kaspersky

Kaspersky Small Office Security

Содержание

Часто задаваемые вопросы

Предоставление данных

- Предоставление данных в рамках Лицензионного соглашения
- Предоставление данных в рамках Лицензионного соглашения на территории Европейского союза, Великобритании, Бразилии, Вьетнама, Индии, а также резидентами штата Калифорния
- Сохранение данных в отчет о работе приложения
- Предоставление данных в Kaspersky Security Network
- Локально обрабатываемые данные
- Сохранение данных для Службы технической поддержки
- Об использовании приложения на территории Европейского союза, Великобритании, Бразилии, Вьетнама, Индии, а также резидентами штата Калифорния

Что нового

Сравнение функций приложения в зависимости от типа операционной системы

Аппаратные и программные требования

Совместимость с другими приложениями "Лаборатории Касперского"

Как установить и удалить приложение

- Как установить приложение
- Как активировать приложение
- Расширение Kaspersky Protection для браузеров
- Как удалить приложение
- Как обновить приложение Kaspersky Small Office Security

Лицензирование приложения

- О Лицензионном соглашении
- О лицензии
- О подписке
- О коде активации
- Как восстановить коды активации
- Как купить или продлить лицензию
- Продление лицензии с помощью нового кода активации
- О режиме ограниченной функциональности

Удаленное управление защитой компьютера

- Об удаленном управлении защитой компьютеров
- Об аккаунте в Центре управления Kaspersky Small Office Security
- Подключение компьютера к Центру управления Kaspersky Small Office Security
- Как настроить проверку надежности пароля для удаленного доступа к файловому серверу

Основные возможности приложения

- Анализ состояния защиты компьютера и устранение проблем безопасности
- Как исправить проблемы безопасности компьютера
- История действий приложения и подробный отчет
- Как настроить интерфейс приложения
  - Как настроить уведомления приложения
  - Как сменить тему оформления приложения
  - Как настроить значок приложения
  - Как защитить доступ к управлению приложением с помощью пароля

- Как восстановить стандартные настройки приложения
- Как применить настройки приложения на другом компьютере
- Как приостановить и возобновить защиту компьютера
- Поиск по функциональности приложения

Безопасность

- Проверка компьютера
  - Как запустить полную проверку
  - Как запустить выборочную проверку
  - Как запустить быструю проверку
  - Как запустить проверку внешних дисков
  - Как запустить проверку файла или папки из контекстного меню
  - Как включить или выключить фоновую проверку
  - Как создать расписание проверки
  - Как выполнить поиск уязвимостей в приложениях, установленных на вашем компьютере
  - Как исключить файл, папку или тип угрозы из проверки
  - Проверка файлов в облачном хранилище OneDrive
- Обновление антивирусных баз и модулей приложения
  - Об обновлении антивирусных баз и модулей приложения
  - Как запустить обновление баз и модулей приложения
- Предотвращение вторжений
  - О Предотвращении вторжений
  - Как изменить настройки Предотвращения вторжений
  - Проверка репутации приложения
- Мониторинг сети
- Восстановление компьютера
  - О восстановлении операционной системы после заражения
  - Восстановление операционной системы с помощью мастера восстановления
  - Об аварийном восстановлении операционной системы
- Как восстановить удаленный или вылеченный файл
- Защита электронной почты
  - Настройка Почтового Антивируса
- Участие в Kaspersky Security Network
  - Как включить и выключить участие в Kaspersky Security Network
  - Как проверить подключение к Kaspersky Security Network
- Защита с помощью аппаратной виртуализации
  - О защите с помощью аппаратной виртуализации
  - Как включить защиту с помощью аппаратной виртуализации
- Защита с помощью Antimalware Scan Interface (AMSI)
  - О защите с помощью Antimalware Scan Interface
  - Как включить защиту с помощью Antimalware Scan Interface
  - Как исключить скрипт из проверки с помощью Antimalware Scan Interface

Производительность

- Обновление приложений
  - Об обновлении приложений
  - Как изменить настройки Обновления приложений
  - Поиск обновлений для приложений
  - Как настроить режим поиска обновлений

Просмотр списка обновлений для приложений
Удаление обновления или приложения из списка исключений
Резервное копирование данных
О резервном копировании данных
Как создать задачу резервного копирования
Шаг 1. Выбор файлов и папок для резервного копирования
Шаг 2. Выбор хранилища резервных копий
Шаг 3. Создание расписания резервного копирования
Шаг 4. Настройка хранилища резервных копий
Завершение работы мастера
Как запустить или возобновить задачу резервного копирования
Восстановление данных из резервной копии
Восстановление данных из FTP-хранилища
Восстановление данных из резервной копии с помощью Kaspersky Restore Utility
Об Облачном хранилище
Как активировать Облачное хранилище
Текущая активность
Режим "Не беспокоить"
Как сохранить ресурсы операционной системы
Экономия заряда батареи
Оптимизация нагрузки на операционную систему
Приватность
Безопасное VPN-соединение
О безопасном подключении к сетям Wi-Fi
Как включить безопасное VPN-соединение
Защита от сбора данных в интернете
О защите от сбора данных в интернете
Запрет на сбор данных
Разрешение на сбор данных на всех сайтах
Разрешение на сбор данных в виде исключения
Просмотр отчета о попытках сбора данных в интернете
Управление защитой от сбора данных в браузере
Менеджер паролей
Безопасные платежи
О защите финансовых операций и покупок в интернете
Как изменить настройки Безопасных платежей
Как настроить Безопасные платежи для определенного сайта
Как отправить отзыв о работе Безопасных платежей
Контроль камеры и микрофона
О доступе приложений к камере и микрофону
Как изменить настройки доступа приложений к камере или микрофону
Как разрешить или запретить доступ избранного приложения к камере
Как разрешить или запретить доступ избранного приложения к микрофону
Обнаружение сталкерских и других приложений
Анти-Баннер
Об Анти-Баннере
Как включить компонент Анти-Баннер

- Запрет баннеров
- Разрешение баннеров
- Как настроить фильтры Анти-Баннера
- Как управлять Анти-Баннером в браузере
- Блокировщик скрытых установок
- Удалять рекламные приложения
- Как изменить настройки Менеджера приложений
- Секретная папка
- О секретной папке
- Как поместить файлы в секретную папку
- Как получить доступ к файлам, хранящимся в секретной папке
- Уничтожитель файлов
- Удаление следов активности
- Защита персональных данных в интернете
- О защите персональных данных в интернете
- Об Экранной клавиатуре
- Как открыть Экранную клавиатуру
- Как настроить отображение значка Экранной клавиатуры
- О защите ввода данных с аппаратной клавиатуры
- Как изменить настройки защиты ввода данных с аппаратной клавиатуры
- Проверка безопасности сайта
- Как изменить настройки защищенных соединений
- Настройка уведомлений об уязвимостях сети Wi-Fi

Как удалить несовместимые приложения

Работа с приложением из командной строки

Обращение в Службу технической поддержки

- Способы получения технической поддержки
- Сбор информации для Службы технической поддержки
- О составе и хранении служебных файлов данных
- Как включить или отключить трассировку
- Как сделать запись экрана, если у вас возникла проблема с приложением

Ограничения и предупреждения

Другие источники информации о приложении

Сетевые параметры для взаимодействия с внешними службами

Информация о стороннем коде

Уведомления о товарных знаках

Часто задаваемые вопросы

Начало работы

- Как установить расширение Kaspersky Protection в браузерах
- Как удаленно управлять защитой компьютеров
- Как настроить уведомления Kaspersky Small Office Security

Безопасность

- Как запустить полную проверку компьютера
- Как запустить быструю проверку компьютера
- Как запустить обновление баз и модулей приложения
- Как восстановить удаленный или вылеченный файл
- Как восстановить операционную систему после заражения

Производительность

- Как завершить работу приложения, замедляющего компьютер
- Как сохранить ресурсы операционной системы
- Как включить Режим сосредоточенной работы
- Как обновить приложения, установленные на компьютере
- Как выполнить резервное копирование

Приватность

- Как защитить ваши покупки в интернете
- Как запретить сайтам собирать данные о вас
- Как проверить безопасность сайта

- Как защитить ваши пароли в интернете
- Как защитить вашу веб-камеру

Предоставление данных

Этот раздел содержит информацию о том, какие данные вы предоставляете в "Лабораторию Касперского". Подраздел Сохранение данных в отчет о работе приложения содержит данные, которые хранятся локально на вашем компьютере и не отправляются в "Лабораторию Касперского".

Предоставление данных в рамках Лицензионного соглашения

Информация о том, какие данные передаются в "Лабораторию Касперского", если у вас установлена версия приложения, не предназначенная для использования на территории Европейского союза, Великобритании, Бразилии, Вьетнама, Индии, а также резидентами штата Калифорния, содержится в Лицензионном соглашении (файл license.txt), расположенном в папке установки приложения.

Предоставление данных в рамках Лицензионного соглашения на территории Европейского союза, Великобритании, Бразилии, Вьетнама, Индии, а также резидентами штата Калифорния

Этот раздел содержит информацию о том, какие данные передаются в "Лабораторию Касперского", если у вас установлена версия приложения, предназначенная для использования на территории Европейского союза, Великобритании, Бразилии, Вьетнама, Индии, а также резидентами штата Калифорния.

Дополнительное положение (только для Индии)

Приложение Kaspersky Small Office Security соответствует положениям Закона о защите персональных данных (Digital Personal Data Protection, DPDP). Для этого приложение предложит вам принять Дополнительное положение об обработке данных (Дополнительное положение) во время установки.

