла** – размер обнаруженного файла.
- **Версия файла** – версия обнаруженного файла.
- **MD5** – MD5-хеш файла.
- **SHA256** – SHA256-хеш файла.
- **Поставщик** – компания, выпустившая программу, к которой относится процесс.
- **Версия программы** – версия программы.
- **Подписано** – автор сертификата, в котором содержится цифровая подпись к обнаруженному файлу.
- **Подпись действительна** – дата истечения срока действия сертификата.
- **Обнаружено в локальной сети** – дата и время обнаружения процесса в локальной сети.
- **Обнаружено на компьютерах** – количество раз, которое этот процесс был обнаружен в локальной сети.
- **Компьютеров с подобной активностью** – количество компьютеров, на которых был обнаружен подобный процесс.
- **Популярность файла в мире** – популярность файла, запустившего процесс, в мире.
- **Популярность пути в мире** – популярность пути, по которому был загружен процесс, в мире.

Информация в блоке История изменения обнаружения

В блоке **Журнал изменений** может отображаться следующая информация об обнаружении:

- Дата и время изменения обнаружения.
- Автор изменений.
Например, **Система** или имя пользователя программы.
- 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, произведенном модулями и компонентами программы (кроме модулей URL Reputation и AM Engine) 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, выполните следующие действия:*

1. В окне веб-интерфейса программы 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 предоставить их в "Лабораторию Касперского" для дальнейшего исследования.

Действия пользователей над обнаружениями

При работе в веб-интерфейсе программы под учетной записью с ролью **Старший сотрудник службы безопасности** или **Сотрудник службы безопасности** вы можете выполнять следующие действия над обнаружениями:

- Назначить обнаружение себе или другому пользователю веб-интерфейса программы.
Вы можете просмотреть все обнаружения, назначенные определенному пользователю, используя фильтр обнаружений по состоянию их обработки пользователем.
- Назначить обнаружение себе, не раскрывая информацию об обнаружении.
- Отметить обнаружение как обработанное.
Вы можете отмечать те обнаружения, обработку которых вы закончили, как обработанные. Вы можете просмотреть все обнаружения, обработанные определенным пользователем, используя фильтр обнаружений по состоянию их обработки пользователем.
- Добавить комментарий к обнаружению.
Вы можете найти события, содержащие комментарий, по ключевым словам комментария, используя фильтр обнаружений по полученной информации (см. раздел "Фильтрация и поиск обнаружений по полученной информации" на стр. [187](#)).

Пользователи **Старший сотрудник службы безопасности** также могут отметить обнаружение как VIP – принадлежность обнаружения группе обнаружений с особыми правами доступа. Например, обнаружения группы VIP недоступны для просмотра пользователями программы **Сотрудник службы безопасности**.

Пользователи **Старший сотрудник службы безопасности** могут просмотреть все события, принадлежащие группе VIP, используя фильтр событий по принадлежности группе.

В этом разделе

Назначение обнаружения определенному пользователю	202
Назначение обнаружения себе.....	203
Отметка о завершении обработки обнаружения	203
Отметка о принадлежности обнаружения группе VIP	204
Добавление комментария к обнаружению	204
Сохранение списка всех обнаружений на жесткий диск компьютера	205

Назначение обнаружения определенному пользователю

► *Чтобы назначить обнаружение себе или другому пользователю веб-интерфейса программы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.
Откроется таблица обнаружений.
2. Выберите одну из закладок:

- **Все**, если вы хотите просмотреть все обнаружения.
 - **Комплексные**, если вы хотите просмотреть комплексные обнаружения.
3. Выберите обнаружение.
Откроется окно с информацией об обнаружении.
 4. Если вы хотите назначить обнаружение себе, в раскрывающемся списке в правом верхнем углу окна с информацией об обнаружении нажмите на кнопку **Назначить мне**.
 5. Если вы хотите назначить событие другому пользователю, выполните следующие действия:
 - a. Раскройте список пользователей под записью **Назначить мне**, если событие еще никому не назначено или под записью **Переназначить**, если событие назначено вам.
 - b. Нажатием левой клавиши мыши выберите пользователя, которому вы хотите назначить событие.
 6. Нажмите на кнопку **Закрыть**.
Обнаружение будет назначено выбранному пользователю.

Вы можете просмотреть все обнаружения, назначенные определенному пользователю, используя фильтр обнаружений по состоянию их обработки пользователем.

Назначение обнаружения себе

► *Чтобы назначить обнаружение себе, не раскрывая информацию об обнаружении, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.
Откроется таблица обнаружений.
2. Выберите одну из закладок:
 - **Все**, если вы хотите просмотреть все обнаружения.
 - **Комплексные**, если вы хотите просмотреть комплексные обнаружения.
3. Наведите курсор мыши на графу **Состояние** того обнаружения, которое вы хотите назначить себе.
4. Нажмите на левую клавишу мыши.
Откроется список действий над значением.
5. Нажмите на кнопку **Назначить мне**.
Событие будет назначено текущему пользователю.

Вы можете просмотреть все обнаружения, назначенные определенному пользователю, используя фильтр обнаружений по состоянию их обработки пользователем.

Отметка о завершении обработки обнаружения

► *Чтобы отметить обнаружение как обработанное, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.
Откроется таблица обнаружений.

2. Выберите одну из закладок:
 - **Все**, если вы хотите просмотреть все обнаружения.
 - **Комплексные**, если вы хотите просмотреть комплексные обнаружения.
3. Выберите обнаружение.
Откроется окно с информацией об обнаружении.
4. Нажмите на кнопку **Отметить как обработанное**.
Обнаружение будет отмечено как обработанное.

Вы можете просмотреть все обнаружения, обработанные определенным пользователем, используя фильтр обнаружений по состоянию их обработки пользователем.

Отметка о принадлежности обнаружения группе VIP

Пользователи **Старший сотрудник службы безопасности** могут отмечать обнаружения как принадлежащие группе VIP.

► *Чтобы отметить обнаружение как принадлежащее группе VIP, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.
Откроется таблица обнаружений.
2. Выберите одну из закладок:
 - **Все**, если вы хотите просмотреть все обнаружения.
 - **Комплексные**, если вы хотите просмотреть комплексные обнаружения.
3. Выберите обнаружение.
Откроется окно с информацией об обнаружении.
4. Установите флажок рядом с названием группы **VIP**.
Событие будет отмечено как принадлежащее группе VIP.

Пользователи **Старший сотрудник службы безопасности** могут просмотреть все события, принадлежащие группе VIP, используя фильтр обнаружений по принадлежности группе (см. раздел "Фильтрация обнаружений по принадлежности группе" на стр. [184](#)).

Добавление комментария к обнаружению

► *Чтобы добавить комментарий к обнаружению, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.
Откроется таблица обнаружений.
2. Выберите одну из закладок:
 - **Все**, если вы хотите просмотреть все обнаружения.

- **Комплексные**, если вы хотите просмотреть комплексные обнаружения.
3. Выберите обнаружение.
Откроется окно с информацией об обнаружении.
 4. В поле добавления комментария под названием блока **Журнал изменений** введите комментарий к обнаружению.
 5. 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. [187](#)).

Сохранение списка всех обнаружений на жесткий диск компьютера

► *Чтобы сохранить список всех обнаружений на жесткий диск компьютера, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.
2. Нажмите на кнопку **Экспортировать все** в правой верхней части окна.

Архив с файлами, содержащими список всех обнаружений, 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 Kaspersky Anti Targeted Attack Platform.

Информация о событиях


При работе в веб-интерфейсе программы пользователи **Старший сотрудник службы безопасности** или **Сотрудник службы безопасности** могут просматривать информацию о событиях, кроме событий группы VIP. События группы VIP могут просматривать только пользователи **Старший сотрудник службы безопасности**.

В этом разделе

Просмотр таблицы событий.....	206
Просмотр информации о событии.....	208
Информация о запуске процесса	208
Информация об удаленном соединении	210
Информация о загрузке модуля	212
Информация о срабатывании запрета запуска файла	214
Информация о блокировании документа	216
Информация о создании файла	219
Информация о событии в журнале Windows.....	221
Информация об изменении в реестре	222
Информация о прослушивании порта.....	223
Информация о загрузке драйвера.....	224
Информация об изменении имени хоста.....	226

Просмотр таблицы событий

Таблица событий отображается в разделе **Поиск угроз** окна веб-интерфейса программы после выполнения поиска событий.

События сгруппированы по хостам. Для каждого хоста по кнопке  отображается отдельная таблица событий.

В таблице событий содержится следующая информация:

1. **Событие** – тип события.
2. **Сведения** – сведения о событии.
3. **Дополнительно** – дополнительная информация о событии.
4. **Имя пользователя** – имя пользователя.
5. **Время события** – дата и время обнаружения события.

Каждому типу событий соответствует свой тип значения ячейки в графах таблицы событий **Сведения** и **Дополнительно** (см. таблицу ниже).

Таблица 4. Соответствие типов значений ячеек в графах **Событие**, **Сведения** и **Дополнительно**

Событие	Сведения	Дополнительно
Запущен процесс	Имя файла процесса, который был запущен	Хеш SHA256 и MD5
Загружен модуль	Имя динамической библиотеки, которая была загружена	Хеш SHA256 и MD5
Удаленное соединение	URL-адрес, к которому была произведена попытка удаленного подключения	Имя файла, который пытался осуществить удаленное подключение
Сработал запрет запуска файла	Имя файла приложения, запуск которого был заблокирован	Хеш SHA256 и MD5
Документ заблокирован	Имя документа, запуск которого был заблокирован	Хеш SHA256 и MD5
Создан файл	Имя созданного файла	Хеш SHA256 и MD5
Событие в журнале Windows	Канал записи событий в журнал Windows	Идентификатор типа события
Свойства реестра	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	Хеш SHA256 и MD5
Изменено имя хоста	Старое имя хоста	Новое имя хоста


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 типа значения ячейки вы можете выполнить одно из следующих действий:

- Любой тип значения ячейки:
 - **Добавить в фильтр.**
 - **Исключить из фильтра.**
 - **Скопировать значение в буфер.**
- Имя файла:
 - **Завершить процесс.**
 - **Удалить файл.**
 - **Получить файл.**

- Отправить файл в Карантин.
- Хеш MD5:
 - Найти на [Kaspersky Threat Intelligence Portal](#).
 - Запретить запуск этого файла.
 - Найти файл в Хранилище.
- Хеш SHA256:
 - Запретить запуск этого файла.
 - Найти файл в Хранилище.
- IP-адрес: Найти на [Kaspersky Threat Intelligence Portal](#).

Просмотр информации о событии

► Чтобы просмотреть информацию о событии, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**.
Откроется форма поиска событий.
2. Выполните поиск событий с помощью режима конструктора или режима исходного кода.
Откроется список хостов с событиями, соответствующими заданным условиям поиска.
3. В списке хостов по кнопке  откройте таблицу событий хоста.
4. Выберите событие, информацию о котором вы хотите просмотреть.
Откроется окно с информацией о событии.

Информация о запуске процесса

В окне **Информация о событии** содержится следующая информация о событиях типа **Свойства запущенного процесса**:

- **Дерево событий.**
Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.
Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях о них.
- **Запущен процесс.**
Блок параметров **Запущен процесс** содержит следующую информацию о параметрах события:
 - **Время события** – время запуска процесса.
 - **Имя файла** – имя файла процесса.
По ссылке рядом с названием параметра **Имя файла** раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - **Скопировать значение в буфер.**

- **Найти в базе Событий.**
- **Завершить процесс.**
- **Удалить файл.**
- **Получить файл.**
- **Отправить файл в Карантин.**
- **Параметры запуска** – параметры запуска процесса.
- **MD5** – MD5-хеш файла процесса.

По ссылке рядом с названием параметра **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на Kaspersky Threat Intelligence Portal.**
- **Скопировать значение в буфер.**
- **Найти в базе Событий.**
- **Запретить запуск этого файла.**
- **SHA256** – SHA256-хеш файла процесса.
По ссылке рядом с названием параметра **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - **Найти на virustotal.com.**
 - **Скопировать значение в буфер.**
 - **Найти в базе Событий.**
 - **Запретить запуск этого файла.**
- **Размер** – размер файла процесса.
- **ID процесса** – идентификатор процесса.
- **Время завершения процесса** – время завершения процесса.
- **Время создания** – время создания файла процесса.
- **Время изменения** – время последнего изменения файла процесса.
- **Имя хоста** – имя хоста, на котором был запущен процесс.

По ссылке рядом с названием параметра **Имя хоста** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на Kaspersky Threat Intelligence Portal.**
- **Скопировать значение в буфер.**
- **Завершить процесс.**
- **Удалить файл.**
- **Получить файл.**
- **Отправить файл в Карантин.**
- **Выполнить программу.**
- **Имя пользователя** – имя пользователя, запустившего процесс.

- **Родительский процесс.**

Блок параметров **Родительский процесс** содержит следующую информацию о родительском процессе события:

- **Имя файла** – имя файла родительского процесса.

По ссылке рядом с названием параметра **Имя файла** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Скопировать значение в буфер.
- Найти в базе Событий.
- Завершить процесс.
- Удалить файл.
- Получить файл.
- Отправить файл в Карантин.

- **MD5** – MD5-хеш файла родительского процесса.

По ссылке рядом с названием параметра **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти на Kaspersky Threat Intelligence Portal.
- Скопировать значение в буфер.
- Найти в базе Событий.
- Запретить запуск этого файла.

- **SHA256** – SHA256-хеш файла родительского процесса.

По ссылке рядом с названием параметра **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти на virustotal.com.
- Скопировать значение в буфер.
- Найти в базе Событий.
- Запретить запуск этого файла.

- **ID процесса** – идентификатор родительского процесса.

Информация об удаленном соединении

В окне **Информация о событии** содержится следующая информация о событиях типа **Удаленное соединение**:

- **Дерево событий.**

Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях о них.

- **Удаленное соединение.**

Блок параметров **Удаленное соединение** содержит следующую информацию о параметрах события:

- **Время события** – время попытки удаленного соединения.
- **URL** – веб-адрес, на который была произведена попытка удаленного соединения.
- **Удаленный хост** – IP-адрес хоста, на который была произведена попытка удаленного соединения.
- **Локальный IP-адрес** – IP-адрес локального компьютера, с которого была произведена попытка удаленного соединения.
- **Имя хоста** – имя хоста, с которого была произведена попытка удаленного соединения.

По ссылке рядом с названием параметра **Имя хоста** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на Kaspersky Threat Intelligence Portal.**
- **Скопировать значение в буфер.**
- **Завершить процесс.**
- **Удалить файл.**
- **Получить файл.**
- **Отправить файл в Карантин.**
- **Выполнить программу.**
- **Имя пользователя** – имя пользователя, который пытался установить удаленное соединение.
- **Родительский процесс.**

Блок параметров **Родительский процесс** содержит следующую информацию о родительском процессе события:

- **Файл** – имя файла родительского процесса.

По ссылке рядом с названием параметра **Файл** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Скопировать значение в буфер.**
- **Найти в базе Событий.**
- **Завершить процесс.**
- **Удалить файл.**
- **Получить файл.**
- **Отправить файл в Карантин.**
- **MD5** – MD5-хеш файла родительского процесса.

По ссылке рядом с названием параметра **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на Kaspersky Threat Intelligence Portal.**
- **Скопировать значение в буфер.**
- **Найти в базе Событий.**

- **Запретить запуск этого файла.**
- **SHA256** – SHA256-хеш файла родительского процесса.
По ссылке рядом с названием параметра **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - **Найти на [virustotal.com](https://www.virustotal.com).**
 - **Скопировать значение в буфер.**
 - **Найти в базе Событий.**
 - **Запретить запуск этого файла.**

Информация о загрузке модуля

В окне **Информация о событии** содержится следующая информация о событиях типа **Загружен модуль**:

- **Дерево событий.**
Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.
Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях о них.
- **Загружен модуль.**
Блок параметров **Загружен модуль** содержит следующую информацию о параметрах события:
 - **Время события** – время загрузки модуля.
 - **Файл** – имя файла загруженного модуля.
По ссылке рядом с названием параметра **Файл** раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - **Скопировать значение в буфер.**
 - **Найти в базе Событий.**
 - **Завершить процесс.**
 - **Удалить файл.**
 - **Получить файл.**
 - **Отправить файл в Карантин.**
 - **MD5** – MD5-хеш файла загруженного модуля.
По ссылке рядом с названием параметра **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - **Найти на [Kaspersky Threat Intelligence Portal](https://www.kaspersky.com/threat-intelligence-portal).**
 - **Скопировать значение в буфер.**
 - **Найти в базе Событий.**
 - **Запретить запуск этого файла.**
 - **SHA256** – SHA256-хеш файла загруженного модуля.

По ссылке рядом с названием параметра **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на virustotal.com.**
 - **Скопировать значение в буфер.**
 - **Найти в базе Событий.**
 - **Запретить запуск этого файла.**
- **Имя хоста** – имя хоста, на котором был загружен модуль.

По ссылке рядом с названием параметра **Имя хоста** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на Kaspersky Threat Intelligence Portal.**
 - **Скопировать значение в буфер.**
 - **Завершить процесс.**
 - **Удалить файл.**
 - **Получить файл.**
 - **Отправить файл в Карантин.**
 - **Выполнить программу.**
- **Имя пользователя** – имя пользователя, загрузившего модуль.
 - **Размер** – размер загруженного модуля.
 - **Время создания** – время создания загруженного модуля.
 - **Время изменения** – дата последнего изменения загруженного модуля.
- **Родительский процесс.**

Блок параметров **Родительский процесс** содержит следующую информацию о родительском процессе события:

- **Файл** – имя файла родительского процесса.

По ссылке рядом с названием параметра **Файл** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Скопировать значение в буфер.**
 - **Найти в базе Событий.**
 - **Завершить процесс.**
 - **Удалить файл.**
 - **Получить файл.**
 - **Отправить файл в Карантин.**
- **MD5** – MD5-хеш файла родительского процесса.

По ссылке рядом с названием параметра **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на Kaspersky Threat Intelligence Portal.**

- Скопировать значение в буфер.
- Найти в базе Событий.
- Запретить запуск этого файла.
- **SHA256** – SHA256-хеш файла родительского процесса.

По ссылке рядом с названием параметра **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти на [virustotal.com](https://www.virustotal.com).
- Скопировать значение в буфер.
- Найти в базе Событий.
- Запретить запуск этого файла.

Информация о срабатывании запрета запуска файла

В окне **Информация о событии** содержится следующая информация о событиях типа **Сработал запрет запуска файла**:

- Дерево событий.

Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях о них.

- **Сработал запрет запуска файла.**

Блок параметров **Сработал запрет запуска файла** содержит следующую информацию о параметрах события:

- **Время события** – время срабатывания запрета запуска файла.
- **Имя файла** – имя файла, запуск которого был запрещен..

По ссылке рядом с названием параметра **Имя файла** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Скопировать значение в буфер.
- Найти в базе Событий.
- Завершить процесс.
- Удалить файл.
- Получить файл.
- Отправить файл в Карантин.
- **Параметры запуска** – параметры, с которыми была произведена попытка запуска файла.
- **MD5** – MD5-хеш файла, запуск которого был запрещен.

По ссылке рядом с названием параметра **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти на [Kaspersky Threat Intelligence Portal](#).
 - Скопировать значение в буфер.
 - Найти в базе Событий.
 - Запретить запуск этого файла.
- **SHA256** – SHA256-хеш файла, запуск которого был запрещен.

По ссылке рядом с названием параметра **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти на [virustotal.com](#).
 - Скопировать значение в буфер.
 - Найти в базе Событий.
 - Запретить запуск этого файла.
- **Размер** – размер файла, запуск которого был запрещен.
 - **Время создания** – время создания файла, запуск которого был запрещен.
 - **Время изменения** – дата последнего изменения файла, запуск которого был запрещен.
 - **Имя хоста** – имя хоста, на котором сработал запрет запуска файла.

По ссылке рядом с названием параметра **Имя хоста** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти на [Kaspersky Threat Intelligence Portal](#).
 - Скопировать значение в буфер.
 - Завершить процесс.
 - Удалить файл.
 - Получить файл.
 - Отправить файл в Карантин.
 - Выполнить программу.
- **Имя пользователя** – имя пользователя, попытавшегося запустить файл.
- **Родительский процесс.**

Блок параметров **Родительский процесс** содержит следующую информацию о родительском процессе события:

- **Имя файла** – имя файла родительского процесса.
- По ссылке рядом с названием параметра **Имя файла** раскрывается список, в котором вы можете выбрать одно из следующих действий:
- Скопировать значение в буфер.
 - Найти в базе Событий.
 - Завершить процесс.
 - Удалить файл.
 - Получить файл.

- **Отправить файл в Карантин.**
- **MD5** – MD5-хеш файла родительского процесса.
По ссылке рядом с названием параметра **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - **Найти на Kaspersky Threat Intelligence Portal.**
 - **Скопировать значение в буфер.**
 - **Найти в базе Событий.**
 - **Запретить запуск этого файла.**
- **SHA256** – SHA256-хеш файла родительского процесса.
По ссылке рядом с названием параметра **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - **Найти на virustotal.com.**
 - **Скопировать значение в буфер.**
 - **Найти в базе Событий.**
 - **Запретить запуск этого файла.**
- **ID процесса** – идентификатор родительского процесса.

Если компонент Endpoint Sensors обнаружил комплексное событие, информация о событии не будет отражена в веб-интерфейсе программы.

Информация о блокировании документа

В окне **Информация о событии** содержится следующая информация о событиях типа **Документ заблокирован**:

- **Дерево событий.**
Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.
Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях о них.
- **Документ заблокирован.**
Блок параметров **Документ заблокирован** содержит следующую информацию о параметрах события:
 - **Время события** – время блокирования документа.
 - **Имя файла** – имя заблокированного документа.
По ссылке рядом с названием параметра **Имя файла** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Скопировать значение в буфер.
 - Найти в базе Событий.
 - Завершить процесс.
 - Удалить файл.
 - Получить файл.
 - Отправить файл в Карантин.
- **MD5** – MD5-хеш заблокированного документа.
По ссылке рядом с названием параметра **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - Найти на [Kaspersky Threat Intelligence Portal](#).
 - Скопировать значение в буфер.
 - Найти в базе Событий.
 - Запретить запуск этого файла.
 - **Файл процесса** – имя файла процесса, который попытался открыть документ.
По ссылке рядом с названием параметра **Файл процесса** раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - Скопировать значение в буфер.
 - Найти в базе Событий.
 - Завершить процесс.
 - Удалить файл.
 - Получить файл.
 - Отправить файл в Карантин.
 - **MD5 процесса** – MD5-хеш процесса, который попытался открыть документ.
По ссылке рядом с названием параметра **MD5 процесса** раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - Найти на [Kaspersky Threat Intelligence Portal](#).
 - Скопировать значение в буфер.
 - Найти в базе Событий.
 - Запретить запуск этого файла.
 - **SHA256 процесса** – SHA256-хеш процесса, который попытался открыть документ.
По ссылке рядом с названием параметра **SHA256 процесса** раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - Найти на [virustotal.com](#).
 - Скопировать значение в буфер.
 - Найти в базе Событий.
 - Запретить запуск этого файла.