Персональные и неперсональные данные, указанные в Дополнительном положении, идентичны данным, перечисленным для Лицензионного соглашения.

Информация, указанная в данном разделе, не содержит каких-либо персональных данных Пользователя.

Полученная информация защищается Правообладателем в соответствии с установленными законом требованиями и требуется для обеспечения работы лицензированного вами ПО.

"Лаборатория Касперского" может использовать полученные статистические данные, созданные на основе полученной информации, для мониторинга тенденций в области угроз компьютерной безопасности и публикации отчетов о них.

Сохранение данных в отчет о работе приложения

Файлы отчетов могут содержать персональные данные, полученные в результате работы компонентов защиты, таких как Файловый Антивирус, Почтовый Антивирус, Интернет защита и Веб-Контроль.

Файлы отчетов могут содержать следующие персональные данные:

- IP-адрес устройства пользователя;
- история посещения сайтов;
- заблокированные ссылки;
- версия браузера и операционной системы;
- имена и пути расположения файлов cookie и других файлов;
- адрес электронной почты, отправитель, тема письма, текст сообщений, имена пользователей, список контактов.

Файлы отчетов хранятся локально на вашем компьютере и не передаются в "Лабораторию Касперского". Путь к файлам отчетов: %allusersprofile%\Kaspersky Lab\AVP21.23\Report\Database.

Максимальное количество записей, которое может быть отображено в каждом разделе отчета — 10000.

Отчеты содержатся в следующих файлах:

- reports.db;
- reports.db-wal;
- reports.db-shm (не содержит персональных данных).

Файлы отчетов защищены от несанкционированного доступа, если в приложении Kaspersky Small Office Security включена самозащита. Если самозащита выключена, файлы отчетов не защищаются.

Предоставление данных в Kaspersky Security Network

Состав данных, передаваемых в Kaspersky Security Network, описан в Положении о Kaspersky Security Network.

Чтобы ознакомиться с Положением о Kaspersky Security Network:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части окна приложения.

   Откроется окно **Настройка**.

3. Выберите раздел **Настройки безопасности** → **Kaspersky Security Network**.

   В открывшемся окне **Kaspersky Security Network** отобразятся сведения о Kaspersky Security Network и настройки участия в Kaspersky Security Network.

4. По ссылке **Положении о Kaspersky Security Network** откройте текст Положения о Kaspersky Security Network.

Локально обрабатываемые данные

Данный раздел содержит информацию о локально собираемых и обрабатываемых данных. Эти данные используются для отправки статистики об ошибках работы продукта в целях улучшения его функциональности.

- идентификатор компонента ПО;
- версия компонента ПО;
- путь к исходному объекту;
- номер строки в тексте скрипта, где возникла ошибка;
- имя модуля, в котором предположительно произошел сбой;
- идентификатор модуля ПО;
- вложенная ошибка, возникшая при работе приложения;
- тип ошибки;
- текст сообщения об ошибке;
- стек памяти в процессе ПО в момент сбоя;
- адрес загрузки модуля ПО;
- идентификатор процесса в системе (PID);
- размер обрабатываемого объекта;
- описание обрабатываемого объекта, указанное в его свойствах;
- данные атрибута.

Сохранение данных для Службы технической поддержки

Приложение обрабатывает и хранит следующие персональные данные для анализа Службой технической поддержки:

- Данные, которые отображаются в интерфейсе приложения:
  - адрес электронной почты, используемый для подключения к Центру управления Kaspersky Small Office Security;
  - адреса сайтов, которые были добавлены в исключения (отображаются в компонентах Интернет защита, Анти-Баннер, Защита от сбора данных в интернете, Сеть, а также в окне Отчеты);
  - данные о лицензии.

  Эти данные хранятся локально в немодифицированном виде и доступны для просмотра под любой учетной записью на компьютере.
- Данные о системной памяти процессов Kaspersky Small Office Security на момент создания дампа памяти.
- Данные, собираемые при включении записи событий.

Эти данные хранятся локально в модифицированном виде и доступны для просмотра под любой учетной записью на компьютере. Эти данные передаются в "Лабораторию Касперского" только с вашего согласия при обращении в Службу технической поддержки. Ознакомиться с составом данных можно по ссылке **Положения о технической поддержке** в окне **Мониторинг проблем**.

Об использовании приложения на территории Европейского союза, Великобритании, Бразилии, Вьетнама, Индии, а также резидентами штата Калифорния

Версии приложения, которые "Лаборатория Касперского" и наши партнеры распространяют на территории Европейского союза, Великобритании, Бразилии, Вьетнама и Индии (а также версии приложения, предназначенные для использования резидентами штата Калифорния), отвечают требованиям регламентов, регулирующих сбор и обработку персональных данных в этих регионах.

Чтобы установить приложение, вы должны принять Лицензионное соглашение и условия Политики конфиденциальности.

Кроме этого, мастер установки и удаления предложит вам принять следующие положения об обработке ваших персональных данных:

- Положение о Kaspersky Security Network. Это положение позволяет специалистам "Лаборатории Касперского" своевременно получать информацию об угрозах, обнаруженных на вашем компьютере, о запускаемых приложениях и о скачиваемых подписанных приложениях, а также информацию об операционной системе для улучшения вашей защиты.

- Положение об обработке данных для маркетинговых целей. Это положение позволяет нам делать более выгодные предложения для вас.

Вы можете в любой момент принять или отказаться от Положения о Kaspersky Security Network, а также принять или отказаться от Положения об обработке данных для маркетинговых целей в окне **Настройка** → **Настройки безопасности** → **Kaspersky Security Network**.

Если вы отклоните Положение об обработке данных в маркетинговых целях, для окончательного отключения всех маркетинговых кампаний и уведомлений может потребоваться до 4 дней.

Что нового

В Kaspersky Small Office Security появились следующие новые возможности и улучшения:

В последней версии приложения появились следующие новые возможности и улучшения:

- Приложение было приведено в соответствие с законодательными требованиями Индии.
- Добавлена возможность отправки отчетов, собранных с помощью troubleshoot.exe, непосредственно через утилиту.
- Функция проверки электронной почты была удалена из области проверки, так как необходимую защиту обеспечивает другой компонент приложения.
- Если при загрузке установочных файлов не удаётся установить защищённое соединение, приложение предложит включить последнюю версию TLS в настройках операционной системы и повторить попытку.

Функциональность, удаленная в текущей и предыдущих версиях приложения

Kaspersky Small Office Security 8.18:

- Удалена функциональность Анти-Спам. Хотя эта функциональность была удалена, другие наши функции защищают ваш почтовый ящик от вредоносных вложений в электронной почте.

Kaspersky Small Office Security 8:

- Удалена функциональность Application Advisor.
- Удалена функциональность IM-Антивирус.
- Удалена функциональность Режим безопасных программ.
- Удалена функциональность поиска уязвимостей в операционной системе.
- Ограничена поддержка старого браузера Microsoft Edge. В этом браузере больше не поддерживается Защита ввода данных и Защищенный браузер. Защита при проверке трафика продолжает работать.
- Удалена поддержка расширения Kaspersky Protection в браузере Internet Explorer.
- Удалена возможность сохранения резервных копий на FTP-сервер.
    - Удалена функциональность Настройка браузера.

Kaspersky Small Office Security 6:

- В компоненте Менеджер программ удалена функциональность Контроль изменений настроек операционной системы.
- В компоненте Веб-контроль удалена функциональность Контроль общения в социальных сетях.
- В компоненте Анти-Спам удалены следующие функциональности:
    - Интеграция с Microsoft Office Outlook и Outlook Express.
    - Работа с пользовательской спам-базой.
    - Проверка писем, передаваемых по протоколу Exchange MAPI.
    - Добавление адреса отправителя в список разрешенных адресов при обучении Анти-Спама.
    - Выполнение действий при обнаружении спам-писем: переместить, копировать, удалить, пропустить.

Если вы хотите продолжать использовать удаленную функциональность, вы можете вернуться на предыдущую версию приложения.

Сравнение функций приложения в зависимости от типа операционной системы

В таблице ниже приведено сравнение функций Kaspersky Small Office Security в зависимости от типа операционной системы (персональный компьютер или файловый сервер).

Для персонального компьютера и терминального сервера список функций совпадает.

Сравнение функций Kaspersky Small Office Security

Функциональность	Файловый Сервер	Персональный компьютер
Центр управления Kaspersky Small Office Security	✓	✓
Быстрая проверка	✓	✓
Полная проверка	✓	✓
Выборочная проверка	✓	✓
Проверка внешних дисков	✓	✓
Фоновая проверка	✓	✓
Поиск уязвимостей	✓	✓
Файловый Антивирус	✓	✓
Интернет-защита	✓	✓
Почтовый Антивирус	✓	✓
Обновление баз и модулей приложения	✓	✓
Отчеты	✓	✓
Карантин	✓	✓
Устранение неполадок Windows	✓	✓
Восстановление зараженного компьютера	✓	✓
Защита от эксплойтов	✓	✓
Мониторинг активности	✓	✓
Защита от сетевых атак	✓	✓
Проверка ссылок	✓	✓
Расширение Kaspersky Protection	✓	✓
Предотвращение вторжений	✓	✓
Сетевой экран	✓	✓
Мониторинг сети	✓	✓
Анти-Фишинг	✓	✓
Обновление приложений	✓	✓
Текущая активность	✓	✓
Режим сосредоточенной работы	✓	✓
Режим "Не беспокоить"	✓	✓

Экономия заряда батареи	✓	✓
Сталкерские приложения	✓	✓
Удаление рекламных приложений	✓	✓
Удаление следов активности	✓	✓
Уничтожитель файлов	✓	✓
Секретная папка	✓	✓
Резервное копирование	✓	✓
Менеджер приложений		✓
Экранная клавиатура		✓
Защита ввода данных с аппаратной клавиатуры		✓
Защита от сбора данных в интернете		✓
Безопасные платежи		✓
Веб-контроль		✓
Защита веб-камеры		✓
Блокировщик скрытых установок		✓
Анти-Баннер		✓
Менеджер паролей		✓

Аппаратные и программные требования

Общие требования

- 1500 МБ свободного места на жестком диске.
- Процессор с поддержкой инструкций SSE2.

  > Архитектура ARM не поддерживается.

- Подключение к интернету (для установки и активации приложения, использования Kaspersky Security Network, а также обновления баз и модулей приложения).
- Microsoft Windows® Installer 4.5 или выше.
- Microsoft .NET Framework 4 или выше.
- Защита от несанкционированного доступа к веб-камере предоставляется только для совместимых моделей веб-камер.

При установке на персональный компьютер

Операционная система	Процессор	Свободная оперативная память	Ограничения
Microsoft Windows 11 Home (21H2, 22H2, 23H2, 24H2, 25H2)	1 ГГц или выше	4 ГБ (для 64-разрядной операционной системы)	Подсистема Windows для Linux 2 (WSL2) не поддерживается.
Microsoft Windows 11 Enterprise (21H2, 22H2, 23H2, 24H2, 25H2)			
Microsoft Windows 11 Pro (21H2, 22H2, 23H2, 24H2, 25H2)			
Microsoft Windows 10 Home (версии: 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, 21H1, 21H2, 22H2)	1 ГГц или выше	1 ГБ (для 32-разрядной операционной системы) или 2 ГБ (для 64-разрядной операционной системы)	Подсистема Windows для Linux 2 (WSL2) не поддерживается.
Microsoft Windows 10 Enterprise (версии: 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, 21H1, 21H2, 22H2)			
Microsoft Windows 10 Pro (версии: 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, 21H1, 21H2, 22H2)			
Microsoft Windows 8.1 (Service Pack 0 или выше, Windows 8.1 Update)	1 ГГц или выше	1 ГБ (для 32-разрядной операционной системы) или 2 ГБ (для 64-разрядной операционной системы)	
Microsoft Windows 8.1 Pro (Service Pack 0 или выше, Windows 8.1 Update)			
Microsoft Windows 8.1 Enterprise (Service Pack 0 или выше, Windows 8.1 Update)			
Microsoft Windows 8 (Service Pack 0 или выше)	1 ГГц или выше	1 ГБ (для 32-разрядной операционной системы) или 2 ГБ (для 64-разрядной операционной системы)	
Microsoft Windows 8 Pro (Service Pack 0 или выше)			
Microsoft Windows 8 Enterprise (Service Pack 0 или выше)			

Операционная система	Процессор	Свободная оперативная память	Ограничения
Microsoft Windows 7 Starter (Service Pack 1 или выше)	1 ГГц или выше	1 ГБ (для 32-разрядной операционной системы) или 2 ГБ (для 64-разрядной операционной системы)	
Microsoft Windows 7 Home Basic (Service Pack 1 или выше)			
Microsoft Windows 7 Home Premium (Service Pack 1 или выше)			
Microsoft Windows 7 Professional (Service Pack 1 или выше)			
Microsoft Windows 7 Ultimate (Service Pack 1 или выше)			

Приложение Kaspersky Small Office Security не может быть установлено на Microsoft Windows 7, если не установлены обновления операционной системы: KB4490628 (обновление от 12 марта 2019) и KB4474419 (обновление от 23 сентября 2019).

Для работы компонентов Интернет-защита, Анти-Баннер и Безопасные платежи в операционной системе должна быть запущена служба Base Filtering Engine (служба базовой фильтрации).

Поддержка терминальных серверов

При установке на персональный компьютер приложение поддерживает мультисессионные терминальные подключения для следующих операционных систем:

- Microsoft Windows 10 Enterprise for Virtual Desktops (EVD);
- Microsoft Windows 7 Enterprise for Virtual Desktops (EVD);
- Microsoft Windows Server 2022;
- Microsoft Windows Server 2019;
- Microsoft Windows Server 2016;
- Microsoft Windows Server 2012 R2;
- Microsoft Windows Server 2012;
- Microsoft Windows Server 2008 R2.

Поддержка браузеров

Браузеры, которые поддерживают установку расширения Kaspersky Protection:

- Microsoft Edge на базе Chromium 77.x – 141.x;
- Mozilla™ Firefox™ версий 52.x – 143.x, включая Mozilla Firefox MSIX 94.x;
- Mozilla™ Firefox™ ESR 52.x, 60.x, 68.x, 78.x, 91.x, 102.x, 115.x, 128.x, 140.x;

- Google Chrome™ версий 48.x – 141.x;
- Яндекс.Браузер 18.3.1 – 22.9.5, 24.x, 25.x;
- Opera на базе Chromium 117.x – 122.x.

Браузеры, которые поддерживают Экранную клавиатуру и Проверку защищенных соединений:

- Microsoft Edge на базе Chromium 77.x – 141.x;
- Mozilla Firefox версий 52.x – 143.x, включая Mozilla Firefox MSIX 94.x;
- Mozilla Firefox ESR 52.x, 60.x, 68.x, 78.x, 91.x, 102.x, 115.x, 128.x, 140.x;
- Google Chrome 48.x – 141.x;
- Яндекс.Браузер 18.3.1 – 22.9.5, 23.x, 24.x, 25.x;
- Opera на базе Chromium 117.x – 122.x.

Браузеры, которые поддерживают защищенный режим браузера:

- Microsoft Internet Explorer 8.0, 9.0, 10.0, 11.0;
- Microsoft Edge на базе Chromium 77.x – 141.x;
- Mozilla Firefox версий 52.x – 143.x, за исключением Mozilla Firefox MSIX 94.x в защищенном режиме;
- Mozilla Firefox ESR 52.x, 60.x, 68.x, 78.x, 91.x, 102.x, 115.x, 128.x, 140.x;
- Google Chrome 48.x – 141.x;
- Яндекс.Браузер 18.3.1 – 22.9.5, 23.x, 24.x, 25.x;
- Opera на базе Chromium 117.x – 122.x.

Поддержка более новых версий браузеров возможна, если браузер поддерживает соответствующую технологию.

Kaspersky Small Office Security поддерживает работу с браузерами Google Chrome и Mozilla Firefox как в 32-разрядной, так и в 64-разрядной операционной системе.

Требования для планшетных компьютеров

- Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows 8.1, Microsoft Windows 10, Microsoft Windows 11;
- процессор Intel® Celeron® 1.66 ГГц или выше;
- 1024 МБ свободной оперативной памяти.

Требования для нетбуков

- процессор Intel Atom™ 1600 МГц или выше;
- 1024 МБ свободной оперативной памяти;
- дисплей 10.1 дюймов с разрешением 1024x768;
- графический чипсет Intel GMA 950 или выше.

Требования для Kaspersky Password Manager вы можете найти в справке к этому приложению.

При установке на файловый сервер

Приложение Kaspersky Small Office Security не предназначено для установки на Microsoft Windows Server Datacenter и файловые сервера, работающие в режиме Server Core.

Операционная система	Процессор	Свободная оперативная память
Microsoft Windows Server 2022 Standard	64-разрядный (x64) процессор 1,4 ГГц или выше	2 ГБ
Microsoft Windows Server 2019 Essentials / Standard RTM	64-разрядный (x64) процессор 1,4 ГГц или выше	2 ГБ
Microsoft Windows Server 2016 Essentials / Standard RTM	64-разрядный (x64) процессор 1,4 ГГц или выше	2 ГБ
Microsoft Windows Server 2012 R2 Foundation / Essentials / Standard	64-разрядный (x64) процессор 1,4 ГГц или выше	4 ГБ
Microsoft Windows Server 2012 Foundation / Essentials / Standard	64-разрядный (x64) процессор 1,4 ГГц или выше	4 ГБ
Microsoft Windows Small Business Server 2011 Essentials / Standard Service Pack 1 или выше	64-разрядный (x64) процессор 2 ГГц или выше	8 ГБ
Microsoft Windows Server 2008 R2 Foundation / Standard / Enterprise Service Pack 1 или выше	64-разрядный (x64) процессор 1,4 ГГц или выше или двухъядерный процессор 1,4 ГГц или выше	512 МБ

Совместимость с другими приложениями "Лаборатории Касперского"

Приложение Kaspersky Small Office Security совместимо со следующими приложениями "Лаборатории Касперского":

- Kaspersky Safe Kids 1.5 и Safe Kids 2023;
- Kaspersky Password Manager 10.0, 10.1, 10.2, 10.3, 2023.0, 2023.1, 2023.2, 2024.0, 2024.1, 2024.2, 2024.3, 2025, 2025.1;
- Kaspersky Software Updater 2.1;
- Kaspersky Virus Removal Tool 2015, 2020;
- Kaspersky Secure Connection 4.0, 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, 5.13, 5.14, 5.15, 5.16; 5.17, 5.18, 5.19, 5.20, 5.21, 5.22, 5.23.

Функциональность Безопасное VPN-соединение доступна не во всех регионах.