- **ID процесса** – идентификатор процесса, который попытался открыть документ.
- **Имя хоста** – имя хоста, на котором был заблокирован документ.

По ссылке рядом с названием параметра **Имя хоста** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на Kaspersky Threat Intelligence Portal.**
 - **Скопировать значение в буфер.**
 - **Завершить процесс.**
 - **Удалить файл.**
 - **Получить файл.**
 - **Отправить файл в Карантин.**
 - **Выполнить программу.**
- **Имя пользователя** – имя пользователя, попытавшегося открыть документ.
- **Родительский процесс.**

Блок параметров **Родительский процесс** содержит следующую информацию о родительском процессе события:

- **Имя файла** – имя файла родительского процесса.
По ссылке рядом с названием параметра **Имя файла** раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - **Скопировать значение в буфер.**
 - **Найти в базе Событий.**
 - **Завершить процесс.**
 - **Удалить файл.**
 - **Получить файл.**
 - **Отправить файл в Карантин.**
- **MD5** – MD5-хеш файла родительского процесса.
По ссылке рядом с названием параметра **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - **Найти на Kaspersky Threat Intelligence Portal.**
 - **Скопировать значение в буфер.**
 - **Найти в базе Событий.**
 - **Запретить запуск этого файла.**
- **SHA256** – SHA256-хеш файла родительского процесса.
По ссылке рядом с названием параметра **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - **Найти на virustotal.com.**
 - **Скопировать значение в буфер.**

- **Найти в базе Событий.**
- **Запретить запуск этого файла.**
- **ID процесса** – идентификатор родительского процесса.

Информация о создании файла

В окне **Информация о событии** содержится следующая информация о событиях типа **Создан файл**:

- **Дерево событий.**

Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях о них.

- **Создан файл.**

Блок параметров **Создан файл** содержит следующую информацию о параметрах события:

- **Время события** – время обнаружения события.
- **Имя файла** – имя созданного файла.

По ссылке рядом с названием параметра **Имя файла** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Скопировать значение в буфер.**
- **Найти в базе Событий.**
- **Завершить процесс.**
- **Удалить файл.**
- **Получить файл.**
- **Отправить файл в Карантин.**
- **MD5** – MD5-хеш созданного файла.

По ссылке рядом с названием параметра **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на Kaspersky Threat Intelligence Portal.**
- **Скопировать значение в буфер.**
- **Найти в базе Событий.**
- **Запретить запуск этого файла.**
- **SHA256** – SHA256-хеш созданного файла.

По ссылке рядом с названием параметра **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на virustotal.com.**
- **Скопировать значение в буфер.**
- **Найти в базе Событий.**

- **Запретить запуск этого файла.**
- **Размер** – размер созданного файла.
- **Время создания** – время создания файла.
- **Время изменения** – время последнего изменения файла.
- **Имя хоста** – имя хоста, на котором был создан файл.

По ссылке рядом с названием параметра **Имя хоста** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на Kaspersky Threat Intelligence Portal.**
 - **Скопировать значение в буфер.**
 - **Завершить процесс.**
 - **Удалить файл.**
 - **Получить файл.**
 - **Отправить файл в Карантин.**
 - **Выполнить программу.**
- **Имя пользователя** – имя пользователя, создавшего файл.
 - **Родительский процесс.**

Блок параметров **Родительский процесс** содержит следующую информацию о родительском процессе события:

- **Имя файла** – имя файла родительского процесса.

По ссылке рядом с названием параметра **Имя файла** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Скопировать значение в буфер.**
 - **Найти в базе Событий.**
 - **Завершить процесс.**
 - **Удалить файл.**
 - **Получить файл.**
 - **Отправить файл в Карантин.**
- **MD5** – MD5-хеш файла родительского процесса.

По ссылке рядом с названием параметра **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на Kaspersky Threat Intelligence Portal.**
 - **Скопировать значение в буфер.**
 - **Найти в базе Событий.**
 - **Запретить запуск этого файла.**
- **SHA256** – SHA256-хеш файла родительского процесса.

По ссылке рядом с названием параметра **SHA256** раскрывается список, в котором вы можете

выбрать одно из следующих действий:

- **Найти на [virustotal.com](https://www.virustotal.com).**
- **Скопировать значение в буфер.**
- **Найти в базе Событий.**
- **Запретить запуск этого файла.**

Информация о событии в журнале Windows

В окне **Информация о событии** содержится следующая информация о событиях типа **Событие в журнале Windows**:

- **Дерево событий.**

Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях о них.

- **Событие в журнале Windows.**

Блок параметров **Событие в журнале Windows** содержит следующую информацию о параметрах события:

- **Время события** – время обнаружения события.
- **ID события безопасности** – идентификатор типа события безопасности в журнале Windows.
- **ID записи** – идентификатор события в журнале Windows.
- **Провайдер** – имя провайдера.
- **Имя журнала** – имя журнала Windows.
- **Домен** – домен, которому принадлежит хост, на котором произошло событие.
- **Имя хоста** – имя хоста, на котором произошло событие.

По ссылке рядом с названием параметра **Имя хоста** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на [Kaspersky Threat Intelligence Portal](https://www.kaspersky.com/threat-intelligence-portal).**
- **Скопировать значение в буфер.**
- **Завершить процесс.**
- **Удалить файл.**
- **Получить файл.**
- **Отправить файл в Карантин.**
- **Выполнить программу.**
- **Имя пользователя** – имя пользователя хоста, на котором произошло событие.

Также блок параметров **Событие в журнале Windows** содержит данные из системного журнала Windows. Состав данных зависит от типа события Windows.

Информация об изменении в реестре

В окне **Информация о событии** содержится следующая информация о событиях типа **Изменение в реестре**:

- **Дерево событий.**

Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях о них.

- **Изменение в реестре.**

Блок параметров **Изменение в реестре** содержит следующую информацию о параметрах события:

- **Время события** – время внесения изменения в реестр.
- **Путь к разделу реестра** – путь к разделу реестра, в котором было произведено изменение.
- **Имя параметра** – имя параметра ключа в реестре.
- **Значение** – значение параметра ключа в реестре.
- **Имя хоста** – имя хоста, на котором было произведено изменение в реестре.

По ссылке рядом с названием параметра **Имя хоста** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на Kaspersky Threat Intelligence Portal.**
- **Скопировать значение в буфер.**
- **Завершить процесс.**
- **Удалить файл.**
- **Получить файл.**
- **Отправить файл в Карантин.**
- **Выполнить программу.**
- **Имя пользователя** – имя пользователя, совершившего изменение в реестре.
- **Родительский процесс.**

Блок параметров **Родительский процесс** содержит следующую информацию о родительском процессе события:

- **Имя файла** – имя файла родительского процесса.

По ссылке рядом с названием параметра **Имя файла** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Скопировать значение в буфер.**
- **Найти в базе Событий.**
- **Завершить процесс.**
- **Удалить файл.**
- **Получить файл.**

- **Отправить файл в Карантин.**
- **MD5** – MD5-хеш файла родительского процесса.
По ссылке рядом с названием параметра **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - **Найти на Kaspersky Threat Intelligence Portal.**
 - **Скопировать значение в буфер.**
 - **Найти в базе Событий.**
 - **Запретить запуск этого файла.**
- **SHA256** – SHA256-хеш файла родительского процесса.
По ссылке рядом с названием параметра **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - **Найти на virustotal.com.**
 - **Скопировать значение в буфер.**
 - **Найти в базе Событий.**
 - **Запретить запуск этого файла.**

Информация о прослушивании порта

В окне **Информация о событии** содержится следующая информация о событиях типа **Прослушан порт**:

- **Дерево событий.**
Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.
Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях о них.
- **Прослушан порт.**
Блок параметров **Прослушан порт** содержит следующую информацию о параметрах события:
 - **Время события** – время прослушивания порта.
 - **Порт** – порт, который был прослушан.
 - **IP** – IP-адрес сетевого интерфейса, порт которого был прослушан.
 - **Имя хоста** – имя хоста, порт которого был прослушан.
По ссылке рядом с названием параметра **Имя хоста** раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - **Найти на Kaspersky Threat Intelligence Portal.**
 - **Скопировать значение в буфер.**
 - **Завершить процесс.**
 - **Удалить файл.**
 - **Получить файл.**

- Отправить файл в Карантин.
- Выполнить программу.
- **Имя пользователя** – имя пользователя, от имени которого было совершено прослушивание порта.
- **Родительский процесс.**

Блок параметров **Родительский процесс** содержит следующую информацию о родительском процессе события:

- **Имя файла** – имя файла родительского процесса.
По ссылке рядом с названием параметра **Имя файла** раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - Скопировать значение в буфер.
 - Найти в базе Событий.
 - Завершить процесс.
 - Удалить файл.
 - Получить файл.
 - Отправить файл в Карантин.
- **MD5** – MD5-хеш файла родительского процесса.
По ссылке рядом с названием параметра **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - Найти на **Kaspersky Threat Intelligence Portal**.
 - Скопировать значение в буфер.
 - Найти в базе Событий.
 - Запретить запуск этого файла.
- **SHA256** – SHA256-хеш файла родительского процесса.
По ссылке рядом с названием параметра **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - Найти на **virustotal.com**.
 - Скопировать значение в буфер.
 - Найти в базе Событий.
 - Запретить запуск этого файла.

Информация о загрузке драйвера

В окне **Информация о событии** содержится следующая информация о событиях типа **Загружен драйвер**:

- **Дерево событий.**
Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях о них.

- **Загружен драйвер.**

Блок параметров **Загружен драйвер** содержит следующую информацию о параметрах события:

- **Время события** – время загрузки драйвера.
- **Имя файла** – имя файла загруженного драйвера.

По ссылке рядом с названием параметра **Имя файла** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Скопировать значение в буфер.**
 - **Найти в базе Событий.**
 - **Завершить процесс.**
 - **Удалить файл.**
 - **Получить файл.**
 - **Отправить файл в Карантин.**
- **MD5** – MD5-хеш файла загруженного драйвера.

По ссылке рядом с названием параметра **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на Kaspersky Threat Intelligence Portal.**
 - **Скопировать значение в буфер.**
 - **Найти в базе Событий.**
 - **Запретить запуск этого файла.**
- **SHA256** – SHA256-хеш файла загруженного драйвера.

По ссылке рядом с названием параметра **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на Kaspersky Threat Intelligence Portal.**
 - **Скопировать значение в буфер.**
 - **Завершить процесс.**
 - **Удалить файл.**
 - **Получить файл.**
- **Имя хоста** – имя хоста, на который был загружен драйвер.

По ссылке рядом с названием параметра **Имя хоста** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на Kaspersky Threat Intelligence Portal.**
- **Скопировать значение в буфер.**
- **Завершить процесс.**
- **Удалить файл.**
- **Получить файл.**

- **Отправить файл в Карантин.**
- **Выполнить программу.**
- **Размер** – размер загруженного драйвера.
- **Время создания** – время создания загруженного драйвера.
- **Время изменения** – время последнего изменения загруженного драйвера.

Информация об изменении имени хоста

В окне **Информация о событии** содержится следующая информация о событиях типа **Изменено имя хоста**:

- **Дерево событий.**

Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях о них.
- **Изменено имя хоста.**

Блок параметров **Изменено имя хоста** содержит следующую информацию о параметрах события:

 - **Время события** – время изменения имени хоста.
 - **Имя хоста** – новое имя хоста.

По ссылке рядом с названием параметра **Имя хоста** раскрывается список, в котором вы можете выбрать одно из следующих действий:

 - **Найти на Kaspersky Threat Intelligence Portal.**
 - **Скопировать значение в буфер.**
 - **Завершить процесс.**
 - **Удалить файл.**
 - **Получить файл.**
 - **Отправить файл в Карантин.**
 - **Выполнить программу.**
 - **Имя пользователя** – имя пользователя, изменившего имя хоста.
 - **Старое имя хоста** – старое имя хоста.

Поиск угроз по базе событий

При работе в веб-интерфейсе программы пользователи **Старший сотрудник службы безопасности** или **Сотрудник службы безопасности** могут выполнять следующие действия над событиями: формировать поисковые запросы и использовать IOC-файлы для поиска угроз по базе событий.

Для формирования поисковых запросов вы можете использовать *режим конструктора* или *режим исходного кода*.

В режиме конструктора вы можете создавать и изменять поисковые запросы с помощью раскрывающихся списков с вариантами типа значения поля и операторов.

В режиме исходного кода вы можете создавать и изменять поисковые запросы с помощью текстовых команд.

В этом разделе

Поиск событий с помощью режима конструктора	227
Поиск событий с помощью режима исходного кода	230
Изменение условий поиска событий	230
Скачивание файла с описанием событий на локальный компьютер	231
Импорт IOC-файла для поиска событий	231
Сохранение условия поиска событий	232

Поиск событий с помощью режима конструктора

► *Чтобы создать условие поиска событий в режиме конструктора, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**.
Откроется форма поиска событий.
2. В раскрывающемся списке выберите один из следующих типов значения поля, которое вы хотите использовать для поиска событий:
 - **Поиск по всему тексту: FullTextSearch.**
 - **Общие:**
 - **Host.**
 - **EventType.**
 - **UserName.**
 - **Свойства файла:**
 - **CreationTime.**
 - **FileName.**
 - **FilePath.**
 - **FileFullName.**
 - **ModificationTime.**

- **FileSize.**
 - **Md5.**
 - **Sha256.**
 - **Свойства запущенного процесса:**
 - **PID.**
 - **ParentFileFullName.**
 - **ParentMd5.**
 - **ParentSha256.**
 - **StartupParameters.**
 - **ParentPID.**
 - **Свойства сетевого соединения:**
 - **HTTPMethod.**
 - **LocalIP.**
 - **LocalPort.**
 - **RemoteHostName.**
 - **RemoteIP.**
 - **RemotePort.**
 - **URI.**
 - **Свойства реестра:**
 - **RegistryKey.**
 - **RegistryValueName.**
 - **RegistryValue.**
 - **Свойства события в журнале Windows:**
 - **WinLogEventId.**
 - **WinLogName.**
 - **WinLogEventRecordId.**
 - **WinLogProviderName.**
 - **WinLogTargetDomainName.**
 - **WinLogObjectName.**
 - **WinLogPackageName.**
 - **WinLogProcessName.**
 - **Изменение имени хоста: OldHostName.**
3. В раскрывающемся списке выберите один из следующих операторов сравнения:
- **=.**
 - **!=.**

- **CONTAINS.**
- **!CONTAINS.**
- **STARTS.**
- **!STARTS.**
- **ENDS.**
- **!ENDS.**
- **>.**
- **<.**

Для каждого типа значения поля будет доступен свой релевантный набор операторов сравнения. 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, нажмите на кнопку **Время** и выберите один из следующих периодов поиска событий:
 - **Все**, если вы хотите, чтобы программа отображала в таблице события, найденные за все время.
 - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице события, найденные за предыдущий час.
 - **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице события, найденные за предыдущий день.
 - **Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице события, найденные за указанный вами период.
9. 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.
10. Нажмите на кнопку **Найти**.

Откроется таблица событий, соответствующих заданным вами условиям поиска.

Поиск событий с помощью режима исходного кода

► Чтобы создать условие поиска событий в режиме исходного кода, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**.

Откроется форма поиска событий.

По ссылке **Перейти в режим исходного кода** откройте поле ввода исходного кода.

2. Введите условия поиска событий, используя команды, логические операторы **OR** и **AND**, а также скобки для создания групп условий.

Команды должны соответствовать следующему синтаксису: <тип поля> <оператор сравнения> <значение поля>.

Пример:

```
EventType = "filechange"
AND (
  FileName CONTAINS "example"
  OR UserName = "example"
)
```

3. Если вы хотите выполнить поиск событий за определенный период, нажмите на кнопку **Время** и выберите один из следующих периодов поиска событий:

- **Все**, если вы хотите, чтобы программа отображала в таблице события, найденные за все время.
- **Прошедший час**, если вы хотите, чтобы программа отображала в таблице события, найденные за предыдущий час.
- **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице события, найденные за предыдущий день.
- **Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице события, найденные за указанный вами период.

4. 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.

5. Нажмите на кнопку **Найти**.

Откроется таблица событий, соответствующих введенным вами условиям поиска.

Изменение условий поиска событий

► Чтобы изменить сохраненные условия поиска событий, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **ИОС-проверка**.

Откроется таблица IOC-файлов.

2. Выберите закладку **База Событий**.
3. Выберите сохраненные условия поиска событий, которые вы хотите изменить.
4. Нажмите на кнопку **Изменить запрос**.

Откроется новая закладка с разделом **Поиск угроз**.

5. Выполните одно из следующих действий:

- Если вы хотите использовать режим конструктора, нажмите на кнопку .

- Если вы хотите использовать режим исходного кода, нажмите на кнопку .


6. Внесите необходимые изменения.
7. Нажмите на кнопку **Найти**.

Откроется таблица событий, соответствующих введенным вами условиям поиска.

Скачивание файла с описанием событий на локальный компьютер

После выполнения поиска событий вы можете скачать файл с описанием событий, удовлетворяющих критериям поиска, на локальный компьютер. Найденные события сохраняются в отдельный файл для каждого хоста.

► *Чтобы скачать файл с описанием событий, выполните следующие действия:*


1. В списке хостов наведите курсор мыши на хост, описание событий которого вы хотите скачать.
2. Нажмите на кнопку .
3. В зависимости от параметров вашего браузера, сохраните файл в папку по умолчанию или укажите папку для сохранения файла.

Файл с описанием событий в формате JSON будет сохранен на ваш локальный компьютер. Для просмотра этого файла вам нужно использовать JSON-парсер, например, вы можете воспользоваться сайтом <http://jsoneditoronline.org> <http://jsoneditoronline.org>.

Импорт IOC-файла для поиска событий

► *Чтобы импортировать IOC-файл, выполните следующие действия:*


1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**.
Откроется форма поиска событий.

2. Нажмите на кнопку .

3. В раскрывающемся списке выберите действие **Импортировать IOC-файл**.
Откроется окно выбора файлов.
4. Выберите IOC-файл, который хотите импортировать, и нажмите на кнопку **Открыть**.
IOC-файл начнет использоваться для поиска событий.

Сохранение условия поиска событий

► Чтобы сохранить условие поиска событий, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**.
Откроется форма поиска событий.
2. Выполните поиск событий с помощью режима конструктора или режима исходного кода.
3. Нажмите на кнопку .
4. В раскрывающемся списке выберите **Сохранить как**.
Откроется окно **Сохранить**.
5. В поле **Сохранить как новый IOC-файл под именем** введите имя условия поиска событий.
6. Нажмите на кнопку **Сохранить**.
Условие поиска событий будет сохранено.

Работа с задачами

При работе в веб-интерфейсе программы пользователи **Старший сотрудник службы безопасности** могут работать с файлами и программами на хостах путем создания и удаления задач: выполнять и останавливать программы, скачивать и удалять файлы, помещать объекты в Хранилище и Карантин, а также восстанавливать их из Карантина.

Пользователи **Сотрудник службы безопасности** могут работать только с задачами, которые они создали, и не имеют доступа к задачам для адресов группы VIP.

Максимальное время выполнения задачи составляет 24 часа. Если за это время задача не успела завершиться, ее выполнение останавливается.

В этом разделе

Просмотр таблицы задач	233
Просмотр информации о задаче	235
Создание задачи завершения процесса	235
Создание задачи выполнения программы	236
Создание задачи получения файла	237
Создание задачи удаления файла	238
Создание задачи помещения файла в Карантин	239
Создание задачи восстановления файла из Карантина	239
Создание копии задачи	240
Удаление задачи	240
Фильтрация задач по времени создания	240
Фильтрация задач по типу	241
Фильтрация задач на основе имени и пути к файлу	242
Фильтрация задач по описанию	242
Фильтрация задач по автору	243
Фильтрация задач по статусу	243
Фильтрация результатов выполнения задачи по имени хоста	244

Просмотр таблицы задач

Таблица задач содержит список созданных задач и находится в разделе **Задачи** окна веб-интерфейса программы.

Таблица имеет следующие закладки:

- **Все.** Отображает задачи, созданные всеми пользователями.
- **Мои.** Отображает задачи, созданные текущим пользователем.

В таблице задач содержится следующая информация:

1. **Время создания** – дата и время создания задачи.
2. **Тип** – тип задачи.

Задача может быть одного из следующих типов:

- **Завершить процесс.**
- **Выполнить программу.**
- **Получить файл.**
- **Удалить файл.**
- **Отправить файл в Карантин.**
- **Восстановить файл из Карантина.**

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.**

3. **Хосты** – хосты, для которых создана задача.
4. **Сведения** – полный путь к файлу, для которого создана задача.

По ссылке со сведениями о задаче раскрывается список, в котором можно выбрать одно из следующих действий:

- **Добавить в фильтр.**
- **Исключить из фильтра.**
- **Скопировать значение в буфер.**

5. **Описание** – описание задачи.
6. **Автор** – имя пользователя, создавшего задачу.

Если вы выбрали закладку **Мои**, эта графа не будет отображаться.

7. **Состояние** – статус выполнения задачи.

Задача может иметь один из следующих статусов:

- **Ожидает.**
- **В обработке.**
- **Завершено.**

Просмотр информации о задаче

► Чтобы просмотреть информацию о задаче, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.
Откроется таблица задач.
2. Выберите одну из следующих закладок:
 - **Все**.
 - **Мои**.
3. 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.
- **Команда** – команда запуска программы.
- **Рабочий каталог** – рабочий каталог программы.
- **Запущено от имени** – параметр запуска программы: от имени текущего пользователя или от имени локальной системы.
- **Автор** – имя пользователя, создавшего задачу.
- **Время создания** – время создания задачи.
- **Время завершения** – время завершения задачи.
- **Хосты** – список хостов, на которых выполняется задача.

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, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.
Откроется таблица задач.
2. Нажмите на кнопку **Добавить** и выберите **Завершить процесс**.
Откроется окно создания задачи.
3. Укажите следующие параметры:
 - a. **Путь к файлу** – путь к файлу процесса, который вы хотите завершить.
 - b. **Описание** – описание задачи.
 - c. **Задача для** – область применения задачи:

- Если вы хотите завершить процесс на всех хостах, выберите вариант **Всех хостов**.
 - Если вы хотите завершить процесс на некоторых хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты.
4. Нажмите на кнопку **Добавить**.
- Будет создана задача завершения процесса.