Приложение Kaspersky Small Office Security, установленное на файловом сервере, совместимо с приложениями Kaspersky Security for Microsoft Exchange Servers 9.0 Maintenance Release 6 и выше (включая hotfix 1) и Kaspersky Security for Microsoft Exchange Servers 9.0 Maintenance Release 6. Для корректной совместной работы требуется выполнить следующие действия в Kaspersky Small Office Security на файловом сервере:

- Выключить Почтовый Антивирус.
- Выключить Интернет-защиту или в настройках Интернет-защиты внести веб-адреса Exchange Web Services в список доверенных веб-адресов (**Настройки Интернет-защиты** → **Расширенная настройка** → **Доверенные веб-адреса**).

Как установить и удалить приложение

Как установить приложение

"Лаборатория Касперского" подготовила для резидентов штата Калифорния (США) специальную версию приложения. Если вы являетесь резидентом штата Калифорния (США), вам нужно скачать и установить эту версию приложения.

Приложение устанавливается на компьютер в интерактивном режиме с помощью мастера установки и удаления.

Установка на файловый сервер и персональный компьютер выполняется из одного пакета установки. Приложение будет работать в режиме Персонального компьютера, если при установке будет выбран вариант **Использовать для защиты Терминального сервера – RDTS**. Подробнее см. в разделе Сравнение функций приложения в зависимости от типа операционной системы.

Мастер состоит из последовательности окон (шагов). Количество и последовательность шагов мастера зависит от региона, в котором вы устанавливаете приложение. В некоторых регионах мастер предложит вам принять дополнительные соглашения на обработку персональных данных. Для прекращения работы мастера на любом шаге установки следует закрыть окно мастера.

Если приложение будет использовано для защиты более чем одного компьютера (максимально допустимое количество компьютеров определяется условиями Лицензионного соглашения), то процедура установки будет одинаковой на всех компьютерах.

Чтобы установить приложение на ваш компьютер,

- если вы используете установочный диск, вставьте диск в дисковод и следуйте инструкциям, отображенным на экране.
- если вы скачали приложение из интернета, запустите его. Далее установка приложения выполняется с помощью стандартного мастера установки и удаления. При этом для некоторых языков локализации мастер отображает несколько дополнительных шагов установки.

Также возможна **установка приложения из командной строки**.

Вы можете установить Kaspersky Small Office Security с помощью командной строки.

> Некоторые команды можно выполнить только под учетной записью администратора.

Синтаксис командной строки:

```
<путь к файлу установочного пакета> [параметры]
```

Подробная инструкция и перечень настроек установки приведены на сайте Службы технической поддержки.

Мастером установки будут выполнены следующие шаги:

1. Начало установки

   На этом шаге мастер предлагает вам установить приложение.

2. Установка дополнительных приложений

   При установке приложения Kaspersky Small Office Security вы можете дополнительно установить следующие приложения:

   - Kaspersky Secure Connection, предназначенное для включения безопасного VPN-соединения с помощью Virtual Private Network (VPN).

   > Функциональность Безопасное VPN-соединение доступна не во всех регионах.

   - Kaspersky Password Manager, предназначенное для защиты паролей.

   Удалить Kaspersky Secure Connection и Kaspersky Password Manager можно независимо от приложения Kaspersky Small Office Security.

   В зависимости от типа установки и языка локализации на этом шаге мастер может предлагать вам ознакомиться с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", а также принять участие в программе Kaspersky Security Network.

   Просмотр Лицензионного соглашения

   > Этот шаг мастера отображается для некоторых языков локализации при установке приложения, скачанного через интернет.
   >
   > На этом шаге мастер предлагает вам ознакомиться с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского".
   >
   > Внимательно прочитайте Лицензионное соглашение и, если вы согласны со всеми его пунктами, нажмите на кнопку **Продолжить** (в некоторых регионах эта кнопка называется **Принять**).
   >
   > В некоторых версиях приложения Лицензионное соглашение можно открыть по ссылке на приветственном экране мастера. В этом случае в окне с текстом лицензионного соглашения доступна только кнопка **Назад**. Нажимая на кнопку **Продолжить** вы принимаете условия лицензионного соглашения.
   >
   > Установка приложения на ваш компьютер будет продолжена.
   >
   > Если условия Лицензионного соглашения не приняты, установка приложения не производится.
   >
   > > В некоторых регионах для продолжения установки приложения вы также должны принять условия Политики конфиденциальности.

   Просмотр Положения о Kaspersky Security Network

На этом шаге мастер предлагает вам принять участие в программе Kaspersky Security Network. Участие в программе предусматривает отправку в АО "Лаборатория Касперского" информации об угрозах, обнаруженных на вашем компьютере, о запускаемых приложениях и о скачиваемых подписанных приложениях, а также информации об операционной системе. При этом сбор, обработка и хранение ваших персональных данных не производятся.

Ознакомьтесь с Положением о Kaspersky Security Network. Если вы согласны со всеми его пунктами, в окне мастера нажмите на кнопку **Принять**.

Если вы не хотите принимать участие в программе Kaspersky Security Network, нажмите на кнопку **Отказаться**.

После принятия или отказа от участия в Kaspersky Security Network установка приложения продолжится.

В некоторых версиях приложения Положение о Kaspersky Security Network включает информацию об обработке персональных данных.

3. Установка приложения

   Установка приложения занимает некоторое время. Дождитесь ее завершения. По завершении установки мастер автоматически переходит к следующему шагу.

   Проверки во время установки приложения

   Во время установки приложение производит ряд проверок. В результате этих проверок могут быть обнаружены следующие проблемы:

   - *Несоответствие операционной системы программным требованиям*. Во время установки мастер проверяет соблюдение следующих условий:
     - соответствие операционной системы и пакетов обновлений (Service Pack) программным требованиям;
     - наличие необходимых приложений;
     - наличие необходимого для установки свободного места на диске;
     - наличие прав администратора у пользователя, выполняющего установку приложения.

     Если какое-либо из перечисленных условий не выполнено, на экран будет выведено соответствующее уведомление.
   - *Наличие на компьютере несовместимых приложений*. При обнаружении несовместимых приложений их список будет выведен на экран, и вам будет предложено удалить их. Приложения, которые невозможно удалить автоматически, нужно удалить вручную с помощью кнопки **Удалить вручную**.

   Во время удаления несовместимых приложений потребуется перезагрузка операционной системы, после чего установка Kaspersky Small Office Security продолжится автоматически.

4. Завершение установки

   На этом шаге мастер информирует вас о завершении установки приложения.

   Все необходимые компоненты приложения будут запущены автоматически сразу после завершения установки.

   В некоторых случаях для завершения установки может потребоваться перезагрузка операционной системы.

Вместе с приложением устанавливаются расширения для браузеров, обеспечивающие безопасную работу в интернете.

Как активировать приложение

При первом запуске Kaspersky Small Office Security запускается мастер активации приложения.

Активация – это процедура введения в действие полнофункциональной версии приложения на определенный срок.

Удаленное управление лицензированием и защитой подключенных устройств доступно только после того, как вы создадите аккаунт руководителя организации или администратора в Центре управления Kaspersky Small Office Security. Вы можете создать аккаунт в окне подключения к аккаунту в процессе активации приложения. Этот аккаунт будет использоваться для установки Kaspersky Small Office Security на компьютеры и мобильные устройства сотрудников организации. После создания аккаунта необходимо зарегистрировать лицензию Kaspersky Small Office Security в Центре управления Kaspersky Small Office Security.

Чтобы активировать приложение:

Вам предлагаются следующие варианты активации Kaspersky Small Office Security:

- Если вы приобрели лицензию на использование приложения, введите код активации в поле ввода и нажмите на кнопку **Активировать**.
- Если в вашем аккаунте есть действующая лицензия, нажмите на ссылку **Получить лицензию из аккаунта**.

  Укажите адрес электронной почты и пароль и подключитесь к Центру управления Kaspersky Small Office Security для активации приложения.
- Если вы хотите установить пробную версию приложения перед принятием решения о приобретении лицензии, нажмите на кнопку **Активировать пробную версию**. Вы сможете использовать приложение в режиме полной функциональности в течение короткого ознакомительного периода. По истечении срока действия пробной лицензии возможность повторной активации пробной версии приложения будет недоступна.

В процессе активации приложения может потребоваться пройти регистрацию в Центре управления Kaspersky Small Office Security. Вы можете создать аккаунт в окне подключения.

Для активации приложения необходимо подключение к интернету.

Расширение Kaspersky Protection для браузеров

Для полноценной поддержки браузеров приложением Kaspersky Small Office Security в браузерах должно быть установлено и включено расширение Kaspersky Protection. С помощью расширения Kaspersky Protection в веб-страницу, открытую в защищенном режиме браузера, и в трафик внедряется скрипт. Приложение использует этот скрипт для взаимодействия с веб-страницей и для передачи данных в банки, чьи сайты защищаются с помощью компонента Безопасные платежи. Приложение защищает передаваемые скриптом данные с помощью цифровой подписи. Приложение может внедрять скрипт без использования расширения Kaspersky Protection.

Приложение подписывает передаваемые скриптом данные с помощью установленных антивирусных баз и запросов в Kaspersky Security Network. Приложение передает запросы в Kaspersky Security Network независимо от того, приняли вы условия Положения о Kaspersky Security Network или нет.