Создание задачи выполнения программы

► Чтобы создать задачу выполнения программы, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.
Откроется таблица задач.
 2. Нажмите на кнопку **Добавить** и выберите **Выполнить программу**.
Откроется окно создания задачи.
 3. Укажите следующие параметры:
 - a. Если вы хотите запустить программу от имени текущего пользователя, в поле **Параметры** снимите флажок **Запустить от имени SYSTEM**.
По умолчанию флажок установлен. Программа будет запущена от имени SYSTEM.
 - b. Выберите одно из следующих действий:
 - Если вы хотите запустить программу с помощью командной строки (cmd.exe), выберите вариант **Выполнить команду** и введите команду в поле **Команда**.
 - Если вы хотите запустить команду напрямую, выберите вариант **Запустить файл**, укажите полный путь к файлу в поле **Путь к файлу** и ключи запуска в поле **Аргументы**.
 - c. **Рабочий каталог** – рабочий каталог программы.
 - d. **Описание** – описание задачи.
 - e. **Задача для** – область применения задачи:
 - Если вы хотите запустить программу на всех хостах, выберите вариант **Всех хостов**.
 - Если вы хотите запустить программу на некоторых хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты.
 4. Нажмите на кнопку **Добавить**.
- Будет создана задача запуска программы.

Пример:

► Чтобы полностью отключить сетевые интерфейсы хоста с помощью выполнения команды от имени текущего пользователя на всех хостах, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.
Откроется таблица задач.
2. Нажмите на кнопку **Добавить** и выберите **Выполнить программу**.
Откроется окно создания задачи.
3. Укажите следующие параметры:
 - a. В поле **Параметры** снимите флажок **Запустить от имени SYSTEM**.
По умолчанию флажок установлен.
 - b. Выберите вариант **Выполнить команду** и введите команду `netsh interface show interface` в поле **Команда**.
 - c. В поле **Рабочий каталог** укажите рабочий каталог программы.
 - d. В поле **Описание** введите описание задачи.
 - e. Выберите область применения задачи **Всех хостов**.
4. Нажмите на кнопку **Добавить**.
5. Выберите созданную вами задачу отключения сетевого интерфейса хоста.
6. В окне информации о задаче нажмите на кнопку  и перейдите по ссылке **Стандартный вывод**.
Откроется окно со списком активных сетевых интерфейсов удаленного хоста.
7. Для каждого подключенного сетевого интерфейса создайте задачу выполнения команды `netsh interface set interface <Имя интерфейса> admin=disable`.

Сетевой интерфейс, соединяющий хост с компонентом Central Node, отключайте в последнюю очередь.

После успешного выполнения задачи сетевые интерфейсы хоста будут отключены.

Создание задачи получения файла

► Чтобы создать задачу получения файла, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.
Откроется таблица задач.
2. Нажмите на кнопку **Добавить** и выберите **Получить файл**.
Откроется окно создания задачи.
3. Укажите следующие параметры:

- a. **Путь к файлу** – путь к файлу, который вы хотите получить.
 - b. **Описание** – описание задачи.
 - c. **Хост** – имя хоста или IP-адрес сервера, с которого вы хотите получить файл.
4. Если вы хотите отказаться от проверки файла, снимите флажок **Отправить на проверку**.
По умолчанию флажок установлен.
 5. Нажмите на кнопку **Добавить**.

Будет создана задача получения файла. 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.

► *Чтобы скачать полученный файл на ваш локальный компьютер, выполните следующие действия:*

1. Откройте задачу получения файла.
2. В нижней части окна **Получить файл** нажмите на имя хоста или IP-адрес.
Откроется окно с информацией о файле.
3. Нажмите на кнопку **Скачать**.
Файл будет сохранен на ваш локальный компьютер.

Создание задачи удаления файла

► *Чтобы создать задачу удаления файла, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.
Откроется таблица задач.
2. Нажмите на кнопку **Добавить** и выберите **Удалить файл**.
Откроется окно создания задачи.
3. Укажите следующие параметры:
 - a. **Путь к файлу** – путь к файлу, который вы хотите удалить.
 - b. **Описание** – описание задачи.
 - c. **Задача для** – область применения задачи:
 - Если вы хотите удалить файл со всех хостов, выберите вариант **Всех хостов**.
 - Если вы хотите удалить файл с некоторых хостов, выберите вариант **Выбранных хостов** и перечислите эти хосты.
4. Нажмите на кнопку **Добавить**.

Будет создана задача удаления файла.

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.

Создание задачи помещения файла в Карантин

Если вы считаете, что на компьютере находится зараженный или возможно зараженный файл, вы можете изолировать его, поместив в Карантин (см. раздел "Работа с объектами в Хранилище" на стр. [264](#)).

► *Чтобы создать задачу помещения файла в Карантин, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.
Откроется таблица задач.
2. Нажмите на кнопку **Добавить** и выберите **Отправить файл в Карантин**.
Откроется окно создания задачи.
3. Укажите следующие параметры:
 - a. **Путь к файлу** – путь к файлу, который вы хотите поместить в Карантин.
 - b. **Описание** – описание задачи.
 - c. **Хост** – имена хостов, с которых вы хотите удалить файл, поместив его копию в Карантин.
4. Если вы хотите отказаться от проверки файла, снимите флажок **Отправить на проверку**.
По умолчанию флажок установлен.
5. Нажмите на кнопку **Добавить**.

Будет создана задача помещения файла в Карантин. В результате выполнения задачи файл будет удален с выбранных хостов и помещен в Карантин.

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.

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" на стр. [264](#)) на хост.

► *Чтобы создать задачу восстановления файла из Карантина, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.
Откроется таблица задач.
2. Нажмите на кнопку **Добавить** и выберите **Восстановить файл из Карантина**.
Откроется окно создания задачи.
3. Укажите следующие параметры:

- a. **Описание** – описание задачи.
- b. **Файл в Карантине** – имя файла в Карантине.

Также вы можете выбрать файл для восстановления из списка.

4. Нажмите на кнопку **Добавить**.

Будет создана задача восстановления файла из Карантина.

После восстановления файла из Карантина на хост метаданные о файле останутся в таблице объектов, помещенных в Хранилище.

Создание копии задачи

► *Чтобы скопировать задачу, выполните следующие действия:*

1. В окне веб-интерфейса программы 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. Нажмите на кнопку **Добавить**.
Будет создана копия выбранной задачи.

Удаление задачи

Если вы удалите задачу в процессе ее выполнения, результат выполнения задачи может не сохраниться.
Если вы удалите успешно выполненную задачу скачивания файла, файл будет удален.

► *Чтобы удалить задачу, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.
Откроется таблица задач.
2. Откройте задачу, которую вы хотите удалить.
3. Нажмите на кнопку **Удалить**.
Задача будет удалена.

Фильтрация задач по времени создания

► *Чтобы отфильтровать задачи по времени их создания, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

Откроется таблица задач.

- По ссылке **Время** откройте меню фильтрации задач.
- Выберите один из следующих периодов отображения задач:
 - Все**, если вы хотите, чтобы программа отображала в таблице все созданные задачи.
 - Прошедший час**, если вы хотите, чтобы программа отображала в таблице задачи, созданные за предыдущий час.
 - Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице задачи, созданные за предыдущий день.
 - Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице задачи, созданные за указанный вами период.
- Если вы выбрали период отображения задач **Пользовательский диапазон**, выполните следующие действия:
 - В открывшемся календаре укажите даты начала и конца периода отображения задач.
 - Нажмите на кнопку **Применить**.

Календарь закрывается.

Установленный вами фильтр поиска отобразится в таблице вместо заголовка графы **Время** в верхней части окна веб-интерфейса программы.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по типу

► Чтобы отфильтровать задачи по их типу, выполните следующие действия:

- В окне веб-интерфейса программы выберите раздел **Задачи**.
Откроется таблица задач.
- По ссылке **Тип** откройте меню фильтрации задач.
- Установите один или несколько флажков:
 - Получить файл.**
 - Завершить процесс.**
 - Удалить файл.**
 - Отправить файл в Карантин.**
 - Восстановить файл из Карантина.**
 - Выполнить программу.**
- Нажмите на кнопку **Применить**.

Установленный вами фильтр поиска отобразится в таблице вместо заголовка графы **Тип** в верхней части

окна веб-интерфейса программы.


В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач на основе имени и пути к файлу

Вы можете фильтровать задачи по показателю **Сведения** – имя и путь к файлу.

► Чтобы отфильтровать задачи на основе сведений о них, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.
Откроется таблица задач.
2. По ссылке **Сведения** откройте окно настройки 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 или пути к файлу.
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**.

Установленный вами фильтр поиска отобразится в таблице вместо заголовка графы **Сведения** в верхней части окна веб-интерфейса программы.


В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по описанию

► Чтобы отфильтровать задачи по их описанию, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.
Откроется таблица задач.
2. По ссылке **Описание** откройте окно настройки 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 описания задачи.
 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**.

Установленный вами фильтр поиска отобразится в таблице вместо заголовка графы **Описание** в верхней части окна веб-интерфейса программы.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по автору

► Чтобы отфильтровать задачи по их автору, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.
Откроется таблица задач.
2. По ссылке **Автор** откройте меню фильтрации задач.
3. Выберите один из следующих вариантов:
 - **Любой**, если вы хотите просмотреть задачи, созданные всеми пользователями.
 - **Мои задачи**, если вы хотите просмотреть задачи, созданные вами.

Установленный вами фильтр поиска отобразится в таблице вместо заголовка графы **Автор** в верхней части окна веб-интерфейса программы.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по статусу

► Чтобы отфильтровать задачи по их статусу, выполните следующие действия:

1. В окне веб-интерфейса программы 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**.

Установленный вами фильтр поиска отобразится в таблице вместо заголовка графы **Состояние** в верхней части окна веб-интерфейса программы.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация результатов выполнения задачи по имени хоста

Если задача создана для нескольких хостов, вы можете отфильтровать результаты ее выполнения по имени хоста.

► *Чтобы отфильтровать результаты выполнения задачи по имени хоста, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.


Откроется таблица задач.

2. Выберите задачу, результаты которой вы хотите отфильтровать.

Откроется окно свойств задачи.

3. Выберите одну из следующих закладок:


- **Всех хостов.**
- **Завершено.**
- **В обработке.**
- **Ошибка.**
- **Файлы.**

4. По значку  откройте окно настройки фильтрации по хостам.

5. В раскрывающемся списке выберите один из следующих операторов фильтрации задач:

- **Содержит.**
- **Не содержит.**

6. В поле ввода укажите один или несколько символов имени хоста.

7. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку  под списком операторов фильтрации и повторите действия по вводу условий фильтрации.

8. Нажмите на кнопку **Применить**.

Установленный вами фильтр отобразится над списком хостов.

В списке хостов отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Работа с политиками

При работе в веб-интерфейсе программы пользователи **Старший сотрудник службы безопасности** могут управлять запретами запуска файлов на выбранных хостах с помощью политик. Например, вы можете запретить запуск программ, использование которых считаете небезопасным, на выбранном хосте с компонентом Endpoint Sensors. Программа идентифицирует файлы по их хешу с помощью алгоритмов хеширования MD5 и SHA256. Вы можете создавать, удалять и изменять запреты.

Пользователи **Сотрудник службы безопасности** могут только просматривать запреты.

Все изменения в политиках применяются на хостах после установки авторизованного соединения с выбранными хостами. Если соединение с хостами отсутствует, на хостах продолжают действовать старые политики. Также изменения в политиках не влияют на уже запущенные процессы.

Запрет запуска файла на компьютере с компонентом Endpoint Sensors не будет действовать, если попытка запуска будет совершена до запуска компонента Endpoint Sensors на локальном компьютере или после завершения работы компонента Endpoint Sensors.

В этом разделе

Просмотр таблицы запретов.....	246
Просмотр информации о запрете	247
Создание запрета	248
Включение и отключение запрета	248
Удаление запрета	249
Фильтрация запретов по имени.....	249
Фильтрация запретов по хешу файла.....	249

Просмотр таблицы запретов

Таблица запретов находится в разделе **Политики** окна веб-интерфейса программы.

В таблице запретов содержится следующая информация:

1. **Имя** – имя запрета.
2. **Хосты** – количество хостов, на которые распространяется запрет.
3. **Автор** – имя пользователя, создавшего запрет.
4. **Состояние** – текущее состояние запрета.

Запрет может находиться в одном из следующих состояний:

- **Включено.**
- **Отключено.**

5. **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 выбрать одно из следующих действий:

- **Найти на [virustotal.com](https://www.virustotal.com) или Найти на [Kaspersky Threat Intelligence Portal](https://kasperskythreatintelligenceportal.com).**
- **Скопировать значение в буфер.**
- **Найти SHA256 в базе Событий или Найти MD5 в базе Событий.**

В результате выполнения этого действия откроется раздел **Поиск угроз** с событиями, уже отфильтрованными по выбранному вами хешу.

- **Включить запрет.**
- **Удалить запрет.**

Просмотр информации о запрете

► *Чтобы просмотреть информацию о запрете, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Политики**.
Откроется таблица запретов.
2. Выберите запрет, информацию о котором вы хотите просмотреть.
Откроется окно с информацией о запрете.

Окно содержит следующую информацию:

- **MD5** или **SHA256** – хеш файла, запрещенного к запуску.
- **Состояние** – текущее состояние запрета.

Запрет может находиться в одном из следующих состояний:

- **Включено.**
- **Отключено.**

- **Автор** – имя пользователя, создавшего запрет.
- **Имя** – имя файла, запрещенного к запуску.
- **Время создания** – время создания запрета.
- **Запрет для** – список хостов, на которых действует запрет.

Если запрет действует на всех хостах, отображается надпись **Всех хостов**.

- **Найти историю запрета запуска файла в базе Событий.** По ссылке открывается раздел **Поиск угроз** с условием поиска, содержащим выбранный вами запрет.
- **Журнал изменений** – список изменений запрета: время изменения, имя пользователя, изменившего запрет, и действия над запретом.

Создание запрета

► Чтобы создать запрет, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Политики**.
Откроется таблица запретов.
2. Нажмите на кнопку **Добавить**.
Откроется окно добавления запрета.
3. Укажите следующие параметры:
 - a. **MD5/SHA256** – хеш файла, запуск которого вы хотите запретить.
 - b. **Имя** – имя запрета.
 - c. **Запрет для** – область применения запрета:
 - Если вы хотите запретить запуск файла на всех хостах, выберите вариант **Всех хостов**.
 - Если вы хотите запретить запуск файла на некоторых хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты.
4. Нажмите на кнопку **Сохранить**.
Будет создан запрет на запуск файла.

При попытке запуска запрещенного файла пользователю будет показано уведомление о том, что запуск файла заблокирован.

Включение и отключение запрета

► Чтобы включить или отключить запрет, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Политики**.
Откроется таблица запретов.
2. Нажмите на запрет, который вы хотите включить или отключить.
Откроется окно сведений о запрете.
3. Выполните одно из следующих действий:
 - Если вы хотите включить запрет, нажмите на кнопку **Включить**.
Выбранный вами запрет будет включен.
 - Если вы хотите отключить запрет, нажмите на кнопку **Отключить**.
Выбранный вами запрет будет отключен.


Удаление запрета

► Чтобы удалить запрет, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Политики**.
Откроется таблица запретов.
2. Нажмите на запрет, который вы хотите удалить.
Откроется окно сведений о запрете.
3. Нажмите на кнопку **Удалить**.
Запрет будет удален.

Фильтрация запретов по имени

► Чтобы отфильтровать запреты по их имени, выполните следующие действия:


1. В окне веб-интерфейса программы выберите раздел **Политики**.
Откроется таблица запретов.
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 запрета.
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 политик отобразятся только запреты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация запретов по хешу файла

► Чтобы отфильтровать запреты по хешу файла, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Политики**.
Откроется таблица запретов.
2. По ссылке **Хеш файла** 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 хеша файла.
 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 политик отобразятся только запреты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

ИОС-проверка событий

ИОС (*Indicator of Compromise*) или *индикатор компрометации* – это набор данных о вредоносном объекте или действии. Kaspersky Anti Targeted Attack Platform использует ИОС-файлы открытого стандарта описания индикаторов компрометации OpenIOC. ИОС-файлы содержат набор индикаторов, при совпадении с которыми программа считает событие обнаружением. Вероятность обнаружения может повыситься, если в результате проверки были найдены точные совпадения данных об объекте с несколькими ИОС-файлами.

При работе с данными, полученными в течение длительного времени, совпадение данных проверяемого объекта с индикаторами компрометации может не свидетельствовать о возможном обнаружении.

При работе в веб-интерфейсе программы пользователи **Старший сотрудник службы безопасности** могут управлять ИОС-файлами: добавлять, изменять и удалять ИОС-файлы, а также управлять параметрами проверки объектов. Пользователи **Старший сотрудник службы безопасности** или **Сотрудник службы безопасности** могут использовать ИОС-файлы для поиска признаков целевых атак, зараженных и возможно зараженных объектов в базе событий и обнаружений, а также для проверки локальных компьютеров с установленным компонентом Endpoint Sensors.

В этом разделе

Просмотр таблицы ИОС-файлов	251
Просмотр информации об ИОС-файле	252
Загрузка ИОС-файла	253
Скачивание ИОС-файла на локальный компьютер	254
Включение и отключение использования ИОС-файла при проверке событий	254
Изменение ИОС-файла	255
Удаление ИОС-файла	255
Настройка расписания ИОС-проверки	256
Поиск результатов ИОС-проверки в базе обнаружений	256
Поиск результатов ИОС-проверки в базе событий	257
Фильтрация и поиск ИОС-файлов по степени важности	257
Фильтрация и поиск ИОС-файлов по имени файла	258
Фильтрация и поиск ИОС-файлов по их состоянию	258
Индикаторы компрометации на компьютерах с компонентом Endpoint Sensors	258


Просмотр таблицы ИОС-файлов

Таблица ИОС-файлов содержит список ИОС-файлов, используемых для проверки событий и находится в разделе **ИОС-проверка** окна веб-интерфейса программы.




Таблица имеет следующие закладки:

- **База Событий.** Отображает IOC-файлы, используемые для проверки базы событий.
- **Endpoint Sensors.** Отображает IOC-файлы, используемые для проверки событий, произошедших на компьютерах с компонентом Endpoint Sensors.

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. **Имя IOC-файла** – имя IOC-файла.
 3. **Проверка** – использование IOC-файла при автоматической проверке событий.
Проверка событий с использованием этого IOC-файла может находиться в одном из следующих состояний:
 - **Включено.**
 - **Отключено.**

Просмотр информации об IOC-файле

► Чтобы просмотреть информацию об IOC-файле, выполните следующие действия:



1. В окне веб-интерфейса программы выберите раздел **IOC-проверка**.
Откроется таблица IOC-файлов.
2. Выберите одну из следующих закладок:
 - **База Событий.**
 - **Endpoint Sensors.**
3. Выберите IOC-файл, информацию о котором вы хотите просмотреть.
Откроется окно с информацией об IOC-файле.

Окно содержит следующую информацию:

- **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.
- **Автоматическая проверка** – использование IOC-файла при автоматической проверке событий.
Проверка событий с использованием этого IOC-файла может находиться в одном из следующих состояний:
 - **Включено.**
 - **Отключено.**
- **Последняя проверка** – время последней проверки с использованием этого IOC-файла.
- **Найти в базе Обнаружений.** По ссылке открывается раздел **Обнаружения** с условием фильтрации, содержащим выбранный вами IOC-файл.
- **Найти историю запрета запуска файла в базе Событий.** По ссылке открывается раздел **Поиск угроз** с условием поиска, содержащим выбранный вами IOC-файл.
- **Скачать**, если вы выбрали закладку **Endpoint Sensors**. По ссылке открывается окно скачивания IOC-файла.
- **Изменить запрос**, если вы выбрали закладку **База Событий**. По ссылке открывается конструктор запросов в разделе **Поиск угроз**.
- **XML**, если вы выбрали закладку **Endpoint Sensors**. Отображает содержимое IOC-файла в формате XML.
- **Запрос**, если вы выбрали закладку **База Событий**. Отображает исходный код запроса, по которому осуществляется проверка.

Загрузка IOC-файла

IOC-файлы со свойствами UserItem для доменных пользователей не поддерживаются.

► Чтобы загрузить IOC-файл, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **IOC-проверка**.
Откроется таблица IOC-файлов.
2. Выберите одну из следующих закладок:
 - **База Событий**, если вы хотите загрузить IOC-файл для проверки базы событий.
 - **Endpoint Sensors**, если вы хотите загрузить IOC-файл для проверки событий, произошедших на компьютерах с компонентом Endpoint Sensors.
3. Нажмите на кнопку **Загрузить**.
Откроется окно выбора файла на вашем локальном компьютере.
4. Выберите файл, который вы хотите загрузить.
5. Укажите следующие параметры:

- a. **Имя** – имя IOC-файла.
 - b. **Важность** – степень важности, которая будет присвоена обнаружению, произведенному с использованием этого IOC-файла:
 - **Низкая.**
 - **Средняя.**
 - **Высокая.**
 - c. **Автоматическая проверка** – использование IOC-файла при автоматической проверке событий:
 - **Включено.**
 - **Отключено.**
6. Нажмите на кнопку **Сохранить**.
- IOC-файл будет загружен в формате XML.

Скачивание IOC-файла на локальный компьютер

Вы можете скачать на локальный компьютер IOC-файл, ранее загруженный на компьютеры с компонентом Endpoint Sensors.

► *Чтобы скачать IOC-файл на локальный компьютер, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **IOC-проверка**.
Откроется таблица IOC-файлов.
2. Выберите закладку **Endpoint Sensors**.
3. Выберите IOC-файл, который вы хотите скачать.
Откроется окно с информацией об IOC-файле.
4. 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 ваш локальный компьютер.

Включение и отключение использования IOC-файла при проверке событий

Вы можете включить или отключить использование IOC-файла при проверке событий.

► *Чтобы включить или отключить использование IOC-файла при проверке событий, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **IOC-проверка**.
Откроется таблица IOC-файлов.
2. Выберите одну из следующих закладок:
 - **База Событий**, если вы хотите включить или отключить использование IOC-файла при проверке базы событий.

- **Endpoint Sensors**, если вы хотите включить или отключить использование IOC-файла на компьютерах с компонентом Endpoint Sensors.
3. Выберите IOC-файл, использование которого вы хотите включить или отключить.
 4. Выберите одно из следующих состояний использования IOC-файла при проверке событий:
 - **Включено**, если вы хотите использовать IOC-файл при проверке событий.
 - **Отключено**, если вы не хотите использовать IOC-файл при проверке событий.
 5. Нажмите на кнопку **Сохранить**.
- Использование IOC-файла при проверке событий будет включено или отключено.

Изменение IOC-файла

Вы можете изменить IOC-файл, использующийся для проверки базы событий.

► *Чтобы изменить IOC-файл, выполните следующие действия*

1. В окне веб-интерфейса программы выберите раздел **IOC-проверка**.
Откроется таблица IOC-файлов.
 2. Выберите закладку **База Событий**.
 3. Выберите IOC-файл, который вы хотите изменить.
 4. Нажмите на кнопку **Изменить запрос**.
Откроется новая закладка с разделом **Поиск угроз**.
 5. По ссылке с запросом откройте форму поиска событий.
 6. Внесите необходимые изменения.
 7. Нажмите на кнопку **Найти**.
- Результат вашего запроса отобразится в таблице событий.

Удаление IOC-файла

► *Чтобы удалить IOC-файл, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **IOC-проверка**.
Откроется таблица IOC-файлов.
2. Выберите одну из следующих закладок:
 - **База Событий**, если вы хотите удалить IOC-файл, использующийся для проверки событий.
 - **Endpoint Sensors**, если вы хотите удалить IOC-файл, использующийся для проверки на компьютерах с компонентом Endpoint Sensors.
3. Выберите IOC-файл, который вы хотите удалить.
Откроется окно с информацией об IOC-файле.
4. Нажмите на кнопку **Удалить**.

IOC-файл будет удален.

Настройка расписания IOC-проверки

Вы можете настроить расписание IOC-проверки для компьютеров, на которых установлен компонент Endpoint Sensors.

► *Чтобы настроить расписание IOC-проверки, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **IOC-проверка**.
Откроется таблица IOC-файлов.
2. Выберите закладку **Endpoint Sensors**.
3. Нажмите на кнопку **Расписание**.
4. В раскрывающихся списках **Время запуска** выберите время начала проверки.
5. В раскрывающемся списке **Ограничение по времени** выберите ограничение по времени выполнения проверки.

Если проверка не завершится за указанное время, некоторые события могут быть не найдены.

Новые параметры вступят в силу немедленно. Результаты проверки будут отображаться в списке обнаружений.

Поиск результатов IOC-проверки в базе обнаружений

► *Чтобы просмотреть список обнаружений, найденных с помощью IOC-файла, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **IOC-проверка**.
Откроется таблица IOC-файлов.
2. Выберите одну из следующих закладок:
 - **База Событий**, если вы хотите просмотреть список обнаружений, найденных с помощью IOC-файла, использующегося для проверки событий.
 - **Endpoint Sensors**, если вы хотите просмотреть список обнаружений, найденных с помощью IOC-файла, использующегося для проверки на компьютерах с компонентом Endpoint Sensors.

3. Выберите IOC-файл, для которого вы хотите просмотреть список обнаружений.

Откроется окно с информацией об IOC-файле.

4. По ссылке **Найти в базе Обнаружений** перейдите в базу обнаружений.

Откроется новая закладка с обнаружениями, найденными с помощью этого IOC-файла.


Поиск результатов ИОС-проверки в базе событий

► Чтобы просмотреть список событий, найденных с помощью ИОС-файла, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **ИОС-проверка**.
Откроется таблица ИОС-файлов.
2. Выберите одну из следующих закладок:
 - **База Событий**, если вы хотите просмотреть список событий, найденных с помощью ИОС-файла, используемого для проверки событий.
 - **Endpoint Sensors**, если вы хотите просмотреть список событий, найденных с помощью ИОС-файла, используемого для проверки на компьютерах с компонентом Endpoint Sensors.
3. Выберите ИОС-файл, для которого вы хотите просмотреть список событий.
Откроется окно с информацией об ИОС-файле.
4. По ссылке **Найти в базе Событий** перейдите в базу событий.
Откроется новая закладка с событиями, найденными с помощью этого ИОС-файла.

Фильтрация и поиск ИОС-файлов по степени важности

► Чтобы отфильтровать или найти ИОС-файлы по степени важности, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **ИОС-проверка**.
Откроется таблица ИОС-файлов.
2. По значку  откройте окно настройки фильтрации ИОС-файлов.
3. Выберите одну или несколько из следующих степеней важности:
 - **Низкая.**
 - **Средняя.**
 - **Высокая.**
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице ИОС-файлов отобразятся только ИОС-файлы, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск IOC-файлов по имени файла

► Чтобы отфильтровать или найти IOC-файлы по имени, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **IOC-проверка**.
Откроется таблица IOC-файлов.
2. По ссылке **Имя IOC-файла** откройте окно настройки фильтрации IOC-файлов.
3. Введите один или несколько символов имени IOC-файла.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице IOC-файлов отобразятся только IOC-файлы, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск IOC-файлов по их состоянию

► Чтобы отфильтровать или найти IOC-файлы по их состоянию, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **IOC-проверка**.
Откроется таблица IOC-файлов.
2. По ссылке **Проверка** откройте окно настройки фильтрации IOC-файлов.
3. Установите один или несколько флажков рядом со значениями состояний:
 - **Включено**.
 - **Отключено**.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице IOC-файлов отобразятся только IOC-файлы, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Индикаторы компрометации на компьютерах с компонентом Endpoint Sensors

Kaspersky Anti Targeted Attack Platform поддерживает индикаторы компрометации открытого стандарта OpenIOC, приведенные в таблице ниже.

Таблица 5. Поддерживаемые индикаторы компрометации

Индикатор компрометации OpenIOC	Ограничения в реализации (если имеются)
FileItem/FileName	Нет значения.
FileItem/Md5sum	Нет значения.
FileItem/FilePath	Не поддерживается раскрытие user-specific переменных окружения. Например, %APPDATA%, %UserName%.
FileItem/SizeInBytes	Нет значения.
RegistryItem/KeyPath	Нет значения.
RegistryItem/Path	Не поддерживаются сканирование user-specific ключей через HKEY_CURRENT_USER и HKEY_CLASSES_ROOT для неавторизованных пользователей.
RegistryItem/Value	Нет значения.
FileItem/PEInfo/PETimeStamp	Нет значения.
FileItem/FullPath	Не поддерживается раскрытие user-specific переменных окружения. Например, %APPDATA%, %UserName%.
PortItem/remotelP	Нет значения.
FileItem/PEInfo/DetectedAnomalies/string	Поддерживается только checksum_is_zero.
FileItem/FileExtension	Нет значения.
DnsEntryItem/RecordName	Нет значения.
ProcessItem/name	Нет значения.
RegistryItem/ValueName	Нет значения.
RegistryItem/Text	Нет значения.
ServiceItem/name	Нет значения.
FileItem/PEInfo/Exports/ExportedFunctions/string	Нет значения.
FileItem/PEInfo/Exports/DllName	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/OriginalFilename	Нет значения.
FileItem/PEInfo/ImportedModules/Module/ImportedFunctions/string	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/FileDescription	Нет значения.
ProcessItem/arguments	Нет значения.
PortItem/remotePort	Нет значения.

Индикатор компрометации OpenIOC	Ограничения в реализации (если имеются)
DnsEntryItem/RecordData/IPv4Address	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/InternalName	Нет значения.
FileItem/PEInfo/Exports/NumberOfFunctions	Нет значения.
FileItem/PEInfo/DigitalSignature/SignatureExists	Нет значения.
ProcessItem/SectionList/MemorySection/Name	Нет значения.
FileItem/PEInfo/Type	Нет значения.
ProcessItem/path	Нет значения.
PortItem/localPort	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/CompanyName	Нет значения.
ProcessItem/SectionList/MemorySection/Md5sum	Нет значения.
DnsEntryItem/Host	Нет значения.
PortItem/protocol	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/ProductName	Нет значения.
ServiceItem/description	Нет значения.
FileItem/PEInfo/ResourceInfoList/ResourceInfoItem/Name	Нет значения.
FileItem/PEInfo/ResourceInfoList/ResourceInfoItem/Language	Нет значения.
ServiceItem/descriptiveName	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/Language	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/LegalCopyright	Нет значения.
FileItem/PEInfo/ImportedModules/Module/Name	Нет значения.
ServiceItem/serviceDLL	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/FileVersion	Нет значения.
FileItem/PEInfo/Sections/Section/Name	Нет значения.
FileItem/PEInfo/DigitalSignature/SignatureVerified	Нет значения.
ServiceItem/path	Нет значения.
FileItem/PEInfo/Subsystem	Нет значения.
FileItem/Sha256sum	Нет значения.
RegistryItem/Type	Нет значения.
FileItem/PEInfo/DigitalSignature/CertificateSubject	Нет значения.
EventLogItem/EID	Нет значения.
FileItem/PEInfo/ResourceInfoList/ResourceInfoItem/Type	Нет значения.
VolumItem/Name	Нет значения.

Индикатор компрометации OpenIOC	Ограничения в реализации (если имеются)
EventLogItem/source	Нет значения.
PortItem/state	Нет значения.
UserItem/Username	Сканируются только локальные пользователи. Сканирование доменных пользователей не поддерживается.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/ProductVersion	Нет значения.
DnsEntryItem/RecordType	Нет значения.
VolumeItem/VolumeName	Нет значения.
PortItem/localIP	Нет значения.
ProcessItem/parentpid	Нет значения.
FileItem/PEInfo/DigitalSignature/CertificateIssuer	Нет значения.
ProcessItem/SectionList/MemorySection/Protection	Нет значения.
ProcessItem/SectionList/MemorySection/Sha256sum	Нет значения.
FileItem/PEInfo/Exports/ExportsTimeStamp	Нет значения.
ProcessItem/Username	Нет значения.
ServiceItem/status	Нет значения.
ArpEntryItem/CacheType	Нет значения.
ArpEntryItem/IPv4Address	Нет значения.
ArpEntryItem/Interface	Нет значения.
ArpEntryItem/PhysicalAddress	Нет значения.
DnsEntryItem/DataLength	Нет значения.
DnsEntryItem/Flags	Нет значения.
DnsEntryItem/RecordData/Host	Нет значения.
DnsEntryItem/RecordName	Нет значения.
DnsEntryItem/TimeToLive	Нет значения.
VolumeItem/ActualAvailableAllocationUnits	Нет значения.
VolumeItem/BytesPerSector	Нет значения.
VolumeItem/CreationTime	Нет значения.
VolumeItem/DevicePath	Нет значения.
VolumeItem/DriveLetter	Нет значения.
VolumeItem/FileSystemFlags	Нет значения.
VolumeItem/FileSystemName	Нет значения.

Индикатор компрометации OpenIOC	Ограничения в реализации (если имеются)
Volumeltem/IsMounted	Нет значения.
Volumeltem/SectorsPerAllocationUnit	Нет значения.
Volumeltem/SerialNumber	Нет значения.
Volumeltem/TotalAllocationUnits	Нет значения.
Volumeltem/Type	Нет значения.
UserItem/LastLogin	Нет значения.
UserItem/SecurityID	Нет значения.
UserItem/SecurityType	Нет значения.
UserItem/description	Нет значения.
UserItem/disabled	Нет значения.
UserItem/fullname	Нет значения.
UserItem/homedirectory	Нет значения.
UserItem/lockedout	Нет значения.
UserItem/passwordrequired	Нет значения.
UserItem/scriptpath	Нет значения.
UserItem/userpasswordage	Нет значения.
PortItem/CreationTime	Нет значения.
PortItem/path	Нет значения.
PortItem/pid	Нет значения.
PortItem/process	Нет значения.
EventLogItem/log	Нет значения.
EventLogItem/index	Нет значения.
EventLogItem/user	Нет значения.
EventLogItem/genTime	Нет значения.
EventLogItem/machine	Нет значения.
EventLogItem/CorrelationActivityId	Нет значения.
EventLogItem/CorrelationRelatedActivityId	Нет значения.
EventLogItem/ExecutionProcessId	Нет значения.
EventLogItem/ExecutionThreadId	Нет значения.
RegistryItem/Hive	Не поддерживаются сканирование user-specific ключей через HKEY_CURRENT_USER и HKEY_CLASSES_ROOT для неавторизованных пользователей.

Индикатор компрометации OpenIOC	Ограничения в реализации (если имеются)
ServiceItem/pid	Нет значения.
ServiceItem/type	Нет значения.
ServiceItem/startedAs	Нет значения.
ServiceItem/arguments	Нет значения.
ServiceItem/mode	Нет значения.
ProcessItem/pid	Нет значения.
ProcessItem/startTime	Нет значения.
ProcessItem/SectionList/MemorySection/RegionSize	Нет значения.
ProcessItem/SectionList/MemorySection/RegionStart	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/Comments	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/LegalTrademarks	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/PrivateBuild	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/SpecialBuild	Нет значения.
FileItem/PEInfo/BaseAddress	Нет значения.
FileItem/PEInfo/Exports/NumberOfNames	Нет значения.
FileItem/PEInfo/ImportedModules/Module/NumberOfFunctions	Нет значения.
FileItem/PEInfo/ResourceInfoList/ResourceInfoItem/Size	Нет значения.
FileItem/PEInfo/Sections/ActualNumberOfSections	Нет значения.
FileItem/PEInfo/Sections/NumberOfSections	Нет значения.
FileItem/PEInfo/Sections/Section/SizeInBytes	Нет значения.

Работа с объектами в Хранилище

При работе в веб-интерфейсе программы пользователи **Старший сотрудник службы безопасности** могут поместить копии объектов, которые хотят проверить, в специальное Хранилище с помощью задачи **Получить файл**. Хранилище расположено на сервере с компонентом Central Node.

Пользователи **Сотрудник службы безопасности** могут работать только с файлами, полученными в результате выполнения задач, которые создали эти пользователи.

Если вы считаете объект опасным, вы можете поместить его в Карантин.

Карантин – это специальная область Хранилища, предназначенная для хранения файлов, которые могут нанести вред компьютерам или локальной сети организации. Вы можете переместить файлы с хоста в Карантин для проверки перед удалением или восстановлением в случае отсутствия угрозы.

При отправке объекта в Карантин выполняется его перемещение, а не копирование: объект удаляется с хоста и сохраняется в Карантине.

Вы можете управлять объектами в Хранилище: удалять, скачивать, отправлять на проверку, а также фильтровать списки объектов.

Kaspersky Anti Targeted Attack Platform отображает объекты в Хранилище в виде таблицы объектов.

По умолчанию максимальный объем Хранилища (помимо Карантина) составляет 10 ГБ. Как только объем Хранилища превышает заданное по умолчанию пороговое значение, программа начинает удалять из Хранилища самые старые копии объектов. Когда объем Хранилища снова становится меньше порогового значения, программа прекращает удалять копии объектов из Хранилища.

Максимальный объем Карантина составляет 10 ГБ. Если объем Карантина превысит заданное по умолчанию пороговое значение, вы не сможете помещать в него новые объекты, пока не удалите часть старых объектов. Информация о степени заполненности Карантина отображается на закладке **Хранилище** в верхней части окна веб-интерфейса программы.

Максимальный объем файла, который можно поместить в Карантин, составляет 100 МБ.

Реальный размер файла может быть больше видимого размера файла из-за метаданных, необходимых для восстановления файла из Карантина. При помещении в Карантин учитывается реальный размер файла. Зашифрованные файлы могут передаваться в расшифрованном виде (в зависимости от параметров шифрования), сжатые файлы передаются в исходном виде.

В этом разделе

Просмотр таблицы объектов, помещенных в Хранилище	265
Скачивание объектов из Хранилища	266
Проверка объектов из Хранилища	266
Удаление объектов из Хранилища.....	267
Фильтрация объектов в Хранилище по типу	267
Фильтрация объектов в Хранилище по описанию	268
Фильтрация объектов в Хранилище по результатам проверки.....	268
Фильтрация объектов в Хранилище по IP-адресу или имени хоста	269
Фильтрация объектов по времени помещения в Хранилище	269



Просмотр таблицы объектов, помещенных в Хранилище

Таблица объектов, помещенных в Хранилище, находится в разделе **Хранилище** окна веб-интерфейса программы.

В таблице объектов, помещенных в Хранилище, содержится следующая информация:

1. **Тип** – расположение объекта в Хранилище.

Объект может располагаться в Хранилище следующим образом:

-  – объект не помещен в Карантин;
-  – объект помещен в Карантин.

2. **Объект** – описание объекта. Например, путь к файлу.

По ссылке с описанием объекта раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр.**
- **Исключить из фильтра.**
- **Найти в базе Событий.**
- **Найти MD5 в базе Событий.**
- **Найти SHA256 в базе Событий.**
- **Найти эту директорию в базе Событий.**
- **Найти MD5 в базе Событий.**
- **Найти SHA256 в базе Событий.**
- **Запретить запуск этого файла.**
- **Скопировать значение в буфер.**

3. **Результаты проверки** – результат проверки объекта.

Результат проверки отображается в виде одного из следующих значений:

- **Не обнаружено** – в результате проверки технологии Anti-Malware Engine, YARA и компонент Sandbox не обнаружили признаков целевой атаки, возможно зараженных объектов или подозрительной активности.
 - **С ошибкой** – проверка объекта завершилась с ошибкой.
 - **Выполняется** – проверка объекта еще не завершилась.
 - **Не выполнялась** – объект не был отправлен на проверку.
 - **Обнаружено** – в результате проверки технологии Anti-Malware Engine, YARA и компонент Sandbox обнаружили признаки целевой атаки, возможно зараженный объект или подозрительную активность.
4. **Хост/IP** – IP-адрес или имя хоста, с которого получен объект.
- По ссылке с IP-адресом или именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:
- **Добавить в фильтр.**
 - **Исключить из фильтра.**
 - **Найти хост в базе Событий.**
 - **Скопировать значение в буфер.**
5. **Время** – дата и время помещения объекта в Хранилище.

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, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**.
Откроется таблица объектов.
2. Нажмите на объект, который вы хотите скачать.
Откроется окно сведений об объекте.
3. Нажмите на кнопку **Скачать**.
4. Укажите папку для сохранения объекта.
Объект будет сохранен на ваш локальный компьютер.

Проверка объектов из Хранилища

Вы можете проверить объекты, помещенные в Хранилище, компонентом Central Node с помощью технологий Anti-Malware Engine и YARA, а также компонентом Sandbox. Например, вы можете проверить объекты, если

проверка при помещении в Хранилище была отключена, или после обновления баз.

► *Чтобы отправить объект из Хранилища на проверку, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**.

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.

Удаление объектов из Хранилища

► *Чтобы удалить объект из Хранилища, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**.

Откроется таблица объектов.

2. Нажмите на объект, который вы хотите удалить.

Откроется окно сведений об объекте.

3. Нажмите на кнопку **Удалить**.

Объект будет удален из Хранилища.

Фильтрация объектов в Хранилище по типу

► *Чтобы отфильтровать объекты в Хранилище по их типу, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**.

Откроется таблица объектов.

2. По ссылке **Тип** откройте меню фильтрации объектов.

3. Установите один или несколько флажков:

- **Файл в Хранилище**, если вы хотите, чтобы программа отображала в таблице объекты, содержащиеся в Хранилище, но не помещенные в Карантин.
- **Файл в Карантине**, если вы хотите, чтобы программа отображала в таблице объекты, помещенные в Карантин.


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

► Чтобы отфильтровать объекты в Хранилище по описанию объекта, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**.
Откроется таблица объектов.
2. По ссылке **Объект** откройте меню фильтрации объектов.
3. В раскрываемся списке выберите один из следующих вариантов:
 - **Путь к файлу**, если вы хотите отфильтровать объекты по пути к объекту.
 - **MD5**, если вы хотите отфильтровать объекты по хешу MD5.
 - **SHA256**, если вы хотите отфильтровать объекты по хешу SHA256.
4. В раскрываемся списке выберите один из следующих операторов фильтрации объектов:
 - **Содержит**.
 - **Не содержит**.
5. В поле ввода укажите один или несколько символов описания объекта.
6. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку  под списком операторов фильтрации и повторите действия по вводу условий 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, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**.
Откроется таблица объектов.
2. По ссылке **Результаты проверки** откройте меню фильтрации объектов.
3. Установите один или несколько флажков:
 - **Не обнаружено**.
 - **С ошибкой**.
 - **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 IP-адресу или имени хоста

► Чтобы отфильтровать объекты в Хранилище по IP-адресу или имени хоста, с которого они были получены, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**.

Откроется таблица объектов.

2. По ссылке **Хост/IP** откройте меню фильтрации объектов.

3. В раскрываемом списке выберите один из вариантов:

- **Имя хоста.**
- **IP.**

4. В раскрываемом списке выберите один из следующих операторов фильтрации объектов:

- **Содержит.**
- **Не содержит.**

5. В поле ввода укажите один или несколько символов IP-адреса или имени хоста.

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, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**.

Откроется таблица объектов.

2. По ссылке **Время** откройте меню фильтрации объектов.

3. Выберите один из следующих периодов отображения объектов:
 - **Все**, если вы хотите, чтобы программа отображала в таблице все помещенные в Хранилище объекты.
 - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице объекты, помещенные в Хранилище за предыдущий час.
 - **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице объекты, помещенные в Хранилище за предыдущий день.
 - **Пользовательский диапазон**, если вы хотите, чтобы программа отображала 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**.Календарь закроется.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Управление компонентом Endpoint Sensors

Компонент Endpoint Sensors (на стр. [51](#)) устанавливается на отдельные компьютеры, входящие в IT-инфраструктуру организации и работающие под управлением операционной системы Microsoft Windows. Осуществляет постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами.

Вы можете оценить регулярность получения данных с компьютеров, на которых установлен компонент Endpoint Sensors, на закладке **Endpoint Sensors** окна веб-интерфейса программы и настроить отображение данных на этой странице.

Для оказания поддержки при неполадках в работе компонента Endpoint Sensors специалисты Службы технической поддержки могут попросить вас в отладочных целях выполнить следующие действия (в том числе в режиме Technical Support Mode (см. стр. [329](#))):

- Активировать функциональность получения расширенной диагностической информации.
- Изменить параметры отдельных компонентов программы.
- Изменить параметры хранения и отправки получаемой диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

Вся необходимая для выполнения перечисленных действий информация (описание последовательности шагов, изменяемые параметры, конфигурационные файлы, скрипты, дополнительные возможности командной строки, отладочные модули, специализированные утилиты и т.д.), а также состав собираемых в отладочных целях данных будут сообщены вам специалистами Службы технической поддержки. Собранные расширенная диагностическая информация сохраняется на компьютере пользователя. Автоматическая пересылка собранных 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 программы способами, не описанными в Руководстве администратора или в рекомендациях специалистов Службы технической поддержки, может привести к замедлению и сбоям в работе операционной системы, снижению уровня защиты компьютера, а также к нарушению доступности и целостности обрабатываемой информации.