С помощью расширения Kaspersky Protection при работе в браузере вы можете:

- Управлять Защитой от сбора данных в интернете
- Управлять Анти-Баннером
- Безопасные платежи
- **Сообщить о подозрении на фишинг**

  Чтобы сообщить о подозрении на фишинговый сайт:

  1. Убедитесь, что вы находитесь на странице сайта, который подозреваете в фишинге.
  2. В панели инструментов браузера нажмите на кнопку **Kaspersky Protection**.
  3. В меню расширения выберите **Сообщить о подозрении на фишинг**.

     Функция **Сообщить о подозрении на фишинг** отключена, если это действие недоступно для текущего веб-сайта.
  4. Проверьте, что в открывшемся окне отображается веб-адрес сайта, который вы подозреваете в фишинге.
  5. Нажмите на кнопку **Сообщить**.

  Сообщение будет доставлено в Kaspersky Security Network.

- **Сообщить о проблеме с сайтом**

  Чтобы сообщить о проблеме с сайтом:

  1. Убедитесь, что вы находитесь на странице сайта, о проблеме которого вы хотели бы сообщить.
  2. В панели инструментов браузера нажмите на кнопку **Kaspersky Protection**.
  3. В меню расширения выберите **Сообщить о проблеме с сайтом**.

     Функция **Сообщить о проблеме с сайтом** отключена, если это действие недоступно для текущего веб-сайта.
  4. Проверьте, что в открывшемся окне отображается веб-адрес сайта.
  5. Опишите проблему в поле ввода.
  6. Нажмите на кнопку **Сообщить**.

  Сообщение будет доставлено.

- Открыть экранную клавиатуру

Установка расширения Kaspersky Protection в браузеры Microsoft Edge на базе Chromium, Mozilla Firefox, Яндекс.Браузер, Google Chrome и Opera на базе Chromium

Автоматическая установка расширения Kaspersky Protection в браузеры Microsoft Edge на базе Chromium, Mozilla Firefox, Яндекс.Браузер, Google Chrome и Opera на базе Chromium не предусмотрена. Вам необходимо скачать и установить расширение Kaspersky Protection вручную. Скачать и установить расширение можно из окна уведомления, которое появляется, когда вы первый раз запускаете браузер после установки приложения. Кроме того, вы можете загрузить и установить расширение из окна приложения или из магазина Chrome.

Как скачать и установить расширение Kaspersky Protection в браузеры Microsoft Edge на базе Chromium, Mozilla Firefox, Яндекс.Браузер, Google Chrome и Opera на базе Chromium

1. Откройте главное окно приложения и выполните одно из следующих действий:
   - В главном окне найдите рекомендацию установить расширение для браузера и нажмите на кнопку **Включить**.
   - Выберите раздел **Безопасность**.
     a. Выберите раздел **Расширение Kaspersky Protection**.
     b. В блоке **Расширение Kaspersky Protection** выберите необходимый браузер и по ссылке **Включить** перейдите в окно установки расширения.
2. Выполните стандартную процедуру установки расширения в вашем браузере (смотрите справку вашего браузера).
3. После завершения установки включите расширение в вашем браузере, если необходимо (смотрите справку вашего браузера).

Блок **Расширение Kaspersky Protection** и рекомендация установить расширение Kaspersky Protection в главном окне становятся доступными после первого запуска браузера с момента установки приложения Kaspersky Small Office Security.

Поддержка Яндекс.Браузера

При использовании Яндекс.Браузера работают следующие компоненты приложения:

- Безопасные платежи (защищенный режим браузера);
- Проверка ссылок;
- Интернет-защита;
- Анти-Фишинг;
- Анти-Баннер;
- Защита от сбора данных в интернете;

- Экранная клавиатура;
- Защита ввода данных.

Поддержка Internet Explorer

Расширение Kaspersky Protection не поддерживает браузер Internet Explorer.

Как удалить приложение

В результате удаления приложения компьютер и ваши персональные данные окажутся незащищенными.

При удалении приложения вам будет предложено заполнить краткий опрос, чтобы рассказать о причинах вашего решения. Это поможет нам улучшить приложение и сделать его более удобным для вас в будущем.

Удаление приложения выполняется с помощью мастера установки и удаления.

Как удалить приложение в операционной системе Windows 7

Чтобы запустить мастер в операционной системе Microsoft Windows 7 и ниже,

в меню **Пуск** выберите пункт **Все Программы** → **Kaspersky Small Office Security** → **Удалить Kaspersky Small Office Security**.

Как удалить приложение в операционной системе Windows 8 и выше

Чтобы запустить мастер в операционной системе Microsoft Windows 8 и выше:

1. Найдите установленное приложение одним из следующих способов:
   - В Windows 8 нажмите на кнопку **Пуск** и найдите приложение Kaspersky Small Office Security на экране быстрого запуска.
   - В Windows 10 и выше нажмите на кнопку **Пуск** и найдите приложение в списке, либо воспользуйтесь строкой поиска.
2. Нажмите правой клавишей мыши на значке приложения Kaspersky Small Office Security.
3. В контекстном меню выберите пункт **Удалить**.
4. В открывшемся окне выберите в списке Kaspersky Small Office Security.
5. Нажмите на кнопку **Удалить** / **Изменить** в верхней части списка.

Будет запущен мастер установки и удаления приложения.

В процессе удаления необходимо выполнить следующие шаги:

1. Чтобы удалить приложение, требуется ввести пароль для доступа к настройкам приложения. Если вы по каким-либо причинам не можете указать пароль, удаление приложения будет невозможно.

   Этот шаг отображается, если был установлен пароль на удаление приложения.

2. Сохранение данных для повторного использования

   На этом шаге вы можете указать, какие используемые приложением данные вы хотите сохранить для дальнейшего использования при повторной установке приложения (например, при установке более новой версии).

Вы можете сохранить следующие данные:

- **Информация о лицензии** – данные, позволяющие в дальнейшем не активировать устанавливаемое приложение, а использовать его по уже действующей лицензии, если срок действия лицензии не истечет к моменту установки.
- **Файлы карантина** – файлы, проверенные приложением и помещенные на карантин.
- После удаления приложения с компьютера файлы на карантине недоступны. Для работы с этими файлами нужно установить приложение Kaspersky Small Office Security.
- **Настройки работы приложения** – параметры работы приложения, установленные во время его настройки.

  Вы также можете экспортировать настройки защиты при помощи командной строки, используя команду `avp.com EXPORT <имя_файла>`
- **Данные iChecker** – файлы, содержащие информацию об объектах, уже проверенных с помощью технологии iChecker.
- **Секретная папка** – файлы, которые вы помещали на хранение в секретную папку.

  Перенос настроек из приложения для персонального компьютера в приложение для файлового сервера и наоборот не поддерживается.

1. Подтверждение удаления

   Поскольку удаление приложения ставит под угрозу защиту компьютера и ваших персональных данных, требуется подтвердить свое намерение удалить приложения. Для этого нажмите на кнопку **Удалить**.

2. Завершение удаления

На этом шаге мастер удаляет приложение с вашего компьютера. Дождитесь завершения процесса удаления.

Эта функциональность может быть недоступна в некоторых регионах.

В процессе удаления требуется перезагрузка операционной системы. Если вы откажетесь от немедленной перезагрузки, завершение процедуры удаления будет отложено до того момента, когда операционная система будет перезагружена или компьютер будет выключен и включен снова.

Как обновить приложение Kaspersky Small Office Security

Приложение обновляется автоматически, если в окне настройки обновления выбран режим запуска обновлений **Автоматически** (**Безопасность** → **Обновление антивирусных баз** → **Расписание обновления баз**).

Также приложение автоматически обновляется, если вы устанавливаете новую версию приложения поверх старой. При обновлении приложения все ваши настройки сохраняются.

Если в момент доставки обновления у пользователя есть приостановленные задачи сканирования, то приложение принудительно завершит эти задачи и запустит обновление. Активные задачи сканирования принудительно не завершаются.

Установка Kaspersky Small Office Security поверх Kaspersky Small Office Security 5, 6 или 7

Если вы устанавливаете Kaspersky Small Office Security на компьютер, на котором уже установлено приложение Kaspersky Small Office Security 5, 6 или 7, следующие типы данных будут недоступны: файлы на карантине.

При наличии действующей лицензии на использование предыдущей версии Kaspersky Small Office Security вам не понадобится активировать приложение: мастер установки и удаления автоматически получит информацию о лицензии на использование предыдущей версии Kaspersky Small Office Security и применит ее во время установки Kaspersky Small Office Security.

Во время скачивания обновления приложение сравнивает Лицензионное соглашение, Положение о Kaspersky Security Network и Положение об обработке данных для маркетинговых целей предыдущей и новой версий. Если соглашения или положения различаются, приложение предложит вам заново прочитать и принять их.

Обновление предыдущей версии приложения имеет ограничения.

Если вы создавали контейнер в приложении Kaspersky Small Office Security 4, то при первом обращении к контейнеру Kaspersky Small Office Security преобразует контейнер в секретную папку. Файлы в секретной папке станут доступны по завершении преобразования. Преобразование контейнеров в секретные папки может выполняться в течение продолжительного времени.

Приложение может быть обновлено, если на вашем компьютере установлены следующие версии Kaspersky Small Office Security:

- Kaspersky Small Office Security 5;
- Kaspersky Small Office Security 6;
- Kaspersky Small Office Security 7.

Ограничения при обновлении предыдущей версии приложения

Обновление приложения Kaspersky Small Office Security имеет следующие ограничения и особенности:

- После обновления предыдущей версии приложения Kaspersky Small Office Security запускается автоматически, даже если в сохраненных настройках автозапуск приложения выключен. При последующих перезагрузках операционной системы Kaspersky Small Office Security не запускается автоматически, если в сохраненных настройках автозапуск приложения выключен.

- Если в предыдущей версии Kaspersky Small Office Security на файловом сервере не было компонента Мониторинг активности, при обновлении на новую версию этот компонент по умолчанию будет включен. Если вы обновляетесь с версии Kaspersky Small Office Security, в которой уже был компонент Мониторинг активности, настройки компонента сохраняются.

Лицензирование приложения

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием приложения Kaspersky Small Office Security.

О Лицензионном соглашении

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

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

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения при установке приложения. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку приложения и не должны использовать приложение.

О лицензии

Функциональность доступна не во всех регионах.

Лицензия – это ограниченное по времени право на использование приложения, предоставляемое вам на основании Лицензионного соглашения.

Список доступных функций и срок использования приложения зависят от типа лицензии, по которой было активировано приложение.

Предусмотрены следующие типы лицензий:

- *Пробная* – бесплатная лицензия, предназначенная для ознакомления с приложением.

  Пробная лицензия имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Small Office Security прекращает выполнять все свои функции. Чтобы продолжить использование приложения, вам нужно приобрести коммерческую лицензию.

  Вы можете активировать приложение по пробной лицензии только один раз.

- *Коммерческая* – платная лицензия, предоставляемая при приобретении приложения.

  По истечении срока действия коммерческой лицензии приложение прекращает выполнять свои основные функции. Для продолжения работы Kaspersky Small Office Security вам нужно продлить срок действия коммерческой лицензии. По истечении срока действия коммерческой лицензии вы не сможете продолжать использовать приложение и должны удалить его со своего устройства.

  Вы можете получить специальное предложение, которое позволит вам включить автоматическое продление и получить скидку на следующий период лицензии при активации текущей лицензии. Если вы согласны подключить автоматическое продление, нажмите **Забрать скидку** и вы будете перенаправлены на сайт, где сможете указать платежную информацию. Если вы не хотите включать автоматическое продление прямо сейчас, вы можете сделать это позже. Специальное предложение будет доступно в секции **Профиль**.

  Рекомендуется продлевать лицензию не позднее даты ее окончания, чтобы обеспечить максимальную защиту от всех угроз компьютерной безопасности.

Перед приобретением лицензии вы можете ознакомиться с пробной версией Kaspersky Small Office Security без выплаты вознаграждения. Пробная версия Kaspersky Small Office Security выполняет свои функции в течение короткого ознакомительного периода. После окончания ознакомительного периода Kaspersky Small Office Security прекращает выполнять все свои функции. Для продолжения использования приложения требуется приобрести лицензию.

Kaspersky Small Office Security может быть установлен на следующих устройствах:

- Microsoft Windows;
- Microsoft Windows Server;
- Android (версия Kaspersky Small Office Security для этой операционной системы);
- macOS (версия Kaspersky Small Office Security для этой операционной системы).

Лицензия на Kaspersky Small Office Security дает вам право на использование Kaspersky Password Manager.

Также вы получаете доступ к Центру управления Kaspersky Small Office Security для управления защитой устройств.

О подписке

Подписка определяет настройки приложения (срок действия подписки, количество защищаемых устройств).

Подписку можно оформить у поставщика услуг (например, у интернет-провайдера). Вы можете приостанавливать или возобновлять подписку, продлевать ее в автоматическом режиме, а также отменить ее. Подпиской можно управлять в аккаунте на сайте поставщика услуг, у которого вы оформили подписку. В зависимости от поставщика услуг, набор возможных действий при управлении подпиской может различаться.

Чтобы активировать подписку на устройстве, нужно применить код активации, предоставленный поставщиком услуг. В некоторых случаях код активации может загружаться и применяться автоматически.

Если на момент оформления подписки у поставщика услуг приложение уже используется по действующей лицензии, то приложение будет использоваться по подписке от поставщика услуг. Текущую лицензию можно использовать на другом устройстве в течение ее срока действия.

Подписка может быть неограниченной (без даты окончания) или ограниченной (например, на один год). Неограниченная подписка продлевается автоматически при условии своевременного внесения предоплаты поставщику услуг. Для продолжения работы приложения после окончания ограниченной подписки необходимо самостоятельно продлить ее.

Если вы не продлили подписку или поставщику услуг не удалось автоматически продлить подписку, по ее окончании вам может предоставляться льготный период для продления подписки, в течение которого функциональность приложения сохранена. По истечении льготного периода приложение может перейти в режим ограниченной функциональности. Если льготный период и режим ограниченной функциональности не предусмотрены поставщиком услуг, по истечении срока действия подписки все функции приложения станут недоступны.

О коде активации

Код активации – это код, который вы получаете, приобретая лицензию на использование Kaspersky Small Office Security. Этот код необходим для активации приложения.

Код активации представляет собой уникальную последовательность из двадцати латинских букв и цифр в формате xxxxx-xxxxx-xxxxx-xxxxx.

В зависимости от способа приобретения приложения возможны следующие варианты получения кода активации:

- Если вы приобрели коробочную версию Kaspersky Small Office Security, код активации указан в документации или на коробке, в которой находится установочный компакт-диск.
- Если вы приобрели Kaspersky Small Office Security в интернет-магазине, код активации высылается по адресу электронной почты, указанному вами при заказе.

Отсчет срока действия лицензии начинается с даты активации приложения. Если вы приобрели лицензию, допускающую использование Kaspersky Small Office Security на нескольких устройствах, то отсчет срока действия лицензии начинается с даты первого применения кода активации.

Мы рекомендуем вам создать аккаунт Центра управления Kaspersky Small Office Security, чтобы не потерять код активации при переустановке операционной системы, установке приложения на новое устройство или переустановке приложения на текущем устройстве. Создать аккаунт Центра управления Kaspersky Small Office Security можно во время установки и активации приложения. Если вы не создали аккаунт Центра управления Kaspersky Small Office Security, во время установки и активации приложения, вы можете создать аккаунт в уже установленном приложении.

Если вы случайно удалили или потеряли код активации, вы можете попробовать восстановить его.

Как восстановить коды активации

Если вы потеряли ранее предоставленный вам код активации, вы можете восстановить его одним из следующих способов:

- Если у вас есть аккаунт Центра управления Kaspersky Small Office Security, вы можете найти ваши коды активации в разделе **Лицензии** на сайте Центр управления Kaspersky Small Office Security.
- Если у вас нет аккаунта Центра управления Kaspersky Small Office Security, но есть установленное и активированное приложение на каком-либо устройстве, создайте аккаунт Центра управления Kaspersky Small Office Security на этом устройстве и подключитесь к Центру управления Kaspersky Small Office Security. Приложение передаст данные о вашей лицензии в аккаунт. Код активации отобразится в разделе **Лицензии** на сайте Центр управления Kaspersky Small Office Security.
- Если у вас нет аккаунта Центра управления Kaspersky Small Office Security и нет активированного приложения ни на одном из ваших устройств, обратитесь в Службу технической поддержки.

Как купить или продлить лицензию

После истечения бесплатного пробного периода лицензия продлится и активируется автоматически без вашего участия. С указанного вами способа оплаты спишется стоимость продления лицензии.

В некоторых регионах может быть не предусмотрен автоматический переход на платную лицензию. Если вы не ввели платежные данные для последующего продления при активации бесплатной пробной лицензии, вам необходимо будет купить лицензию, чтобы обеспечить защиту ваших устройств.

Чтобы купить или продлить лицензию, выполните следующие действия:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Профиль** и выполните одно из следующий действий:
   - Чтобы продлить текущую лицензию, нажмите на кнопку **Продлить сейчас**.
   - Если ваша пробная лицензия истекла, нажмите на кнопку **Купить сейчас**.

   Откроется веб-страница интернет-магазина "Лаборатории Касперского" или компании-партнера, где вы можете продлить или купить лицензию.
3. При продлении или покупке лицензии на указанный адрес электронной почты будет отправлен код активации.
4. Активируйте приложение с помощью этого кода активации.

Продление лицензии с помощью нового кода активации

Если у вас есть новый код активации, вы можете заранее добавить его в свой аккаунт Центра управления Kaspersky Small Office Security. После истечения срока действия вашей текущей лицензии приложение можно будет активировать с помощью нового кода активации.

Чтобы добавить новый код активации в ваш аккаунт Центра управления Kaspersky Small Office Security:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Профиль**.
3. В блоке с информацией о лицензии нажмите на три точки и выберите **Сохранить код активации**.
4. Если вы вошли в свой аккаунт Центра управления Kaspersky Small Office Security, вам будет предложено сохранить код активации. Если вы не вошли в аккаунт, то сначала нужно будет войти в него, затем вам будет предложено сохранить код.
5. Введите код активации в предложенное поле, затем нажмите на кнопку **Сохранить код активации**. Лицензия будет сохранена в вашем аккаунте Центр управления Kaspersky Small Office Security.

Когда срок действия вашей текущей подписки истечет, вы сможете отправить этот код активации на свое устройство из своего аккаунта Центра управления Kaspersky Small Office Security. Подробную информацию о том, как отправить лицензию на подключенное к вашему аккаунту устройство, вы найдете в Справке Центра управления Kaspersky Small Office Security.

Резервные коды активации, добавленные в предыдущих версиях приложения, будут удалены после обновления. Если резервный код доступен, вы получите уведомление до обновления и сможете сохранить его в своем аккаунте Центра управления Kaspersky Small Office Security.