В этом разделе

Просмотр таблицы компьютеров с компонентом Endpoint Sensors	272
Просмотр информации о хосте	275
Фильтрация и поиск компьютеров с компонентом Endpoint Sensors по имени хоста	276
Фильтрация и поиск компьютеров с компонентом Endpoint Sensors по IP-адресу.....	277
Фильтрация и поиск компьютеров с компонентом Endpoint Sensors по версии операционной системы...	278
Фильтрация и поиск компьютеров с компонентом Endpoint Sensors по версии Endpoint Sensor.....	279
Фильтрация и поиск компьютеров с компонентом Endpoint Sensors по их активности.....	279
Фильтрация и поиск компьютеров с компонентом Endpoint Sensors по имени сервера Central Node	280
Фильтрация и поиск компьютеров по типу установленного компонента Endpoint Sensors	281
Фильтрация и поиск компьютеров по состоянию компонента Endpoint Sensors	281
Фильтрация и поиск компьютеров с компонентом Endpoint Sensors по статусу хоста	282
Фильтрация и поиск компьютеров по наличию ошибок в работе компонента Endpoint Sensors	283
Быстрое создание фильтра компьютеров с компонентом Endpoint Sensors	283
Настройка показателей активности Endpoint Sensors	284

Просмотр таблицы компьютеров с компонентом Endpoint Sensors

Таблица компьютеров с компонентом Endpoint Sensors находится на закладке **Endpoint Sensors** окна веб-интерфейса программы.

Таблица компьютеров с компонентом Endpoint Sensors имеет следующие закладки:

- **Central Node** – данные о компьютерах с компонентом Endpoint Sensors.

На закладке **Central Node** отображается следующая информация:

- **Имя хоста** – имя хоста компьютера с компонентом Endpoint Sensors.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Завершить процесс.**
- **Удалить файл.**
- **Получить файл.**
- **Отправить файл в Карантин.**
- **Выполнить программу.**
- **Запретить запуск файла.**
- **Найти хост в базе Событий.**
- **Найти в базе Обнаружений.**
- **Добавить в фильтр.**

- **Исключить из фильтра.**
- **Скопировать значение в буфер.**
- **IP** – IP-адрес компьютера с компонентом Endpoint Sensors.
По ссылке с IP-адресом компьютера раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - **Перейти к обнаружениям, отфильтрованным по этому значению.**
 - **Добавить в фильтр.**
 - **Исключить из фильтра.**
 - **Скопировать значение в буфер.**
- **ОС** – версия операционной системы, установленной на компьютере с компонентом Endpoint Sensors.
По ссылке с названием версии операционной системы раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - **Добавить в фильтр.**
 - **Исключить из фильтра.**
 - **Скопировать значение в буфер.**
- **Версия** – версия компонента Endpoint Sensors, установленного на компьютере.
По ссылке с номером версии компонента Endpoint Sensors раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - **Добавить в фильтр.**
 - **Исключить из фильтра.**
 - **Скопировать значение в буфер.**
- **Активность** – время, прошедшее с последнего получения данных от компьютера с компонентом Endpoint Sensors.
- **KSC** – данные о компьютерах с агентом администрирования Kaspersky Security Center.
На закладке **KSC** отображается следующая информация:
 - **Имя хоста** – имя хоста компьютера с агентом администрирования Kaspersky Security Center.
По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - **Найти хост в базе Событий.**
 - **Найти в базе Обнаружений.**
 - **Добавить в фильтр.**
 - **Исключить из фильтра.**
 - **Скопировать значение в буфер.**
 - **IP** – IP-адрес компьютера с агентом администрирования Kaspersky Security Center.
По ссылке с IP-адресом компьютера раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Перейти к обнаружениям, отфильтрованным по этому значению.**
- **Добавить в фильтр.**
- **Исключить из фильтра.**
- **Скопировать значение в буфер.**
- **ОС** – версия операционной системы, установленной на компьютере с компонентом Endpoint Sensors.

По ссылке с названием версии операционной системы раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр.**
- **Исключить из фильтра.**
- **Скопировать значение в буфер.**
- **Endpoint Sensor** – тип компонента, используемого в качестве Endpoint Sensors.

Компонент может быть одного из следующих типов:

- **Отдельный.**
- **В составе KES.**
- **Версия** – версия компонента Endpoint Sensors, установленного на компьютере.

По ссылке с номером версии компонента Endpoint Sensors раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр.**
- **Скопировать значение в буфер.**
- **Сервер** – имя сервера с компонентом Central Node.

По ссылке с именем сервера раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр.**
- **Исключить из фильтра.**
- **Скопировать значение в буфер.**
- **Состояние сенсора** – статус компонента Endpoint Sensors, установленного на компьютере.

Компонент Endpoint Sensors может иметь один из следующих статусов:

- **Остановлен.**
- **Запущено.**
- **Сбой.**
- **Не установлен.**
- **Состояние хоста** – состояние хоста компьютера с компонентом Endpoint Sensors.

Хост может находиться в одном из следующих состояний:

- **Онлайн.**
- **Оффлайн.**

- **С ошибкой** – статус наличия ошибок в работе компонента Endpoint Sensors. Статус может принимать значение **Нет ошибок** или содержать информацию о типе ошибки работы компонента Endpoint Sensors.

Просмотр информации о хосте

► Чтобы просмотреть информацию о хосте, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.
2. Выберите одну из следующих закладок:
 - **Central Node**.
 - **KSC**.
3. Выберите хост, информацию о котором вы хотите просмотреть.

Откроется окно с информацией о хосте.

Окно содержит следующую информацию:

- **Состояние** – состояние хоста компьютера с компонентом Endpoint Sensors.
Хост может находиться в одном из следующих состояний:
 - **Онлайн**.
 - **Оффлайн**.
- **Имя хоста** – имя хоста компьютера с компонентом Endpoint Sensors.
По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - **Завершить процесс**.
 - **Удалить файл**.
 - **Получить файл**.
 - **Отправить файл в Карантин**.
 - **Выполнить программу**.
 - **Запретить запуск файла**.
 - **Найти хост в базе Событий**.
 - **Найти в базе Обнаружений**.
 - **Скопировать значение в буфер**.
- **IP** – IP-адрес компьютера с компонентом Endpoint Sensors.
- **ОС** – версия операционной системы, установленной на компьютере с компонентом Endpoint Sensors.
- **Защита** – состояние статуса защиты компьютера с компонентом Endpoint Sensors с помощью агента Kaspersky Endpoint Security.
- **Сервер** – имя сервера с компонентом Central Node.
- **Время подключения** – время последнего соединения с сервером с компонентом Central Node.


- **Версия** – тип и версия компонента Endpoint Sensors, установленного на компьютере.
- **Статус** – статус компонента Endpoint Sensors, установленного на компьютере.
- **Найти в базе Обнаружений.** По ссылке открывается раздел **Обнаружения** с условием фильтрации, содержащим выбранный вами хост.
- **Найти историю запрета запуска файла в базе Событий.** По ссылке открывается раздел **Поиск угроз** с условием поиска, содержащим выбранный вами хост.
- **Хеши файлов, запрещенных к запуску на этом компьютере.** По ссылке открывается таблица файлов со следующей информацией:
 - **Имя.**
 - **Состояние.**
 - **Хеш.**По ссылке с типом хеша раскрывается список, в котором вы можете выбрать одно из следующих действий:
 - **Найти на Kaspersky Threat Intelligence Portal.**
 - **Скопировать значение в буфер.**
 - **Найти в базе Событий.**
- **Задачи.** По ссылке открывается таблица задач, созданных для этого хоста. Таблица задач содержит следующую информацию:
 - **Время создания.**
 - **Тип задачи.**
 - **Сведения.**
 - **Состояние.**

Фильтрация и поиск компьютеров с компонентом Endpoint Sensors по имени хоста

► Чтобы отфильтровать или найти компьютеры с компонентом Endpoint Sensors по имени хоста, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.
2. Выберите одну из следующих закладок:
 - **Central Node.**
 - **KSC.**Откроется таблица компьютеров с компонентом Endpoint Sensors.
3. По ссылке **Имя хоста** откройте окно настройки фильтрации.
4. В раскрывающемся списке выберите один из следующих операторов фильтрации компьютеров с компонентом Endpoint Sensors:
 - **Содержит.**
 - **Не содержит.**

5. В поле ввода укажите один или несколько символов имени хоста компьютера.

6. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку  под списком операторов фильтрации и повторите действия по вводу условий фильтрации.

7. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закрывается.

Установленный вами фильтр поиска отобразится в таблице вместо заголовка графы **Имя хоста** в верхней части окна веб-интерфейса программы.

В таблице компьютеров с компонентом Endpoint Sensors отобразятся только компьютеры, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск компьютеров с компонентом Endpoint Sensors по IP-адресу

► Чтобы отфильтровать или найти компьютеры с компонентом Endpoint Sensors по IP-адресу, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.

2. Выберите одну из следующих закладок:

- **Central Node**.
- **KSC**.


Откроется таблица компьютеров с компонентом Endpoint Sensors.

3. По ссылке **IP** откройте окно настройки фильтрации.

4. В раскрывающемся списке выберите один из следующих операторов фильтрации компьютеров с компонентом Endpoint Sensors:

- **Содержит**.
- **Не содержит**.

5. 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).

6. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку  под списком операторов фильтрации и повторите действия по вводу условий фильтрации.

7. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закрывается.

Установленный вами фильтр поиска отобразится в таблице вместо заголовка графы **IP** в верхней части окна веб-интерфейса программы.

В таблице компьютеров с компонентом Endpoint Sensors отобразятся только компьютеры,

соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск компьютеров с компонентом Endpoint Sensors по версии операционной системы

► Чтобы отфильтровать или найти компьютеры с компонентом Endpoint Sensors по версии операционной системы, установленной на компьютере, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.

2. Выберите одну из следующих закладок:

- **Central Node**.
- **KSC**.


Откроется таблица компьютеров с компонентом Endpoint Sensors.

3. По ссылке **ОС** откройте окно настройки фильтрации.

4. В раскрывающемся списке выберите один из следующих операторов фильтрации компьютеров с компонентом Endpoint Sensors:

- **Содержит**.
- **Не содержит**.

5. В поле ввода укажите один или несколько символов версии операционной системы.

6. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку  под списком операторов фильтрации и повторите действия по вводу условий фильтрации.

7. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.


Установленный вами фильтр поиска отобразится в таблице вместо заголовка графы **ОС** в верхней части окна веб-интерфейса программы.

В таблице компьютеров с компонентом Endpoint Sensors отобразятся только компьютеры, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск компьютеров с компонентом Endpoint Sensors по версии Endpoint Sensor

► Чтобы отфильтровать или найти компьютеры с компонентом Endpoint Sensors по версии компонента Endpoint Sensors, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.
2. Выберите одну из следующих закладок:
 - **Central Node**.
 - **KSC**.Откроется таблица компьютеров с компонентом Endpoint Sensors.
3. По ссылке **Версия** откройте окно настройки фильтрации.
4. В раскрывающемся списке выберите один из следующих операторов фильтрации компьютеров с компонентом Endpoint Sensors:
 - **Содержит**.
 - **Не содержит**.
5. В поле ввода укажите один или несколько символов версии компонента Endpoint Sensors.
6. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку  под списком операторов фильтрации и повторите действия по вводу условий фильтрации.
7. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закрывается.

Установленный вами фильтр поиска отобразится в таблице вместо заголовка графы **Версия** в верхней части окна веб-интерфейса программы.

В таблице компьютеров с компонентом Endpoint Sensors отобразятся только компьютеры, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск компьютеров с компонентом Endpoint Sensors по их активности

► Чтобы отфильтровать или найти компьютеры с компонентом Endpoint Sensors по их активности, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.
2. Выберите закладку **Central Node**.

Откроется таблица компьютеров с компонентом Endpoint Sensors.

3. По ссылке **Активность** откройте окно настройки фильтрации.
4. Установите флажки рядом с одним или несколькими показателями активности компьютеров с компонентом Endpoint Sensor (см. раздел "Настройка показателей активности Endpoint Sensors" на стр. [284](#)):
 - **Нормальная**, если вы хотите найти компьютеры, от которых последние данные были получены недавно.
 - **Низкая**, если вы хотите найти компьютеры, от которых последние данные были получены давно.
 - **Очень низкая**, если вы хотите найти компьютеры, от которых последние данные были получены очень давно.
5. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

Установленный вами фильтр поиска отобразится в таблице вместо заголовка графы **Активность** в верхней части окна веб-интерфейса программы.

В таблице компьютеров с компонентом Endpoint Sensors отобразятся только компьютеры, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск компьютеров с компонентом Endpoint Sensors по имени сервера Central Node

- Чтобы отфильтровать или найти компьютеры с компонентом Endpoint Sensors по имени сервера Central Node, выполните следующие действия:
1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.
 2. Выберите закладку **KSC**.
Откроется таблица компьютеров с компонентом Endpoint Sensors.
 3. По ссылке **Сервер** откройте окно настройки фильтрации.
 4. В раскрывающемся списке выберите один из следующих операторов фильтрации компьютеров с компонентом Endpoint Sensors:
 - **Содержит**.
 - **Не содержит**.
 5. В поле ввода укажите один или несколько символов имени сервера Central Node.
 6. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку  под списком операторов фильтрации и повторите действия по вводу условий фильтрации.
 7. Нажмите на кнопку **Применить**.
- Окно настройки фильтрации закроется.

Установленный вами фильтр поиска отобразится в таблице вместо заголовка графы **Сервер** в верхней части окна веб-интерфейса программы.

В таблице компьютеров с компонентом Endpoint Sensors отобразятся только компьютеры, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск компьютеров по типу установленного компонента Endpoint Sensors

► Чтобы отфильтровать или найти компьютеры по типу установленного компонента Endpoint Sensors, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.

2. Выберите закладку **KSC**.

Откроется таблица компьютеров с компонентом Endpoint Sensors.

3. По ссылке **Endpoint Sensor** откройте окно настройки фильтрации.

4. Настройте фильтрацию событий:

- Если вы хотите, чтобы в таблице компьютеров с компонентом Endpoint Sensors отображались компьютеры с отдельно установленным компонентом Endpoint Sensors, установите флажок **Отдельный**.
- Если вы хотите, чтобы в таблице компьютеров с компонентом Endpoint Sensors отображались компьютеры с Endpoint Sensors в составе KES, установите флажок **В составе KES**.

5. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закрывается.

Установленный вами фильтр поиска отобразится в таблице вместо заголовка графы **Endpoint Sensor** в верхней части окна веб-интерфейса программы.

В таблице компьютеров с компонентом Endpoint Sensors отобразятся только компьютеры, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск компьютеров по состоянию компонента Endpoint Sensors

► Чтобы отфильтровать или найти компьютеры по состоянию компонента Endpoint Sensors,

выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.
2. Выберите закладку **KSC**.
Откроется таблица компьютеров с компонентом Endpoint Sensors.
3. По ссылке **Состояние сенсора** откройте окно настройки фильтрации.
4. Настройте фильтрацию компьютеров с компонентом Endpoint Sensors:
 - Если вы хотите, чтобы в таблице отображались компьютеры, на которых запущен компонент Endpoint Sensors, установите флажок **Запущено**.
 - Если вы хотите, чтобы в таблице отображались компьютеры, на которых остановлен компонент Endpoint Sensors, установите флажок **Остановлен**.
 - Если вы хотите, чтобы в таблице отображались компьютеры, на которых произошел сбой в работе компонента Endpoint Sensors, установите флажок **Сбой**.
 - Если вы хотите, чтобы в таблице отображались компьютеры, на которых не установлен компонент Endpoint Sensors, установите флажок **Не установлен**.
5. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

Установленный вами фильтр поиска отобразится в таблице вместо заголовка графы **Состояние сенсора** в верхней части окна веб-интерфейса программы.

В таблице компьютеров с компонентом Endpoint Sensors отобразятся только компьютеры, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск компьютеров с компонентом Endpoint Sensors по статусу хоста

► Чтобы отфильтровать или найти компьютеры с компонентом Endpoint Sensors по статусу хоста, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.
2. Выберите закладку **KSC**.
Откроется таблица компьютеров с компонентом Endpoint Sensors.
3. По ссылке **Состояние хоста** откройте окно настройки фильтрации.
4. В раскрывающемся списке выберите один из следующих вариантов:
 - **Все**.
 - **Оффлайн**.

- **Онлайн.**

Окно настройки фильтрации закрывается.

Установленный вами фильтр поиска отобразится в таблице вместо заголовка графы **Состояние хоста** в верхней части окна веб-интерфейса программы.

В таблице компьютеров с компонентом Endpoint Sensors отобразятся только компьютеры, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск компьютеров по наличию ошибок в работе компонента Endpoint Sensors

► Чтобы отфильтровать или найти компьютеры по наличию ошибок в работе компонента Endpoint Sensors, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.

2. Выберите закладку **KSC**.

Откроется таблица компьютеров с компонентом Endpoint Sensors.

3. По ссылке **С ошибкой** откройте окно настройки фильтрации.

4. В раскрываемом списке выберите один из следующих вариантов:

- Если вы хотите, чтобы в таблице компьютеров с компонентом Endpoint Sensors отображались все компьютеры, установите флажок **Все**.
- Если вы хотите, чтобы в таблице компьютеров с компонентом Endpoint Sensors отображались компьютеры, на которых компонент Endpoint Sensors работает с ошибками, установите флажок **С ошибкой**.

Окно настройки фильтрации закрывается.

Установленный вами фильтр поиска отобразится в таблице вместо заголовка графы **С ошибкой** в верхней части окна веб-интерфейса программы.

В таблице компьютеров с компонентом Endpoint Sensors отобразятся только компьютеры, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Быстрое создание фильтра компьютеров с компонентом Endpoint Sensors

► Чтобы быстро создать фильтр компьютеров с компонентом Endpoint Sensors, выполните

следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.
2. Выберите одну из следующих закладок:
 - **Central Node**.
 - **KSC**.

Откроется таблица компьютеров с компонентом Endpoint Sensors.
3. Выполните следующие действия по быстрому добавлению условий фильтрации в создаваемый фильтр:
 - a. Наведите курсор мыши на ссылку с тем значением графы 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.
4. Если вы хотите добавить несколько условий фильтрации в создаваемый фильтр, выполните действия по быстрому добавлению каждого из условий фильтрации в создаваемый фильтр.


Добавленные вами условия фильтрации отобразятся в заголовках граф, к которым они относятся.

В таблице компьютеров с компонентом Endpoint Sensors отобразятся только компьютеры, соответствующие заданным вами условиям.

Настройка показателей активности Endpoint Sensors

Пользователи **Администратор** и **Старший сотрудник службы безопасности** могут определить, какой период бездействия компьютеров с компонентом Endpoint Sensors считать нормальной, низкой и очень низкой активностью, а также настроить показатели активности компонентов Endpoint Sensors. Просматривать настройки показателей активности Endpoint Sensors могут все пользователи.

► *Чтобы настроить показатели активности компонентов Endpoint Sensors, выполните следующие действия:*

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Endpoint Sensors**.
2. В полях под названием раздела введите количество дней бездействия компьютеров с компонентом Endpoint Sensors, которое вы хотите отображать как **Предупреждение** и **Критическая**.
3. Нажмите на кнопку **Применить**.

Настроенные вами показатели активности компонентов Endpoint Sensors отобразятся в графе **Активность** таблицы компьютеров с компонентом Endpoint Sensors в разделе **Endpoint Sensors** окна веб-интерфейса программы.

Работа с отчетами

При работе в веб-интерфейсе программы пользователи **Старший сотрудник службы безопасности** могут управлять отчетами о работе системы: создавать, удалять и просматривать отчеты и шаблоны отчетов.

Отчет формируется на основе выборки обнаружений и содержит информацию о работе системы за указанный период.

Управление шаблонами отчетов и отчетами доступно во всех режимах работы программы в соответствии с лицензией.

В этом разделе

Просмотр таблицы шаблонов и отчетов.....	285
Создание отчета	286
Просмотр отчета	286
Удаление отчета	287
Фильтрация отчетов по времени создания	287
Фильтрация отчетов по имени шаблона.....	287
Фильтрация отчетов по имени пользователя, создавшего отчет	288
Создание шаблона отчетов	288
Изменение шаблона отчетов.....	289
Удаление шаблона отчетов	290
Фильтрация шаблонов по имени шаблона.....	290
Фильтрация шаблонов по имени пользователя, создавшего шаблон.....	291
Фильтрация шаблонов по времени создания	291

Просмотр таблицы шаблонов и отчетов

Таблица шаблонов и отчетов находится в разделе **Отчеты** окна веб-интерфейса программы.

Таблица шаблонов и отчетов имеет следующие закладки:

- **Созданные отчеты** – таблица отчетов.

На закладке **Созданные отчеты** отображается следующая информация:

- **Создано** – дата и время создания отчета.
- **Имя отчета** – имя шаблона, с помощью которого создан отчет.
- **Автор** – имя пользователя, создавшего отчет.
- **Период** – период, за который создан отчет.
- **Шаблоны** – таблица шаблонов отчетов.

На закладке **Шаблоны** отображается следующая информация:

- **Имя** – имя шаблона отчетов.

- **Автор** – имя пользователя, создавшего шаблон отчетов.
- **Создано** – дата и время создания шаблона отчетов.
- **Время изменения** – дата и время последнего изменения шаблона отчетов.

Создание отчета


► *Чтобы создать отчет, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, закладку **Созданные отчеты**.
Откроется таблица отчетов.
2. Нажмите на кнопку **Добавить**.
Откроется окно создания отчета.
3. Выполните следующие действия:
 - a. В раскрывающемся списке **Шаблон** выберите один из шаблонов.
 - b. В поле **Период** выберите один из следующих вариантов:
 - **Прошедший час**, если вы хотите, чтобы отчет содержал информацию о работе системы за предыдущий час.
 - **Прошедшие сутки**, если вы хотите, чтобы отчет содержал информацию о работе системы за предыдущий день.
 - **Прошедшие 7 дней**, если вы хотите, чтобы отчет содержал информацию о работе системы за предыдущую неделю.
 - **Прошедшие 30 дней**, если вы хотите, чтобы отчет содержал информацию о работе системы за предыдущий месяц.
 - **Пользовательский**, если вы хотите, чтобы отчет содержал информацию о работе системы за указанный вами период.
4. Если вы выбрали период отображения информации о работе системы **Пользовательский**, выполните следующие действия:
 - a. В открывшемся календаре укажите даты начала и конца периода, за который будет создан отчет.
 - b. Нажмите на кнопку **Применить**.