О режиме ограниченной функциональности

В таблице ниже можно посмотреть, какие функции Kaspersky Small Office Security доступны, а какие недоступны, когда приложение работает в режиме ограниченной функциональности. Если в графе "Режим ограниченной функциональности" указано значение "есть", это значит, что функциональность доступна в режиме ограниченной функциональности. Если в графе "Режим ограниченной функциональности" указано значение "нет", функциональность недоступна. Дополнительная информация указана в графе "Ограничения".

Функции Kaspersky Small Office Security в режиме ограниченной функциональности

Функциональность	Ограничения	Режим ограниченной функциональности
Проверка на вирусы		есть
Обновление антивирусных баз и модулей приложения	Доступны только критические обновления.	нет
Поиск уязвимостей в приложениях		есть

Функциональность	Ограничения	Режим ограниченной функциональности
Интернет-защита		есть на Windows 7, 8 / нет на Windows 10, 11
Файловый Антивирус		есть на Windows 7, 8 / нет на Windows 10, 11
Почтовый Антивирус		есть на Windows 7, 8 / нет на Windows 10, 11
Мониторинг активности		есть на Windows 7, 8 / нет на Windows 10, 11
Проверка репутации файлов в Kaspersky Security Network		нет
Защита ввода данных		нет
Восстановление зараженного компьютера	Доступно скачивание Kaspersky Rescue Disk через интерфейс приложения.	есть
Исключения и действия с найденными объектами		есть
Настройки сети		есть
Отчеты и карантин		есть
Настройка отображения приложения		есть
Режим "Не беспокоить"		нет
Режим сосредоточенной работы		нет
Предотвращение вторжений		есть на Windows 7, 8 / нет на Windows 10, 11
Сетевой экран		есть
Защита от сетевых атак		есть
Анти-Баннер		есть
Безопасные платежи		нет
Защита от сбора данных в интернете		есть
Удаление следов активности		нет
Защита веб-камеры		есть на Windows 7, 8 / нет на Windows 10, 11
Мониторинг сети		есть
Менеджер приложений		нет
Менеджер паролей		есть
Уничтожитель файлов		есть
Секретная папка	Доступно только получение доступа к данным в ранее созданных секретных папках.	нет
Резервное копирование	Доступно только восстановление данных из ранее созданных резервных копий.	нет
Обновление приложений		нет
Безопасное VPN-соединение	Функциональность Безопасное VPN-соединение доступна не во всех регионах.	есть
Устранение неполадок Windows		есть
Текущая активность		нет
Экономия заряда батареи		нет
Сталкерские приложения		нет
Блокировщик скрытых установок		нет

Функциональность	Ограничения	Режим ограниченной функциональности
Удалять рекламные приложения		нет
AMSI-защита		есть только на Windows 10, 11
Управление настройками		есть
Защита паролем настроек приложения		есть
Настройка потребления ресурсов компьютера		есть
История		есть
Советы		есть
Веб-Контроль	Доступен только просмотр отчетов.	нет
Обращение в техническую поддержку		есть

Удаленное управление защитой компьютера

В этом разделе содержится информация об удаленном управлении защитой компьютеров вашей организации с помощью Центра управления Kaspersky Small Office Security.

Об удаленном управлении защитой компьютеров

Если на компьютерах вашей организации установлено приложение Kaspersky Small Office Security, вы можете управлять защитой этих компьютеров удаленно. Удаленное управление защитой компьютеров выполняется на сайте Центр управления Kaspersky Small Office Security.

Настройка удаленного управления выполняется в следующей последовательности:

1. Регистрация аккаунта администратора на сайте Центр управления Kaspersky Small Office Security.
2. Регистрация лицензии Kaspersky Small Office Security на сайте Центр управления Kaspersky Small Office Security.
3. Подключение устройств, защитой которых вы хотите управлять удаленно, к сайту Центр управления Kaspersky Small Office Security в аккаунте администратора.

На сайте Центр управления Kaspersky Small Office Security вы можете решать следующие задачи по обеспечению безопасности компьютеров вашей организации:

- просматривать список проблем безопасности на компьютере и удаленно устранять их;
- проверять компьютер на вирусы и другие приложения, представляющие угрозу;
- обновлять антивирусные базы и модули приложения;
- настраивать компоненты приложения Kaspersky Small Office Security.

Если проверка компьютера запущена с сайта Центр управления Kaspersky Small Office Security, то Kaspersky Small Office Security обрабатывает обнаруженные объекты в автоматическом режиме без вашего участия. В случае обнаружения вируса или другого приложения, представляющего угрозу, приложение Kaspersky Small Office Security попытается выполнить лечение без перезагрузки компьютера. Если лечение без перезагрузки компьютера невозможно, на сайте Центр управления Kaspersky Small Office Security в списке проблем защиты компьютера появляется сообщение о том, что для лечения компьютера требуется перезагрузка.

Если на сайте Центр управления Kaspersky Small Office Security в списке обнаруженных объектов более 10 элементов, то они группируются. В этом случае через сайт обнаруженные объекты можно обработать только одновременно, без возможности просмотреть каждый объект. Для просмотра отдельных объектов в этом случае рекомендуется использовать интерфейс приложения, установленного на компьютере.

Об аккаунте в Центре управления Kaspersky Small Office Security

Для входа на сайт Центр управления Kaspersky Small Office Security, а также для работы с сайтом и некоторыми приложениями "Лаборатории Касперского" требуется *аккаунт*.

Если у вас еще нет аккаунта, вы можете создать его на сайте или в приложении в процессе подключения устройства к аккаунту.

Подключение компьютера к Центру управления Kaspersky Small Office Security

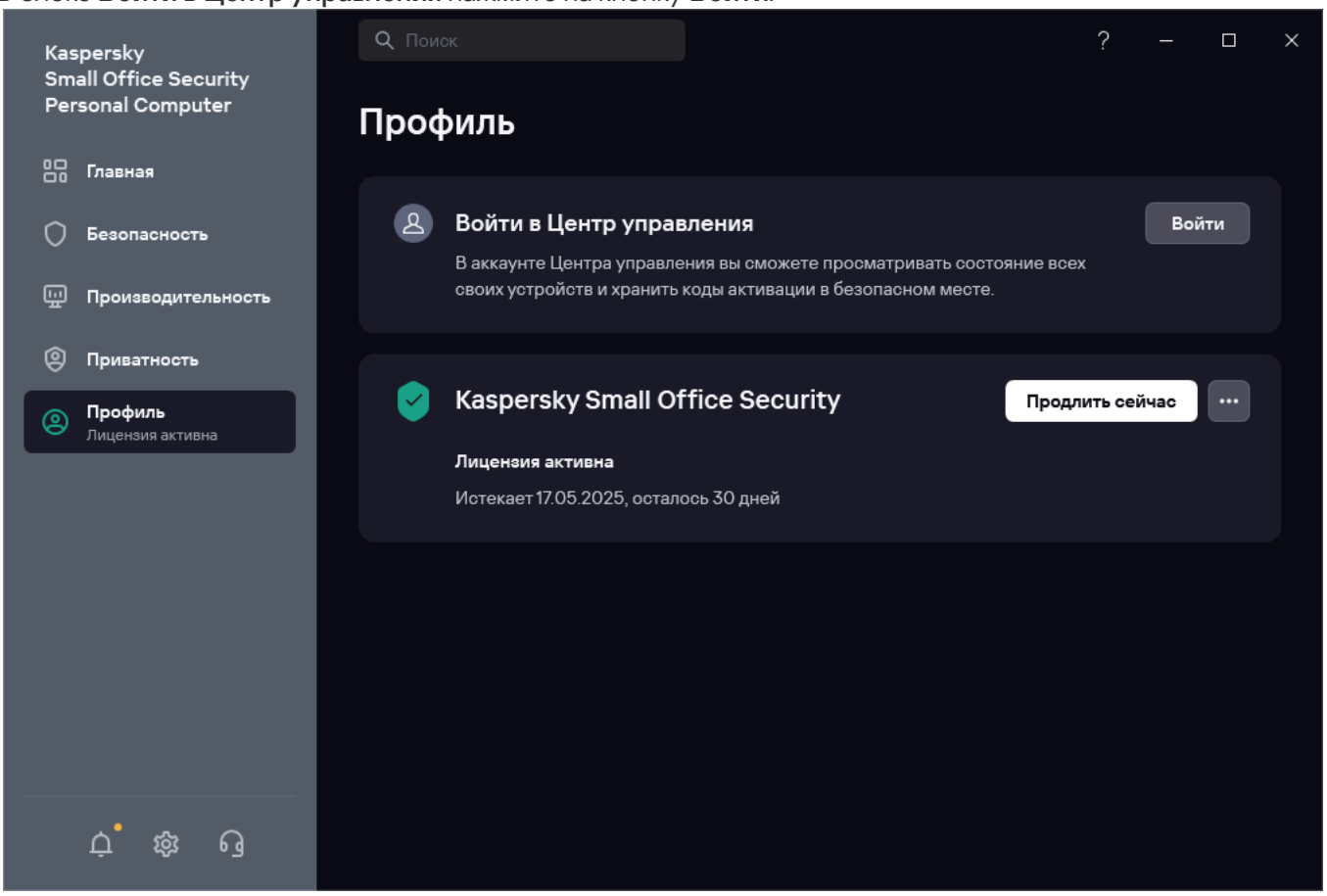
Входить в аккаунт Центр управления Kaspersky Small Office Security вы можете с помощью адреса электронной почты и пароля или вашего аккаунта Google, Facebook*, Apple, Яндекс или VK. Если у вас уже есть аккаунт, вы можете настроить быстрый вход с помощью аккаунта Google, Facebook*, Apple, Яндекс или VK в окне подключения устройства к аккаунту Центр управления Kaspersky Small Office Security. Это возможно, если для создания аккаунта Центр управления Kaspersky Small Office Security использовался адрес электронной почты от аккаунта Google, Facebook*, Apple, Яндекс или VK.