Отчет будет сохранен на сервере с компонентом Central Node в формате HTML.

Просмотр отчета

► *Чтобы просмотреть отчет о работе системы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, закладку **Созданные отчеты**.
Откроется таблица отчетов.
2. В строке с отчетом, который вы хотите просмотреть, нажмите на значок  и укажите, куда сохранить отчет.

Отчет будет сохранен в формате HTML на ваш локальный компьютер в указанную вами папку.

3. Откройте отчет с помощью любой программы для просмотра HTML-файлов (например, с помощью браузера).

Удаление отчета

► Чтобы удалить отчет о работе системы, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, закладку **Созданные отчеты**.
Откроется таблица отчетов.
2. Установите флажок в строке с отчетом, который вы хотите удалить.
3. Нажмите на кнопку **Удалить**.
Выбранный отчет будет удален.

Фильтрация отчетов по времени создания

► Чтобы отфильтровать отчеты по времени их создания, выполните следующие действия:


1. В окне веб-интерфейса программы выберите раздел **Отчеты**, закладку **Созданные отчеты**.
Откроется таблица отчетов.
2. По ссылке **Создано** откройте меню фильтрации отчетов.
3. Выберите один из следующих периодов отображения отчетов:
 - **Все**, если вы хотите, чтобы программа отображала в таблице все созданные отчеты.
 - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице отчеты, созданные за предыдущий час.
 - **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице отчеты, созданные за предыдущий день.
 - **Пользовательский диапазон**, если вы хотите, чтобы программа отображала 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**.
Календарь закроется.

В таблице отчетов отобразятся только отчеты, соответствующие заданным вами условиям.

Фильтрация отчетов по имени шаблона


► Чтобы отфильтровать отчеты по имени шаблона, на основе которого они созданы, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, закладку **Созданные отчеты**.

- Откроется таблица отчетов.
- По ссылке **Имя отчета** откройте меню фильтрации отчетов.
 - В раскрывающемся списке выберите один из следующих операторов фильтрации отчетов:
 - Содержит.**
 - Не содержит.**
 - В поле ввода укажите один или несколько символов имени шаблона, на основе которого созданы отчеты.
 - Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку  под списком операторов фильтрации и повторите действия по вводу условий фильтрации.
 - 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, выполните следующие действия:

- В окне веб-интерфейса программы выберите раздел **Отчеты**, закладку **Созданные отчеты**.
Откроется таблица отчетов.
 - По ссылке **Автор** откройте меню фильтрации отчетов.
 - В раскрывающемся списке выберите один из следующих операторов фильтрации отчетов:
 - Содержит.**
 - Не содержит.**
 - Введите один или несколько символов имени пользователя.
 - 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.

Создание шаблона отчетов

- Чтобы создать шаблон отчетов о работе системы, выполните следующие действия:

- В окне веб-интерфейса программы выберите раздел **Отчеты**.
Откроется таблица отчетов.
- Выберите закладку **Шаблоны**.
Откроется таблица шаблонов отчетов.
- Нажмите на кнопку **Добавить**.

Откроется окно создания шаблона отчетов.

4. Укажите следующие параметры:

- **Имя шаблона** – имя нового шаблона отчетов.
- **Report title** – заголовок шаблона отчетов.
- **Report body** – тело шаблона отчетов.

Тело шаблона отчетов может содержать следующие элементы:

- Текст.

Вы можете форматировать текст с помощью кнопок в блоке **Text** в конструкторе шаблонов отчетов.

- Таблицы.

Вы можете формировать таблицу, добавляя или удаляя столбцы с данными об обнаружениях, а также фильтруя данные по статусу, технологии, выполнившей обнаружение, важности и принадлежности к группе VIP.

- Круговые диаграммы.

Вы можете выбрать тип данных об обнаружениях, на основе которых будет сформирована круговая диаграмма, указать ее имя и количество секторов.

- Изображения.

Вы можете загрузить изображение и выбрать его расположение на странице отчета.

Таблицы и круговые диаграммы строятся на основе информации об обнаружениях. Текст и изображения могут быть произвольными.

5. Нажмите на кнопку **Сохранить**.

Будет создан новый шаблон отчетов о работе системы.

Изменение шаблона отчетов

► Чтобы изменить шаблон отчетов о работе системы, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**.

Откроется таблица отчетов.

2. Выберите закладку **Шаблоны**.

Откроется таблица шаблонов отчетов.

3. Выберите шаблон, который вы хотите изменить.

Откроется окно изменения шаблона отчетов.

4. Вы можете изменить следующие параметры:

- **Имя отчета** – имя шаблона отчетов.
- **Report title** – заголовок шаблона отчетов.
- **Report body** – тело шаблона отчетов.

5. Выберите один из следующих способов сохранения шаблона:

- Если вы хотите применить изменения к текущему шаблону, нажмите на кнопку **Сохранить**. Шаблон отчетов будет изменен.
- Если вы хотите создать новый шаблон, нажмите на кнопку **Сохранить как**.

Имя нового шаблона не должно совпадать с именем уже существующего шаблона.

Новый шаблон отчетов будет сохранен.

Удаление шаблона отчетов


► Чтобы удалить шаблон отчетов о работе системы, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**.
Откроется таблица отчетов.
2. Выберите закладку **Шаблоны**.
Откроется таблица шаблонов отчетов.
3. Установите флажок в строке с шаблоном отчетов, который вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

Выбранный вами шаблон отчетов будет удален.

Фильтрация шаблонов по имени шаблона


► Чтобы отфильтровать шаблоны отчетов по имени шаблона, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**.
Откроется таблица отчетов.
2. Выберите закладку **Шаблоны**.
Откроется таблица шаблонов отчетов.
3. По ссылке **Имя** откройте меню фильтрации шаблонов отчетов.
4. В раскрывающемся списке выберите один из следующих операторов фильтрации шаблонов:
 - **Содержит**.
 - **Не содержит**.
5. Введите один или несколько символов имени шаблона.
6. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку  под списком операторов фильтрации и повторите действия по вводу условий фильтрации.
7. Нажмите на кнопку **Применить**.

В таблице шаблонов отчетов отобразятся только шаблоны, соответствующие заданным вами условиям.

Фильтрация шаблонов по имени пользователя, создавшего шаблон

► Чтобы отфильтровать шаблоны отчетов по имени пользователя, создавшего шаблон, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**.
Откроется таблица отчетов.
2. Выберите закладку **Шаблоны**.
Откроется таблица шаблонов отчетов.
3. По ссылке **Автор** откройте меню фильтрации шаблонов отчетов.
4. В раскрывающемся списке выберите один из следующих операторов фильтрации шаблонов:
 - **Содержит**.
 - **Не содержит**.
5. Введите один или несколько символов имени пользователя.
6. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку  под списком операторов фильтрации и повторите действия по вводу условий фильтрации.
7. Нажмите на кнопку **Применить**.

В таблице шаблонов отчетов отобразятся только шаблоны, соответствующие заданным вами условиям.

Фильтрация шаблонов по времени создания

► Чтобы отфильтровать шаблоны отчетов по времени создания, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**.
Откроется таблица отчетов.
2. Выберите закладку **Шаблоны**.
Откроется таблица шаблонов отчетов.
3. По ссылке **Создано** откройте меню фильтрации шаблонов отчетов.
4. Выберите один из следующих периодов отображения шаблонов:
 - **Все**, если вы хотите, чтобы программа отображала в таблице все созданные шаблоны.
 - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице шаблоны, созданные за предыдущий час.
 - **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице шаблоны, созданные за предыдущий день.
 - **Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице шаблоны, созданные за указанный вами период.
5. 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**.

Календарь закроется.

В таблице шаблонов отчетов отобразятся только шаблоны, соответствующие заданным вами условиям.

Обновление баз программы

Этот раздел содержит информацию об обновлении баз и о том, как просмотреть номера версий компонентов Kaspersky Anti Targeted Attack Platform.

В этом разделе

Об обновлении баз	293
Просмотр состояния обновления баз	294
Загрузка базы YARA-правил	294
Обновление базы YARA-правил.....	294
Удаление базы YARA-правил	295

Об обновлении баз

Базы программы (далее также "базы") представляют собой файлы с записями, на основании которых компоненты и модули программы 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 программы дата выпуска баз соответствует дате выпуска программы, поэтому базы нужно обновить сразу после установки программы.

Программа периодически автоматически проверяет наличие новых пакетов обновлений на серверах обновлений "Лаборатории Касперского" (с периодичностью один раз в 30 минут). По умолчанию, если базы компонентов программы по каким-либо причинам не обновляются в течение 24 часов, Kaspersky Anti Targeted Attack Platform отображает эту информацию в разделе **Мониторинг** окна веб-интерфейса программы.

В качестве баз модуля YARA используются файлы YARA-правил.

Вы можете создавать свои YARA-правила и добавлять файл YARA-правил в Kaspersky Anti Targeted Attack Platform через веб-интерфейс программы.

Подробнее о создании и обновлении YARA-правил версии 3.6.3 и выше см. в документации YARA-правил или на веб-сайте <http://yarrules.com/>.

При установке версии 3.0 все данные, накопленные в процессе работы предыдущих версий программы (например, события и сопутствующая информация), будут потеряны. Если вы хотите сохранить накопленные данные, перед установкой версии 3.0 обратитесь в Службу технической поддержки "Лаборатории Касперского" (https://support.kaspersky.ru/kata/about_kata).

Просмотр состояния обновления баз

► Чтобы просмотреть состояние обновления баз компонентов программы,


в окне веб-интерфейса программы выберите закладку **Мониторинг**, график **Статус компонентов**.

На графике в списке **Обновление баз** отображается следующая информация о состоянии обновления баз программы:

- Если базы модулей и компонентов программы в актуальном состоянии, рядом с именем сервера, на котором установлены модули и компоненты программы, отображается значок ✓.
- Если базы одного или нескольких компонентов программы не обновлялись в течение 24 часов, рядом с именем сервера, на котором установлены модули и компоненты программы, отображается значок ○.

Загрузка базы YARA-правил

► Чтобы загрузить базу YARA-правил, выполните следующие действия:


1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **YARA-правила**.
2. Нажмите на кнопку **Загрузить**.
Откроется окно выбора файлов.
3. Выберите файл YARA-правил, который вы хотите загрузить, и нажмите на кнопку **Открыть**.
Окно выбора файлов закроется.

В разделе **YARA-правила** отобразится следующая информация о загруженной базе YARA-правил:

- **Размер файла** – размер файла YARA-правил.
- **Время загрузки** – дата и время последней загрузки файла YARA-правил.

Обновление базы YARA-правил

► Чтобы обновить базу YARA-правил, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **YARA-правила**.
2. Нажмите на кнопку **Заменить**.
Откроется окно выбора файлов.
3. Выберите файл YARA-правил, которым вы хотите заменить текущий файл YARA-правил, и нажмите на кнопку **Открыть**.
Окно выбора файлов закроется.


Загруженный файл YARA-правил заменит предыдущий файл YARA-правил Kaspersky Anti Targeted Attack Platform.

В разделе **YARA-правила** отобразится следующая информация о загруженной базе YARA-правил:

- **Размер файла** – размер файла YARA-правил.
- **Время загрузки** – дата и время последней загрузки файла YARA-правил.

Удаление базы YARA-правил

► *Чтобы удалить базу YARA-правил, выполните следующие действия:*

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **YARA-правила**.
2. Нажмите на кнопку **Удалить**.
Откроется окно подтверждения удаления базы YARA-правил.
3. Нажмите на кнопку **Да**.
Окно подтверждения удаления базы YARA-правил закроется.
База YARA-правил будет удалена.

Устранение уязвимостей и установка критических обновлений системы Kaspersky Anti Targeted Attack Platform

"Лаборатория Касперского" может выпускать обновления программного обеспечения, 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 (<http://support.kaspersky.ru/general/certificates>) и рассылаются по адресам электронной почты, указанным при заказе программы, а также подписчикам рассылки (подписаться на рассылку можно по ссылке: <http://support.kaspersky.ru/subscribe>). Порядок получения критических обновлений изложен в формуляре.

Программу необходимо периодически (не реже одного раза в полгода) подвергать анализу уязвимостей: организация, осуществляющая эксплуатацию программы, должна проводить такой анализ с помощью открытых источников, содержащих базу уязвимостей, в том числе с веб-сайта "Лаборатории Касперского" (<http://www.bdu.fstec.ru>, <https://support.kaspersky.ru/vulnerability>).

Вы можете сообщать об обнаруженных недостатках безопасности или уязвимостях программы следующими способами:

Через веб-форму на веб-сайте Службы технической поддержки (<https://support.kaspersky.ru/vulnerability.aspx?el=12429>).

По адресу электронной почты vulnerability@kaspersky.com

На форуме "Лаборатории Касперского" (<http://forum.kaspersky.com>).

► Чтобы загрузить архив с пакетом обновления программы на сервер с компонентом Central Node, выполните следующие действия:

1. Войдите в консоль управления сервера с компонентом Central Node по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке программы.

Отобразится меню администратора программы.

3. В меню администратора программы выберите режим Technical Support Mode.

4. Нажмите на клавишу **ENTER**.

Отобразится окно подтверждения входа в режим Technical Support Mode.

5. Выберите **Yes** и нажмите на клавишу **ENTER**.

6. Выполните команду

```
scp <имя пакета обновления программы>.ktgz <имя пользователя с правами администратора сервера Central Node>@<IP-адрес сервера с компонентом Central Node>
```

Например, вы можете выполнить команду `apt-system-3.0.0-tr-patch-122.ktgz`


```
admin@10.10.10.1
```

Вы можете перейти к установке пакета обновления программы.

► *Чтобы установить пакет обновления программы, выполните следующие действия:*

1. Войдите в консоль управления сервера с компонентом Central Node по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке программы.

Отобразится меню администратора программы.

3. В меню администратора программы выберите пункт **System administration**.

4. Нажмите на клавишу **ENTER**.

Отобразится окно выбора действия.

5. Выберите **Install patch** и нажмите на клавишу **ENTER**.

Отобразится окно со списком пакетов обновления программы, доступных к установке.

6. Выберите пакет обновления программы, который вы хотите установить, и нажмите на клавишу **ENTER**.

Отобразится окно выбора действия.

7. Выберите действие **Validate and install <имя пакета обновления программы>.ktgz** и нажмите на клавишу **ENTER**.

Пакет обновления программы будет установлен. Потребуется перезагрузка сервера.

8. Выберите **Go back** и нажмите на клавишу **ENTER**.

Отобразится меню администратора программы.

9. В меню администратора программы выберите пункт **Reboot the machine** и нажмите на клавишу **ENTER**.

Сервер с компонентом Central Node перезагрузится.

Установка пакета обновления программы будет завершена.

Обновление программы с версий 1.0 и 1.0.1 до версии 3.0 не поддерживается. При установке Kaspersky Anti Targeted Attack Platform версии 3.0 на Kaspersky Anti Targeted Attack Platform версий 1.0 и 1.0.1 все данные (обнаружения и сопутствующая информация), накопленные в процессе работы версий программы 1.0 и 1.0.1, будут потеряны.

При необходимости сохранения информации, накопленной во время работы Kaspersky Anti Targeted Attack Platform версий 1.0 и 1.0.1 рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского" до установки Kaspersky Anti Targeted Attack Platform версии 3.0.

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 программы, обновлении программы, замене оборудования, на которое установлена программа 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 программы рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского" или переустановить Kaspersky Anti Targeted Attack Platform.

Работа с белым списком

Вы можете создавать, импортировать и экспортировать *белый список* – список данных, которые Kaspersky Anti Targeted Attack Platform будет считать безопасными и не будет отображать в таблице обнаружений (см. раздел "Таблица обнаружений" на стр. [181](#)). Вы можете включать следующие данные в белый список:


- **MD5.** Обнаружения файлов, MD5-хеш которых входит в белый список, не будут отображаться в таблице обнаружений.
- **Формат.** Обнаружения файлов, формат которых входит в белый список, не будут отображаться в таблице обнаружений.
- **Маска URL.** Обнаружения URL-адресов, маска которых входит в белый список, не будут отображаться в таблице обнаружений.
- **Email.** Обнаружения адресов электронной почты, входящих в белый список, не будут отображаться в таблице обнаружений.
- **Подсеть.** Обнаружения подсетей, входящих в белый список, не будут отображаться в таблице обнаружений.
- **User Agent.** Обнаружения информации о браузере User agent, входящие в белый список, не будут отображаться в таблице обнаружений.

В этом разделе

Добавление записи в белый список.....	299
Удаление записи из белого списка.....	300
Изменение записи в белом списке.....	300
Импорт белого списка.....	301
Экспорт белого списка.....	301
Фильтрация и поиск записей в белом списке по типу правила.....	301
Фильтрация и поиск записей в белом списке по значению правил.....	302

Добавление записи в белый список


► Чтобы добавить запись в белый список, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Белый список**.
2. В правом верхнем углу окна веб-интерфейса программы нажмите на кнопку **Добавить**.
Откроется окно добавления записи в белый список.
3. В раскрывающемся списке **Тип правила** выберите один из следующих критериев добавления записи в белый список:
 - **MD5**, если вы хотите добавить в белый список MD5-хеш файла.
 - **Формат**, если вы хотите добавить в белый список формат файла.
 - **Маска URL**, если вы хотите добавить в белый список маску URL-адреса.

- **Email**, если вы хотите добавить в белый список адрес электронной почты.
 - **Подсеть**, если вы хотите добавить в белый список адрес подсети.
 - **User Agent**, если вы хотите добавить в белый список информацию о браузере User agent.
4. Если в раскрывающемся списке **Тип правила** вы выбрали **MD5**, **Маска URL**, **Email**, **User Agent** или **Подсеть**, в поле **Значение** введите значение соответствующего критерия.
- Например, если в списке **Тип правила** вы выбрали **Email**, в поле **Значение** введите адрес электронной почты, который вы хотите добавить в белый список.
5. Если в раскрывающемся списке **Тип правила** вы выбрали **Формат**, в раскрывающемся списке **Значение** выберите формат файла, который вы хотите добавить.
- Например, вы можете выбрать формат **MSOfficeDoc**.
6. Нажмите на кнопку **Добавить**.
- Запись будет добавлена в белый список.


Удаление записи из белого списка

- *Чтобы удалить одну или несколько записей из белого списка, выполните следующие действия:*

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Белый список**.
 2. Установите флажок слева от каждой записи, которую вы хотите удалить из белого списка.
 3. Если вы хотите удалить все записи, установите флажок над списком.
 4. В правом верхнем углу окна веб-интерфейса программы нажмите на кнопку **Удалить**.
Отобразится подтверждение удаления записей из белого списка.
 5. Нажмите на кнопку **Да**.
- Выбранные записи будут удалены из белого списка.


Изменение записи в белом списке

- *Чтобы изменить запись в белом списке, выполните следующие действия:*

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Белый список**.
2. Выберите запись, которую вы хотите изменить.
Откроется окно изменения записи.
3. Внесите необходимые изменения в поля **Тип правила** и **Значение**.
4. Нажмите на кнопку **Сохранить**.
Запись будет изменена.

Импорт белого списка

► Чтобы импортировать белый список, выполните следующие действия:


1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Белый список**.
2. В правом верхнем углу окна веб-интерфейса программы нажмите на кнопку **Импортировать**.
Отобразится подтверждение импорта списка.

Импортированный белый список заменит текущий белый список.

3. Нажмите на кнопку **Да**.
Откроется окно выбора файлов.
4. Выберите файл формата JSON с белым списком, который вы хотите загрузить, и нажмите на кнопку **Открыть**.
Окно выбора файлов закроется.
Белый список будет импортирован.


Экспорт белого списка

► Чтобы экспортировать белый список, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Белый список**.
2. В правом верхнем углу окна веб-интерфейса программы нажмите на кнопку **Экспортировать**.
Белый список экспортируется в файл формата JSON.

Фильтрация и поиск записей в белом списке по типу правила

► Чтобы отфильтровать или найти записи в белом списке по типу правила, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Белый список**.
2. По ссылке **Тип правила** откройте окно настройки фильтрации.
3. Установите один или несколько флажков рядом с типами правил:
 - **MD5**.
 - **Формат**.
 - **Маска URL**.

- Email.
- Подсеть.
- User Agent.

4. Нажмите на кнопку **Применить**.


Окно настройки фильтрации закрывается.

В белом списке отобразятся только записи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск записей в белом списке по значению правил

► Чтобы отфильтровать или найти записи в белом списке по значению правил, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Белый список**.
2. По ссылке **Значение** откройте окно настройки фильтрации.
3. Введите один или несколько символов значения.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закрывается.

В белом списке отобразятся только записи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Работа со списком адресов группы VIP

Вы можете создавать, импортировать и экспортировать список адресов группы VIP. Обнаружения, связанные с этими адресами, Kaspersky Anti Targeted Attack Platform не будет отображать в таблице обнаружений. Вы можете включать в список адреса следующих типов:


- **IP.** Обнаружения, связанные с IP-адресом компьютера, входящим в список адресов группы VIP, не будут отображаться в таблице обнаружений.
- **Имя хоста.** Обнаружения, связанные именем хоста, входящим в список адресов группы VIP, не будут отображаться в таблице обнаружений.
- **Email.** Обнаружения, связанные с адресом электронной почты, входящим в список адресов группы VIP, не будут отображаться в таблице обнаружений.

В этом разделе

Добавление записи в список адресов группы VIP	303
Удаление записи из списка адресов группы VIP	304
Изменение записи в списке адресов группы VIP	304
Импорт списка адресов группы VIP	304
Экспорт списка адресов группы VIP	305
Фильтрация и поиск адресов группы VIP по типу правила	305
Фильтрация и поиск адресов группы VIP по значению правил	306
Фильтрация и поиск адресов группы VIP по описанию	306

Добавление записи в список адресов группы VIP

► Чтобы добавить запись в список адресов группы VIP, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Группа VIP**.
2. В правом верхнем углу окна веб-интерфейса программы нажмите на кнопку **Добавить**.
Откроется окно добавления записи в список адресов группы VIP.
3. В раскрывающемся списке **Тип правила** выберите один из следующих типов адресов:
 - **IP**, если вы хотите добавить в список IP-адрес компьютера.
 - **Имя хоста**, если вы хотите добавить в список имя хоста.
 - **Email**, если вы хотите добавить в список адрес электронной почты.
4. В поле **Значение** введите нужное значение.
Например, если в списке **Тип правила** вы выбрали **Email**, в поле **Значение** введите адрес


электронной почты, который вы хотите добавить в список адресов группы VIP.

5. В поле **Описание** введите дополнительную информацию, если необходимо.
6. Нажмите на кнопку **Добавить**.

Запись будет добавлена в список адресов группы VIP.

Удаление записи из списка адресов группы VIP


► Чтобы удалить запись из списка адресов группы VIP, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Группа VIP**.
2. Установите флажок слева от каждой записи, которую вы хотите удалить из списка адресов группы VIP.
3. Если вы хотите удалить все записи, установите флажок над списком.
4. В правом верхнем углу окна веб-интерфейса программы нажмите на кнопку **Удалить**.
Отобразится подтверждение удаления записей.
5. Нажмите на кнопку **Да**.

Выбранные записи будут удалены из списка адресов группы VIP.

Изменение записи в списке адресов группы VIP


► Чтобы изменить запись в списке адресов группы VIP, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Группа VIP**.
2. Выберите запись, которую вы хотите изменить.
Откроется окно изменения записи.
3. Внесите необходимые изменения в поля **IP**, **Имя хоста**, **Email**.
4. Нажмите на кнопку **Сохранить**.

Запись будет изменена.

Импорт списка адресов группы VIP

► Чтобы импортировать список адресов группы VIP, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Группа VIP**.
2. Нажмите на кнопку **Импортировать**.
Отобразится подтверждение импорта списка.

Импортированный список адресов группы VIP заменит текущий список адресов группы VIP.

3. Нажмите на кнопку **Да**.

Откроется окно выбора файлов.

4. Выберите файл формата JSON со списком адресов группы VIP, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

Окно выбора файлов закроется.

Список адресов группы VIP будет импортирован.

Экспорт списка адресов группы VIP

- Чтобы экспортировать список адресов группы VIP, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Группа VIP**.

2. В правом верхнем углу окна веб-интерфейса программы нажмите на кнопку **Экспортировать**.

Список адресов группы VIP экспортируется в файл формата JSON.

Фильтрация и поиск адресов группы VIP по типу правила

- Чтобы отфильтровать или найти адреса группы VIP по типу правила, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Группа VIP**.

2. По ссылке **Тип правила** откройте окно настройки фильтрации.

3. Установите один или несколько флажков рядом с типами правил:

- **IP**.
- **Имя хоста**.
- **Email**.

4. Нажмите на кнопку **Применить**.


Окно настройки фильтрации закроется.

В таблице адресов группы VIP отобразятся только адреса, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск адресов группы VIP по значению правил

► Чтобы отфильтровать или найти адреса группы VIP по значению правила, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Группа 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 закрывается.

В таблице адресов группы VIP отобразятся только адреса, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск адресов группы VIP по описанию

► Чтобы отфильтровать или найти адреса группы VIP по описанию, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Группа VIP**.
2. По ссылке **Описание** откройте окно настройки фильтрации.
3. Введите один или несколько символов описания.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закрывается.

В таблице адресов группы VIP отобразятся только адреса, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Отправка уведомлений об обнаружениях

Этот раздел содержит информацию о том, как настроить отправку уведомлений об обнаружениях на адреса электронной почты.

В этом разделе

Состав данных, передаваемых в уведомлениях об обнаруженных событиях	307
Создание правила для отправки уведомлений.....	310
Включение и отключение правила для отправки уведомлений	311
Изменение правила для отправки уведомлений	311
Удаление правила для отправки уведомлений	312
Фильтрация и поиск правил отправки уведомлений по степени важности	312
Фильтрация и поиск правил отправки уведомлений по теме уведомлений.....	313
Фильтрация и поиск правил отправки уведомлений по их состоянию	313

Состав данных, передаваемых в уведомлениях об обнаруженных событиях

Уведомления об обнаруженных событиях могут содержать персональные данные. Рекомендуется настраивать отправку уведомлений на доверенные адреса электронной почты.

В тексте уведомлений могут передаваться данные, указанные в таблице ниже.

Таблица 6. Данные, передаваемые в тексте уведомлений

Тип события	Передаваемые данные
-------------	---------------------

Тип события	Передаваемые данные
<p>Событие обнаружено в сетевом трафике и содержит файл.</p>	<ul style="list-style-type: none"> • Дата и время сетевого события. • IP-адрес и порт клиентского компьютера. • IP-адрес и порт сервера. • Имя хоста, на котором обнаружено событие. • Имя учетной записи пользователя хоста, на котором обнаружено событие. • Имя файла, в котором обнаружено событие. • Размер файла в байтах (если файл содержится в составном объекте, то указывается размер файла отдельно и общий размер всего составного объекта). • Формат составного объекта, в котором обнаружен файл. • MD5-хеш составного объекта и файла, который в нем обнаружен. • SHA2-хеш составного объекта. • Технология, с помощью которой обнаружено событие. • Имя виртуальной машины, на которой обнаружено событие (только для компонента Sandbox). • Список обнаруженных объектов. • Версия баз, с помощью которых проверен файл. • Название протокола прикладного уровня (HTTP(S) или FTP). • Метод HTTP-запроса (только для протокола HTTP(S)). • User Agent клиентского компьютера (только для протокола HTTP(S)). • URL обнаруженного объекта (только для протокола HTTP(S)). • Заголовок HTTP Referrer (только для протокола HTTP(S)).

Тип события	Передаваемые данные
<p>Событие обнаружено в почтовом трафике и содержит файл.</p>	<ul style="list-style-type: none"> • Дата и время, когда программа получила сообщение электронной почты. • Имя файла или составного объекта, в котором обнаружено событие. • Размер файла в байтах (если файл содержится в составном объекте, то указывается размер файла отдельно и общий размер всего составного объекта). • Формат составного объекта, в котором обнаружен файл. • MD5-хеш составного объекта и файла, обнаруженного в нем. • SHA2-хеш составного объекта. • Технология, с помощью которой обнаружено событие. • Имя виртуальной машины, на которой обнаружено событие (только для Sandbox). • Список обнаруженных объектов. • Версия баз, с помощью которых проверен файл. • ID сообщения электронной почты. • Адрес электронной почты отправителя. • Адреса электронной почты получателей. • Тема сообщения.
<p>Событие обнаружено технологией Intrusion Detection System.</p>	<ul style="list-style-type: none"> • Название протокола сетевого уровня (TCP или UDP). • IP-адрес и порт клиентского компьютера. • IP-адрес и порт сервера. • Название обнаруженного объекта по классификации "Лаборатории Касперского". • Название обнаруженного объекта по версии баз модуля Intrusion Detection System. • Номер правила IDS. • Версия баз модуля Intrusion Detection System.
<p>Событие обнаружено технологией URL Reputation в HTTP-трафике.</p>	<ul style="list-style-type: none"> • IP-адрес и порт клиентского компьютера. • IP-адрес и порт сервера. • Имя хоста, на котором обнаружено событие. • Имя учетной записи пользователя хоста, на котором обнаружено событие. • Список категорий, к которым принадлежит URL обнаруженного объекта. • Метод HTTP-запроса. • User Agent клиентского компьютера. • URL обнаруженного объекта. • Заголовок HTTP Referrer.

Тип события	Передаваемые данные
Событие обнаружено технологией URL Reputation в DNS-трафике.	<ul style="list-style-type: none"> • IP-адрес и порт клиентского компьютера. • IP-адрес и порт сервера. • Имя хоста, на котором обнаружено событие. • Имя учетной записи пользователя хоста, на котором обнаружено событие. • Список категорий, к которым принадлежат доменные имена. • Тип DNS-сообщения, в котором обнаружено событие (request или response). • Тип записи из DNS-запроса. • Имя хоста из DNS-запроса. • Список доменных имен DNS-запроса или DNS-ответа.
Событие обнаружено технологией Targeted Attack Analyzer.	<ul style="list-style-type: none"> • IP-адрес хоста, на котором обнаружено событие. • Имя хоста, на котором обнаружено событие. • Имя домена, в котором обнаружено событие. • MD5-хеш, путь и имя файла, в котором обнаружено событие. • Доменное имя учетной записи, под которой совершено событие.

Создание правила для отправки уведомлений

Вы можете настроить отправку уведомлений об обнаружениях в одном или нескольких правилах для отправки уведомлений.

► Чтобы создать правило для отправки уведомлений, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Отправка уведомлений**.
2. Нажмите на кнопку **Добавить**.
Откроется окно **Новое правило отправки уведомлений**.
3. В разделе **Параметры сообщения** в поле **Отправлять на адреса** введите один или несколько адресов электронной почты, на которые вы хотите настроить отправку уведомлений.
Вы можете ввести несколько адресов электронной почты через запятую.
4. В разделе **Параметры сообщения** в поле **Тема** введите тему сообщения с уведомлением.
5. Если вы хотите, чтобы программа подставляла важность обнаружения в тему сообщения, добавьте в поле **Тема** макрос `%importance%`.
6. В разделе **Условия обнаружений** в списке **Важность** 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.
7. В разделе **Условия обнаружений** 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.


8. В разделе **Условия обнаружений** 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.
9. В разделе **Условия обнаружений**, подразделе **Технологии** установите или снимите флажки рядом с названиями одной или нескольких технологий, если вы хотите настроить отправку уведомлений об обнаружениях, выполненных определенными технологиями.
10. Нажмите на кнопку **Добавить**.

Окно **Новое правило отправки уведомлений** закроется.

Правило для отправки уведомлений об обнаружениях будет добавлено в список правил.

Включение и отключение правила для отправки уведомлений

- *Чтобы включить или отключить правило для отправки уведомлений об обнаружениях, выполните следующие действия:*

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Отправка уведомлений**.
2. В списке правил для отправки уведомлений об обнаружениях выберите правило, которое вы хотите включить или отключить.
3. Нажмите на одну из следующих кнопок:
 - **Включить**, если вы хотите включить правило.
 - **Отключить**, если вы хотите отключить правило.


Отобразится подтверждение действия.

4. Нажмите на кнопку **Да**.

Состояние правила для отправки уведомлений об обнаружениях будет изменено.

Изменение правила для отправки уведомлений

- *Чтобы изменить правило для отправки уведомлений об обнаружениях, выполните следующие действия:*


1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Отправка уведомлений**.
2. В списке правил для отправки уведомлений об обнаружениях выберите правило, которое вы хотите изменить.
Откроется окно изменения правила.
3. Если вы хотите изменить адреса электронной почты, на которые будут приходить уведомления, измените один или несколько адресов электронной почты в разделе **Параметры сообщения** в поле **Отправлять на адреса**.

Вы можете ввести несколько адресов электронной почты через запятую.

4. Если вы хотите изменить тему сообщения с уведомлением, измените ее в разделе **Параметры сообщения** в поле **Тема**.
5. Если вы хотите, чтобы программа подставляла важность обнаружения в тему сообщения, добавьте в поле **Тема** макрос `%importance%`.
6. Если вы хотите изменить минимальное значение важности обнаружений для отправки уведомлений, выберите другое значение в разделе **Условия обнаружений** в списке **Важность**.
Например, вы можете настроить отставку уведомлений об обнаружениях только высокой степени важности или только средней и высокой степени важности.
7. Если вы хотите изменить IP-адрес или адрес подсети источника или назначения, с которым связаны обнаружения, измените IP-адрес и маску сети разделе **Условия обнаружений** в поле **Адрес источника или назначения**.
8. Если вы хотите изменить адрес отправителя или получателя сообщений электронной почты, с которым связаны обнаружения, измените адрес электронной почты в разделе **Условия обнаружений** в поле **Email**.
9. Если вы хотите изменить набор технологий, об обнаружениях которых будут приходить уведомления, установите или снимите флажки рядом с названиями одной или нескольких технологий в разделе **Условия обнаружений**, подразделе **Технологии**.
10. Нажмите на кнопку **Сохранить**.
Окно **Изменить уведомление** закроется.
Правило для отправки уведомлений об обнаружениях будет изменено.

Удаление правила для отправки уведомлений

- Чтобы удалить правило для отправки уведомлений об обнаружениях, выполните следующие действия:


1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Отправка уведомлений**.
2. Установите флажок слева от названия каждого правила, которое вы хотите удалить.
3. Если вы хотите удалить все правила, установите флажок над списком.
4. Нажмите на кнопку **Удалить**.
Отобразится подтверждение удаления записей из списка.
5. Нажмите на кнопку **Да**.
Выбранные правила будут удалены из списка правил для отправки уведомлений об обнаружениях.

Фильтрация и поиск правил отправки уведомлений по степени важности

- Чтобы отфильтровать или найти правила отправки уведомлений по степени важности, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся

списке выберите **Отправка уведомлений**.

2. По значку  откройте окно настройки фильтрации правил.
3. Выберите одну или несколько из следующих степеней важности:
 - **Низкая.**
 - **Средняя.**
 - **Высокая.**
4. Нажмите на кнопку **Применить**.


Окно настройки фильтрации закрывается.

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, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите **Отправка уведомлений**.
2. По ссылке **Тема** откройте окно настройки фильтрации.
3. Введите один или несколько символов темы уведомлений.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закрывается.

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, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся

списке выберите **Отправка уведомлений**.

2. По ссылке **Состояние** откройте окно настройки фильтрации.
3. Установите один или несколько флажков рядом со значениями состояний:
 - **Включено**.
 - **Отключено**.
4. 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.

Настройка интеграции с SIEM-системой

Kaspersky Anti Targeted Attack Platform может публиковать обнаружения в *SIEM-систему*, которая уже используется в вашей организации, по протоколу Syslog.

SIEM-система – Система Security Information and Event Management. Решение для управления информацией и событиями в системе безопасности организации.

Вы можете использовать эту возможность для интеграции Kaspersky Anti Targeted Attack Platform в SIEM-систему, которая уже используется в вашей организации.

Вы можете настроить передачу информации об обнаружениях в SIEM-систему без использования TLS-шифрования или с использованием TLS-шифрования.


TLS-шифрование – Шифрование соединения между двумя серверами, обеспечивающее защищенную передачу данных между узлами сети Интернет.

В этом разделе

Включение и отключение записи событий в локальный журнал	315
Включение и отключение записи событий в удаленный журнал	316
Настройка основных параметров интеграции с SIEM-системой	316
Включение и отключение TLS-шифрования соединения с SIEM-системой	316
Загрузка TLS-сертификата	317
Содержание и свойства syslog-сообщений об обнаружениях	317


Включение и отключение записи событий в локальный журнал

► Чтобы включить или отключить запись событий в локальный журнал, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите раздел **Интеграции**, подраздел **SIEM-система**.
2. Выполните одно из следующих действий:
 - Включите переключатель рядом с названием параметра **Локальный журнал**, если вы хотите включить запись событий в локальный журнал.
 - Выключите переключатель рядом с названием параметра **Локальный журнал**, если вы хотите отключить запись событий в локальный журнал.
3. Нажмите на кнопку **Применить** в нижней части окна.


Включение и отключение записи событий в удаленный журнал

► Чтобы включить или отключить запись событий в удаленный журнал, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите раздел **Интеграции**, подраздел **SIEM-система**.
2. Выполните одно из следующих действий:
 - Включите переключатель рядом с названием параметра **Удаленный журнал**, если вы хотите включить запись событий в удаленный журнал.
 - Выключите переключатель рядом с названием параметра **Удаленный журнал**, если вы хотите отключить запись событий в удаленный журнал.
3. Нажмите на кнопку **Применить** в нижней части окна.


Настройка основных параметров интеграции с SIEM-системой

► Чтобы настроить основные параметры интеграции с SIEM-системой, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите раздел **Интеграции**, подраздел **SIEM-система**.
2. Включите переключатель рядом с названием параметра **Удаленный журнал**.
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 **Периодичность сигнала** введите интервал отправки сообщений в SIEM-систему о статусе компонентов Kaspersky Anti Targeted Attack Platform.
6. Нажмите на кнопку **Применить** в нижней части окна.

Включение и отключение TLS-шифрования соединения с SIEM-системой

► Чтобы включить или отключить TLS-шифрование соединения с SIEM-системой, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите раздел **Интеграции**, подраздел **SIEM-система**.
2. Включите переключатель рядом с названием параметра **Удаленный журнал**, если он выключен.
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. [317](#)).

4. Нажмите на кнопку **Применить** в нижней части окна.

Загрузка TLS-сертификата

- Чтобы загрузить TLS-сертификат для шифрования соединения с SIEM-системой, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите раздел **Интеграции**, подраздел **SIEM-система**.
2. Включите переключатель рядом с названием параметра **Удаленный журнал**, если он выключен.
3. В разделе **TLS-шифрование** 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 программу.
5. Нажмите на кнопку **Применить** в нижней части окна.

Содержание и свойства syslog-сообщений об обнаружениях

Информация о каждом обнаружении передается в отдельной syslog-категории (syslog facility), не используемой системой для передачи сообщений от других источников. Информация о каждом обнаружении передается как отдельное syslog-сообщение формата CEF. Информация о каждом обнаружении, выполненном модулем Targeted Attack Analyzer, 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 программы. Текущее значение поля: `Kaspersky Anti Targeted Attack Platform`.
- Версия программы. Текущее значение поля: `3.0`.
- Класс обнаружения. См. таблицу ниже.
- Наименование события. См. таблицу ниже.
- Важность обнаружения. Допустимые значения поля: `Low`, `Medium` или `High`.
- Дополнительная информация.

Содержание syslog-сообщений об обнаружении соответствует информации об этом обнаружении, отображающейся при просмотре обнаружения в веб-интерфейсе программы.

В зависимости от того, в сетевом или почтовом трафике произошло обнаружение, а также от технологии, которая выполнила обнаружение, в syslog-сообщении могут быть использованы разные сокращения. Эти сокращения, а также данные, содержащиеся в сообщении, приведены в таблице ниже.

Таблица 7. Информация об обнаружении в syslog-сообщениях

Класс обнаружения	Наименование и описание обнаружения	Передаваемые данные
file_web	<p>File from web detected</p> <p>В сетевом трафике обнаружен файл.</p>	<ul style="list-style-type: none"> • IP-адрес сервера Kaspersky Anti Targeted Attack Platform (dvc). • ID обнаружения (eventId). • Дата и время обнаружения. • IP-адрес и порт назначения. • IP-адрес и порт источника. • Имя хоста, на котором обнаружен файл . • Имя учетной записи пользователя хоста, на котором обнаружен файл. • Имя обнаруженного файла. • Размер файла в байтах (если файл содержится в составном объекте, то указывается размер файла отдельно и общий размер всего составного объекта). • Формат составного объекта, в котором обнаружен файл. • MD5-хеш составного объекта и файла, который в нем обнаружен. • SHA2-хеш составного объекта. • Путь к файлу внутри составного объекта. • Технология, с помощью которой обнаружен файл. • Имя виртуальной машины, на которой обнаружен файл (только для компонента Sandbox). • Список обнаруженных объектов. • Версия баз, с помощью которых проверен файл. • Название протокола прикладного уровня (HTTP(S) или FTP). • Метод HTTP-запроса (только для протокола HTTP(S)). • User Agent клиентского компьютера (только для протокола HTTP(S)). • URL обнаруженного объекта (только для протокола HTTP(S)). • Заголовок HTTP Referrer (только для протокола HTTP(S)).

Класс обнаружения	Наименование и описание обнаружения	Передаваемые данные
file_mail	<p>File from mail detected</p> <p>В почтовом трафике обнаружен файл</p>	<ul style="list-style-type: none"> • IP-адрес сервера Kaspersky Anti Targeted Attack Platform (dvc). • ID обнаружения (eventId). • Дата и время, когда программа получила сообщение электронной почты. • Имя обнаруженного файла или составного объекта. • Размер файла в байтах (если файл содержится в составном объекте, то указывается размер файла отдельно и общий размер всего составного объекта). • Формат составного объекта, в котором обнаружен файл. • MD5-хеш составного объекта и файла, обнаруженного в нем. • SHA2-хеш составного объекта. • Путь к файлу внутри составного объекта. • Технология, с помощью которой обнаружен файл. • Имя виртуальной машины, на которой обнаружен файл (только для компонента Sandbox). • Список обнаруженных объектов. • Версия баз, с помощью которых проверен файл. • ID сообщения электронной почты. • Адрес электронной почты отправителя. • Адреса электронной почты получателей. • Тема сообщения.
ids	<p>IDS event detected</p> <p>Обнаружение выполнено модулем Intrusion Detection System.</p>	<ul style="list-style-type: none"> • IP-адрес сервера Kaspersky Anti Targeted Attack Platform (dvc). • ID обнаружения (eventId). • Название протокола сетевого уровня (TCP или UDP). • IP-адрес и порт клиентского компьютера. • IP-адрес и порт сервера. • Название обнаруженного объекта по классификации "Лаборатории Касперского". • Название обнаруженного объекта по версии баз модуля Intrusion Detection System. • Номер правила IDS. • Версия баз модуля Intrusion Detection System.

Класс обнаружения	Наименование и описание обнаружения	Передаваемые данные
url_web	<p>URL from web detected</p> <p>Обнаружение выполнено технологией URL Reputation в сетевом трафике.</p>	<ul style="list-style-type: none"> • IP-адрес сервера Kaspersky Anti Targeted Attack Platform (dvc). • ID обнаружения (eventId). • IP-адрес и порт клиентского компьютера. • IP-адрес и порт сервера. • Имя хоста, на котором произошло обнаружение. • Имя учетной записи пользователя хоста, на котором произошло обнаружение. • Список категорий, к которым принадлежит URL обнаруженного объекта. • Метод HTTP-запроса. • User Agent клиентского компьютера. • URL обнаруженного объекта. • Заголовок HTTP Referrer. • Код HTTP-ответа.
url_mail	<p>URL from mail detected</p> <p>Обнаружение выполнено технологией URL Reputation в почтовом трафике.</p>	<ul style="list-style-type: none"> • IP-адрес сервера Kaspersky Anti Targeted Attack Platform (dvc). • ID обнаружения (eventId). • Дата и время, когда программа получила сообщение электронной почты. • ID сообщения электронной почты. • Адрес электронной почты отправителя. • Адреса электронной почты получателей. • Тема сообщения. • URL обнаруженного объекта. • Технология, с помощью которой выполнено обнаружение. • Имя виртуальной машины, на которой произошло обнаружение (только для компонента Sandbox). • Список обнаруженных объектов. • Версия баз, с помощью которых проверен файл (только для компонента Sandbox).

Класс обнаружения	Наименование и описание обнаружения	Передаваемые данные
dns	<p>DNS request detected</p> <p>Обнаружение выполнено технологией URL Reputation в DNS-трафике.</p>	<ul style="list-style-type: none"> • IP-адрес сервера Kaspersky Anti Targeted Attack Platform (dvc). • ID обнаружения (eventId). • IP-адрес и порт клиентского компьютера. • IP-адрес и порт сервера. • Имя хоста, на котором произошло обнаружение. • Имя учетной записи пользователя хоста, на котором произошло обнаружение. • Список категорий, к которым принадлежат доменные имена. • Тип DNS-сообщения, в котором произошло обнаружение (request или response). • Тип записи из DNS-запроса. • Имя хоста из DNS-запроса. • Список доменных имен DNS-запроса или DNS-ответа.
taa	<p>Обнаружение выполнено технологией Targeted Attack Analyzer.</p>	<ul style="list-style-type: none"> • IP-адрес сервера Kaspersky Anti Targeted Attack Platform (dvc). • ID обнаружения (eventId). • IP-адрес хоста, на котором произошло обнаружение. • Имя хоста, на котором произошло обнаружение. • Тип обнаруженного объекта. Комплексные события не передаются в syslog-сообщениях.

Класс обнаружения	Наименование и описание обнаружения	Передаваемые данные
file_endpoint	<p>File from endpoint detected</p> <p>Обнаружение выполнено компонентом Endpoint Sensors на компьютере пользователя и содержит файл.</p>	<ul style="list-style-type: none"> • IP-адрес сервера Kaspersky Anti Targeted Attack Platform (dvc). • ID обнаружения (eventId). • Дата и время получения файла компонентом Endpoint Sensors. • IP-адрес компьютера пользователя. • Полное доменное имя (FQDN) хоста, являющегося источником файла. • Путь к файлу или составному объекту, в котором обнаружен файл. • Размер файла в байтах (если файл содержится в составном объекте, то указывается размер файла отдельно и общий размер всего составного объекта). • Пустое поле вместо формата составного объекта, в котором обнаружен файл. • MD5-хеш составного объекта и файла, обнаруженного в нем. • SHA2-хеш составного объекта. • Технология, с помощью которой выполнено обнаружение. • Имя виртуальной машины, на которой обнаружен файл (только для компонента Sandbox). • Список обнаруженных объектов. • Версия баз, с помощью которых проверен файл.

Настройка интеграции с почтовым сенсором

Вы можете настроить интеграцию с почтовым сенсором – программой "Лаборатории Касперского" Kaspersky Secure Mail Gateway (далее также "KSMG"). KSMG отправляет сообщения электронной почты на обработку в Kaspersky Anti Targeted Attack Platform. По результатам обработки сообщений электронной почты в Kaspersky Anti Targeted Attack Platform KSMG может блокировать пересылку сообщений.

Предусмотрен следующий порядок интеграции Kaspersky Anti Targeted Attack Platform с почтовым сенсором:

1. Ввод параметров интеграции и создание запроса на интеграцию на стороне почтового сенсора. Подробнее о вводе параметров интеграции на стороне почтового сенсора см. *Руководство администратора Kaspersky Secure Mail Gateway* или онлайн-справку Kaspersky Secure Mail Gateway.
2. Подтверждение интеграции на стороне Kaspersky Anti Targeted Attack Platform.
3. Проверка соединения почтового сенсора с Kaspersky Anti Targeted Attack Platform.


В этом разделе

Обработка запроса на интеграцию от почтового сенсора	324
Удаление почтового сенсора из списка разрешенных к интеграции	325
Настройка приоритета обработки трафика от почтовых сенсоров	325

Обработка запроса на интеграцию от почтового сенсора

Вы можете принять или отклонить каждый запрос на интеграцию от почтового сенсора.

► *Чтобы принять или отклонить запрос на интеграцию от почтового сенсора, выполните следующие действия:*

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите раздел **Интеграции**, подраздел **Почтовый сенсор**.

В списке **Запрос на интеграцию** отобразятся запросы на интеграцию с Kaspersky Anti Targeted Attack Platform от почтовых сенсоров. В каждом запросе на интеграцию содержится следующая информация:

- **IP** – IP-адрес сервера почтового сенсора.
 - **IP сервера Central Node** – IP-адрес сервера Kaspersky Anti Targeted Attack Platform с компонентом Central Node, к которому пытается подключиться почтовый сенсор.
 - **Отпечаток сертификата** – отпечаток TLS-сертификата, с помощью которого устанавливается шифрованное соединение между серверами.
 - **Состояние** – состояние запроса на интеграцию.
2. Убедитесь, что отпечаток сертификата почтового сенсора соответствует отпечатку сертификата на стороне почтового сенсора. Например, если вы настраиваете интеграцию с программой Kaspersky


Secure Mail Gateway, вы можете сверить отпечаток сертификата в веб-интерфейсе Kaspersky Anti Targeted Attack Platform с отпечатком сертификата в веб-интерфейсе Kaspersky Secure Mail Gateway.

3. Нажмите на одну из следующих кнопок в строке с запросом на интеграцию от почтового сенсора:
 - **Принять**, если вы хотите принять запрос на интеграцию.
 - **Отклонить**, если вы хотите отклонить запрос на интеграцию.

Удаление почтового сенсора из списка разрешенных к интеграции

После того как вы приняли запрос на интеграцию от почтового сенсора, вы можете удалить почтовый сенсор из списка разрешенных к интеграции. В этом случае соединение между Kaspersky Anti Targeted Attack Platform и почтовым сенсором будет прервано.

► *Чтобы удалить почтовый сенсор из списка разрешенных к интеграции, выполните следующие действия:*

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите раздел **Интеграции**, подраздел **Почтовый сенсор**.

В списке **Запрос на интеграцию** отобразятся запросы на интеграцию с Kaspersky Anti Targeted Attack Platform от почтовых сенсоров.

2. Нажмите на кнопку **Удалить** в строке с запросом на интеграцию от того почтового сенсора, который вы хотите удалить.

Откроется окно подтверждения удаления почтового сенсора.

3. Нажмите на кнопку **Да**.


Окно подтверждения удаления почтового сенсора закроется.

Почтовый сенсор будет удален 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, выполните следующие действия:*

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите раздел **Интеграции**, подраздел **Почтовый сенсор**.

2. Выполните одно из следующих действий:

- Включите переключатель рядом с названием параметра **Обрабатывать трафик с максимальным приоритетом**, если вы хотите включить максимальный приоритет обработки трафика от почтовых сенсоров.

- Выключите переключатель рядом с названием параметра **Обрабатывать трафик с максимальным приоритетом**, если вы хотите отключить максимальный приоритет обработки трафика от почтовых сенсоров.
3. Нажмите на кнопку **Применить** в нижней части окна.

Настройка интеграции с Kaspersky Security Center

При работе в веб-интерфейсе программы пользователи **Администратор** или **Старший сотрудник службы безопасности** могут настроить интеграцию с программой Kaspersky Security Center SP3 и получать статистику работы компонента Endpoint Sensors.

Интеграция с программами Kaspersky Security Center 10 SP2 MR1 или Kaspersky Security Center 10 SP2 не поддерживается.

Для интеграции с программой Kaspersky Security Center SP3 вам необходимо создать в программе Kaspersky Security Center учетную запись пользователя.

► *Чтобы настроить необходимые права учетной записи пользователя, выполните следующие действия:*

1. Откройте консоль KSC.
2. Откройте окно свойств нужного Сервера администрирования.
3. В левой части окна свойств сервера выберите раздел с параметрами безопасности.
4. В правой части окна свойств сервера выберите учетную запись пользователя, права которого вы хотите настроить.
5. Предоставьте пользователю права на следующие действия:
 - a. Чтение и изменение – в узле общего функционала в папке базовой функциональности.
 - b. Чтение и выполнение – в узле общего функционала в папке операций с Сервером администрирования.
 - c. Чтение и создание туннелей – в узле управления системой в папке подключений.
6. Сохраните изменения.

Подробную информацию о работе в программе Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

В этом разделе

Включение и отключение интеграции с Kaspersky Security Center	328
Настройка параметров интеграции с Kaspersky Security Center	328

Включение и отключение интеграции с Kaspersky Security Center

► Чтобы включить или отключить интеграцию с Kaspersky Security Center, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите раздел **Интеграции**, подраздел **KSC**.
2. Выполните одно из следующих действий:
 - Включите переключатель рядом с названием параметра **Интеграция**, если вы хотите включить интеграцию с Kaspersky Security Center.
Интеграция с Kaspersky Security Center будет включена.
 - Выключите переключатель рядом с названием параметра **Интеграция**, если вы хотите отключить интеграцию с Kaspersky Security Center.
Интеграция с Kaspersky Security Center будет отключена.

Настройка параметров интеграции с Kaspersky Security Center

► Чтобы настроить параметры интеграции с Kaspersky Security Center, выполните следующие действия:

1. В нижней части окна веб-интерфейса программы нажмите на кнопку  и в раскрывающемся списке выберите раздел **Интеграции**, подраздел **KSC**.
2. Включите переключатель рядом с названием параметра **Интеграция**, если он выключен.
3. В поле **Хост/IP** введите IP-адрес Kaspersky Security Center.
4. В поле **Порт** введите порт подключения к Kaspersky Security Center.
5. В поле **Имя пользователя KSC** введите имя пользователя с правами администратора Kaspersky Security Center.
6. В поле **Пароль KSC** введите пароль доступа к Kaspersky Security Center.
7. Нажмите на кнопку **Применить** в нижней части окна.

Работа с программой в режиме Technical Support Mode

Вы можете работать с компонентами программы 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 программе и всем данным (в том числе персональным), которые в ней хранятся.

Режим Technical Support Mode позволяет управлять конфигурационными файлами программы. В частности, он позволяет отключить шифрование данных, передаваемых между серверами с компонентами программы, и 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 программы.

Не рекомендуется выполнять действия с Kaspersky Anti Targeted Attack Platform в режиме Technical Support Mode без консультации или указания сотрудников Службы технической поддержки.

► Чтобы начать работу с программой в режиме Technical Support Mode, выполните следующие действия:

1. Зайдите в консоль сервера, с которым вы хотите работать в режиме Technical Support Mode, по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя пользователя `admin` и пароль, заданный при развертывании программы.
Отобразится меню администратора программы.
3. В меню администратора программы выберите режим **Technical Support Mode**.
4. Нажмите на клавишу **ENTER**.
Отобразится окно подтверждения входа в режим Technical Support Mode.
5. Если вы действительно хотите выполнять действия с программой в режиме Technical Support Mode, выберите **Yes** и нажмите на клавишу **ENTER**.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

Способы получения технической поддержки	330
Техническая поддержка по телефону	330
Техническая поддержка через Kaspersky CompanyAccount	330

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе (см. раздел "Источники информации о программе" на стр. [16](#)), рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Перед обращением 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:

- позвонить в Службу технической поддержки по телефону (<https://support.kaspersky.ru/b2c>) ;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>).

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского" (<https://support.kaspersky.ru/b2c>).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>) – это портал для организаций, использующих программы "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).

Глоссарий

А

Advanced persistent threat (APT)

Сложная целевая атака на IT-инфраструктуру организации с одновременным использованием различных методов проникновения в сеть, закрепления в сети и получения регулярного доступа к конфиденциальным данным.

Anti-Malware Engine

Ядро программы. Выполняет проверку файлов и объектов на вирусы и другие программы, представляющие угрозу IT-инфраструктуре организации, с помощью антивирусных баз.

В

Backdoor-программа

Программа, которую злоумышленники устанавливают на взломанном компьютере для того, чтобы повторно получать доступ к этому компьютеру.

С

Central Node

Компонент программы. Выполняет проверку данных, исследование поведения объектов, а также публикацию результатов исследования в веб-интерфейс программы.

CSRF-атака

Cross-Site Request Forgery (также "XSRF-атака"). Атака на пользователей веб-сайтов, использующая уязвимости HTTP-протокола. Атака позволяет производить действия от имени авторизованного пользователя уязвимого веб-сайта. Например, от имени авторизованного пользователя уязвимого веб-сайта злоумышленник может тайно отправлять запрос на сервер сторонней платежной системы для перевода денег на счет злоумышленника.

Е

Endpoint Sensors

Компонент программы. Устанавливается на отдельные компьютеры, входящие в IT-инфраструктуру организации и работающие под управлением операционной системы Microsoft Windows. Осуществляет постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами.

I

ICAP-данные

Данные, полученные по протоколу ICAP (Internet Content Adaptation Protocol). Протокол позволяет фильтровать и изменять данные HTTP-запросов и HTTP-ответов. Например, производить антивирусную проверку данных, блокировать спам, запрещать доступ к персональным ресурсам. В качестве ICAP-клиента обычно выступает прокси-сервер, который взаимодействует с ICAP-сервером, используя протокол ICAP. Kaspersky Anti Targeted Attack Platform получает данные с прокси-сервера вашей организации после их обработки на ICAP-сервере.

Intrusion Detection System

Модуль программы. Выполняет проверку интернет-трафика на наличие признаков вторжения в IT-инфраструктуру организации.

ИОС

Indicator of Compromise (Индикатор компрометации). Набор данных о вредоносном объекте или действии.

ИОС-файл

Файлы, содержащие набор индикаторов ИОС, при совпадении с которыми Kaspersky Anti Targeted Attack Platform считает событие обнаружением.

Вероятность обнаружения может повыситься, если в результате проверки были найдены точные совпадения данных об объекте с несколькими ИОС-файлами.

Kaspersky Anti Targeted Attack Platform использует ИОС-файлы открытого стандарта описания индикаторов компрометации OpenIOC.

K

Kaspersky Anti Targeted Attack Platform

Решение, предназначенное для защиты IT-инфраструктуры организации и своевременного обнаружения таких угроз, как, например, *атаки "нулевого дня"*, *целевые атаки* и сложные целевые атаки *advanced persistent threats* (далее также "APT").

Kaspersky Private Security Network

Решение, позволяющее пользователям антивирусных программ "Лаборатории Касперского" получать доступ к данным Kaspersky Security Network, не отправляя информацию на серверы Kaspersky Security Network "Лаборатории Касперского" со своей стороны.

Kaspersky Secure Mail Gateway

Решение, предназначенное для защиты входящей и исходящей электронной почты от вредоносных объектов и спама, а также выполняющее контентную фильтрацию сообщений. Решение позволяет развернуть виртуальный почтовый шлюз и интегрировать его в существующую почтовую инфраструктуру организации. На виртуальном почтовом шлюзе предустановлена операционная система, почтовый сервер и антивирусная

программа "Лаборатории Касперского".

Kaspersky Security Network (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 программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

O

Open IOC

Открытый стандарт описания индикаторов компрометации (Indicator of Compromise, IOC), созданный на базе XML и содержащий свыше 500 различных индикаторов компрометации.

R

Risk Score Engine

Ядро программы. Выполняет эвристический анализ поведения исполняемых файлов формата APK в операционной системе Android.

S

Sandbox

Компонент программы. Запускает виртуальные образы операционных систем (32-разрядной Windows XP SP3, 32-разрядной Windows 7 и 64-разрядной Windows 7). 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.

Sensor

Компонент программы. Выполняет прием данных.

SIEM-система

Система Security Information and Event Management. Решение для управления информацией и событиями в системе безопасности организации.

SPAN

Switch Port Analyzer. Технология зеркалирования трафика с одного порта на другой.

T

Targeted Attack Analyzer

Модуль программы. Выполняет статистический анализ и проверку сетевой активности программного обеспечения, установленного на компьютеры локальной сети организации. 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.

TLS-шифрование

Шифрование соединения между двумя серверами, обеспечивающее защищенную передачу данных между узлами сети Интернет.

Y

YARA

Модуль программы. 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.

YARA-правила

Общедоступная классификация вредоносных программ, содержащая сигнатуры признаков целевых атак и вторжений в IT-инфраструктуру организации, по которым Kaspersky Anti Targeted Attack Platform производит проверку файлов и объектов.

A

Атака "нулевого дня"

Атака на IT-инфраструктуру организации, использующая уязвимости "нулевого дня" в программном обеспечении, которые становятся известны злоумышленникам до момента выпуска производителем программного обеспечения обновления, содержащего исправления.

B

Вредоносные веб-адреса

Веб-адреса ресурсов, распространяющих вредоносное программное обеспечение.

З

Зеркалированный трафик

Копия трафика, перенаправляемая с одного порта коммутатора на другой порт этого же коммутатора (локальное зеркалирование) или на удаленный коммутатор (удаленное зеркалирование). Администратор сети может настроить, какую часть трафика зеркалировать для передачи в Kaspersky Anti Targeted Attack

Platform.

Л

Лицензионное соглашение

Юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать программу.

С

Сигнатура

Код в базах систем защиты информации, содержащий описание известных угроз.

У

Угрозы нового поколения

Угрозы IT-инфраструктуре организации, способные перезаписывать, изменять, зашифровывать или искажать свои коды так, чтобы невозможно было обнаружить совпадение с сигнатурой в системе защиты информации.

Уязвимость "нулевого дня"

Уязвимость в программном обеспечении, обнаруженная злоумышленниками до момента выпуска производителем программного обеспечения обновления, содержащего исправленный код программы.

Ф

Фишинговые URL-адреса

URL-адреса ресурсов, занимающихся получением неправомерного доступа к конфиденциальным данным пользователей. Как правило, целью фишинга является кража различных финансовых данных.

Ц

Целевая атака

Атака, направленная на конкретного человека или организацию. В отличие от массовых атак компьютерными вирусами, направленных на заражение максимального количества компьютеров, целевые атаки могут быть направлены на заражение сети определенной организации или даже одного сервера в IT-инфраструктуре организации. Для каждой целевой атаки может быть написана специальная троянская программа.

АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку ведущих мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг "IDC Worldwide Endpoint Security Revenue by Vendor"). В России, по данным IDC, "Лаборатория Касперского" – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей ("IDC Endpoint Tracker 2014").

"Лаборатория Касперского" основана в России в 1997 году. Сегодня "Лаборатория Касперского" – это международная группа компаний с 38 офисами в 33 странах мира. В компании работает более 3000 квалифицированных специалистов.

Продукты. Продукты "Лаборатории Касперского" защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики "Лаборатории Касперского" работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами "Лаборатории Касперского".

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программного обеспечения, среди них: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, "Лаборатория Касперского" стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда "Лаборатории Касперского" – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

Сайт "Лаборатории Касперского":

<https://www.kaspersky.ru>

Вирусная энциклопедия:

<https://securelist.ru/>

Вирусная лаборатория:

<https://virusdesk.kaspersky.ru/> (для проверки
подозрительных файлов и сайтов)

Веб-форум "Лаборатории Касперского":

<https://forum.kaspersky.com>

Информация о стороннем коде

Информация о стороннем коде содержится в файле `legal_notices.txt`, расположенном в папке установки программы.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

AMD – товарный знак Advanced Micro Devices, Inc.

Adobe – товарный знак или зарегистрированный в Соединенных Штатах Америки и/или в других странах товарный знак Adobe Systems Incorporated.

Safari – товарный знак Apple Inc.

Android и Google Chrome – товарные знаки Google, Inc.

Intel и Pentium – 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.

McAfee – товарный знак или зарегистрированный в США и других странах товарный знак McAfee, Inc.

Mozilla и Firefox – товарные знаки Mozilla Foundation.

Active Directory, Microsoft, Windows и Windows Server – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

CentOS – товарный знак компании Red Hat, Inc.

Symantec – товарный знак или зарегистрированный в США и других странах товарный знак Symantec Corporation или аффилированных компаний.

Trend Micro – товарный знак компании Trend Micro.

VMware ESXi и VMware vSphere – товарные знаки VMware, Inc. или зарегистрированные в США или других юрисдикциях товарные знаки VMware, Inc.

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 8. Таблица соответствия терминов в документации и ФСТЭК

Термин в документации	Термин в требованиях ФСТЭК
Программа	Продукт, объект оценки, программное изделие
Вирус, программа, представляющая угрозу, вредоносная программа	КВ, компьютерный вирус
Администратор веб-интерфейса	Администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь

Приложение. Значения параметров программы в сертифицированной конфигурации

Этот раздел содержит перечень параметров программы, влияющих на сертифицированную конфигурацию программы. В таблице ниже приведены значения этих параметров в сертифицированной конфигурации программы.

Если вы меняете какие-либо из перечисленных значений параметров (диапазон значений) в сертифицированной конфигурации программы на другие значения, вы выводите программу из сертифицированной конфигурации.

Таблица 9. Параметры и их значения при работе программы в сертифицированной конфигурации

Раздел / подраздел, к которому относится параметр	Название параметра	Значение параметра в сертифицированной конфигурации
Параметры – Отправка уведомлений	Добавить (Добавить правило отправки уведомлений)	Администратор должен создать и включить правило отправки уведомлений о событиях обнаружения вторжений и нарушения безопасности.
Параметры – Отправка уведомлений	Отключить (Отключить правило отправки уведомлений)	Отключение правил отправки уведомлений может привести к выходу из сертифицированной конфигурации.
Параметры – Отправка уведомлений	Удалить (Отключить правило отправки уведомлений)	Удаление правил отправки уведомлений может привести к выходу из сертифицированной конфигурации.
Параметры – Endpoint Sensors	Предупреждение Количество дней бездействия Endpoint Sensors, при котором программа отображает предупреждение.	Установка значений, превышающих значение по умолчанию, может привести к выходу из сертифицированной конфигурации.
Параметры – Endpoint Sensors	Критическая (активность Endpoint Sensors) Количество дней бездействия Endpoint Sensors, которое программа отображает как критическое.	Установка значений, превышающих значение по умолчанию, может привести к выходу из сертифицированной конфигурации.

Раздел / подраздел, к которому относится параметр	Название параметра	Значение параметра в сертифицированной конфигурации
Параметры – YARA-правила	Удалить	Удаление файла YARA-правил может привести к выходу из сертифицированной конфигурации.

Предметный указатель

A

Anti-Malware Engine..... 50, 177, 179

C

Central Node..... 50

E

Endpoint Sensors..... 51, 122, 129, 138

I

Intrusion Detection System 49

IOC..... 231, 251

K

Kaspersky Anti Targeted Attack Platform 18

 о программе 18

Kaspersky Security Center 327

KPSN 147

KSN..... 144

R

Risk Score Engine 50

S

Sandbox..... 50

Sensor..... 49

T	
Targeted Attack Analyzer	50
Technical Support Mode	329
Threat hunting	206, 227
U	
URL Reputation	50
Y	
YARA	50, 179, 294
B	
Веб-интерфейс	
начало работы	141
З	
Задачи	233
Запреты	246
К	
Компоненты программы	49
Л	
Лицензирование программы	26, 27, 28, 29, 30
Лицензия	
Лицензионное соглашение	26
М	
Мониторинг	165

О

Обнаружения	181, 184, 193, 202
Обновление баз	293, 294
Отчеты	285

П

Поиск угроз	206, 227
Политики	246
Почтовый сенсор	324
Принцип работы программы	52

У

Установка	
компонента Central Node.....	80
компонента Endpoint Sensors	122
компонента Sandbox.....	59, 62
компонента Sensor	80
подготовка к установке.....	55
Учетные записи	60, 81, 149