Доступность функции быстрого входа зависит от вашего региона. Более подробную информацию об ограничениях в России можно найти в этой статье (доступна только на английском и русском языках).

Чтобы подключить компьютер к Центру управления Kaspersky Small Office Security:

1. Установите Kaspersky Small Office Security на компьютере, защитой которого вы хотите управлять.
2. Откройте главное окно приложения.
3. Перейдите в раздел **Профиль**.

4. В блоке **Войти в Центр управления** нажмите на кнопку **Войти**.



5. Введите пароль администратора. Этот шаг доступен, если установлена защита доступа к управлению приложением.

6. В окне подключения к аккаунту выберите наиболее удобный для вас способ подключения:

   - **Вход с помощью адреса электронной почты**. Укажите адрес вашей электронной почты в поле ввода. Письмо со ссылкой для создания пароля будет отправлено на указанный адрес электронной почты.

     Если в аккаунте Центр управления Kaspersky Small Office Security вы настроили двухэтапную проверку, на ваш телефон будет отправлено сообщение с проверочным кодом. Введите проверочный код в поле ввода и нажмите на кнопку **Продолжить**.

   - **Вход с помощью аккаунта Google, Facebook*, Apple, Яндекс или VK**.

     a. Нажмите **Войти с Google**, **Войти с Facebook**, **Войти с Apple**, **Войти с Яндекс ID**, или **Войти с VK ID**.

     В открывшемся окне браузера войдите в свой аккаунт Google, Facebook*, Apple, Яндекс или VK и предоставьте приложению доступ к вашему адресу электронной почты.

     Если у вас еще нет аккаунта Google, Facebook*, Apple, Яндекс или VK, вы можете создать его, а затем продолжить настройку быстрого входа в Центр управления Kaspersky Small Office Security.

     Если в вашем аккаунте Центр управления Kaspersky Small Office Security настроена двухэтапная проверка, настройте быстрый вход в своем аккаунте на сайте Центр управления Kaspersky Small Office Security, а затем вернитесь в приложение и войдите с помощью Google, Facebook*, Apple, Яндекс или VK.

     > Если вы используете браузер Microsoft Edge, для настройки входа в Центр управления Kaspersky Small Office Security требуется версия Microsoft Edge на базе Chromium 77.x и выше. В случае возникновения ошибки подключения, выберите другой браузер в качестве браузера по умолчанию, установите последнюю версию браузера Microsoft Edge или обновите операционную систему Microsoft Windows.

     b. Вернитесь в приложение и продолжите создание аккаунта нажатием на кнопку **Продолжить**. Следуйте дальнейшим инструкциям на экране.

     Ваше устройство будет подключено к аккаунту Центр управления Kaspersky Small Office Security. Дополнительно вы можете задать пароль для вашего аккаунта на сайте Центр управления Kaspersky Small Office Security.

     Обработка данных при входе в аккаунт

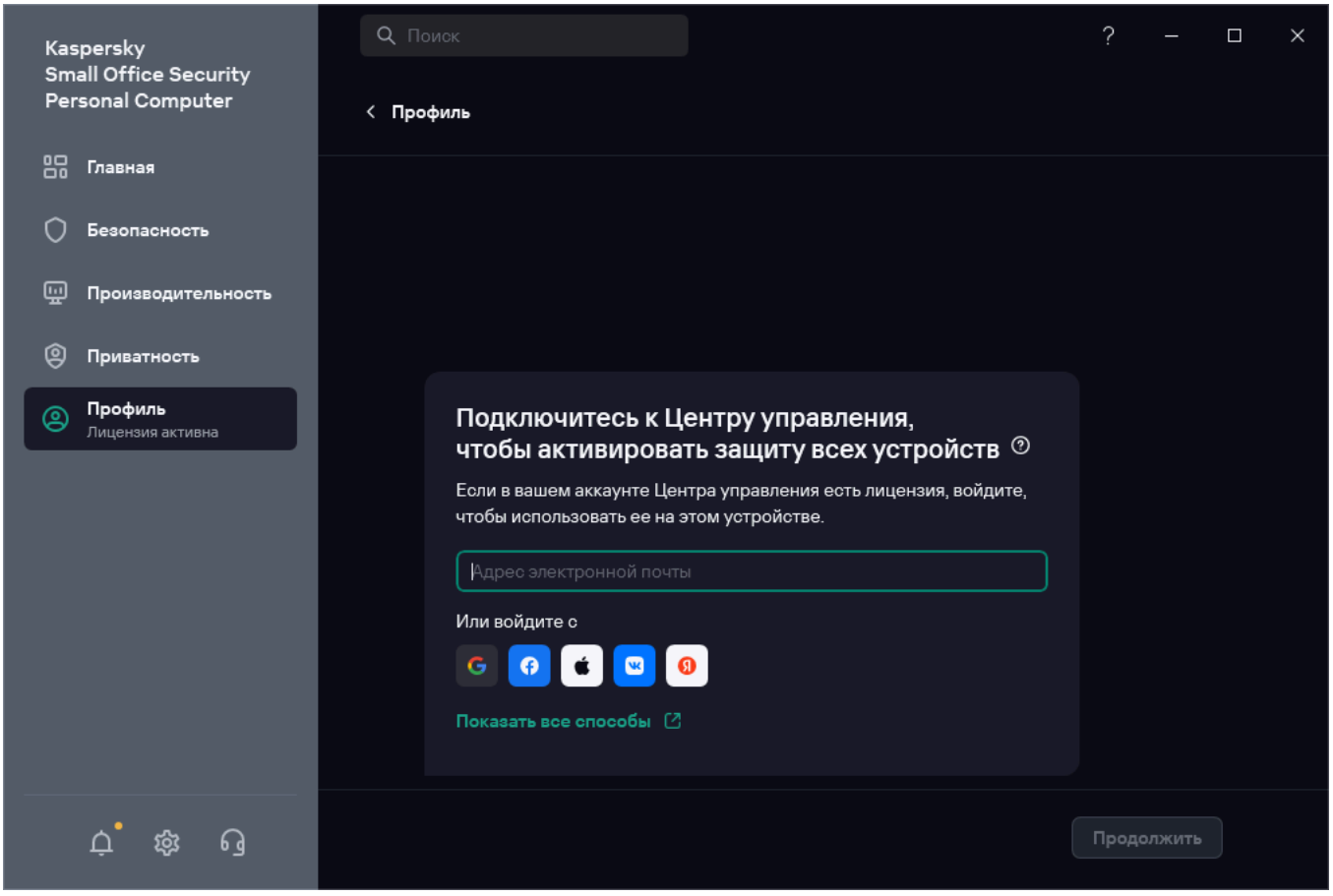
При входе в аккаунт Центр управления Kaspersky Small Office Security с помощью аккаунта Google, Facebook, Apple, Яндекс или VK осуществляется обработка следующих данных:

- идентификатор ресурса Правообладателя;
- значение, генерируемое для верификации запроса;
- тип токена;
- URI, на который отправляется ответ провайдера аутентификации.

При входе в аккаунт на сайте поставщиков услуг с помощью провайдеров аутентификации осуществляется обработка следующих данных:

- идентификатор ресурса Правообладателя;
- токен авторизации в инфраструктуре поставщика услуг;
- тип токена;
- параметры, запрашиваемые у провайдера аутентификации;
- URI, на который отправляется ответ провайдера аутентификации.

В некоторых регионах приложение предложит вам прочитать и принять Положение об обработке данных для использования Веб-Портала. Если вы согласны с условиями положения, нажмите на кнопку **Принять**.



После успешного подключения в разделе **Профиль** отобразится информация о том, что вы подключены к Центру управления Kaspersky Small Office Security. Теперь защитой компьютера можно управлять удаленно из Центра управления Kaspersky Small Office Security.

Как настроить проверку надежности пароля для удаленного доступа к файловому серверу

Kaspersky Small Office Security проверяет надежность пароля учетной записи Windows, который используется для получения удаленного доступа к файловому серверу.

При проверке надежности пароля Kaspersky Small Office Security учитывает следующие критерии:

- время последнего обновления пароля;
- минимальное количество символов, которое должен содержать пароль.

Чтобы настроить проверку надежности пароля:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Перейдите в раздел **Настройки приватности**.
4. В окне **Настройки приватности** нажмите на кнопку **Защита ввода данных**.
5. В разделе **Проверка надежности пароля учетной записи Windows** выполните следующие действия:
   - Установите флажок **Сообщать об устаревшем пароле через ...** и в раскрывающемся списке выберите время, по истечении которого приложение будет показывать уведомление о том, что пароль устарел.
   - В раскрывающемся списке **Рекомендовать изменить пароль через ...** выберите время, по истечении которого приложение будет рекомендовать вам изменить пароль.
   - Установите флажок **Сообщать, если минимально разрешенная длина пароля в настройках Windows менее ...**, если вы хотите, чтобы приложение проверяло, какая минимальная длина пароля задана в политике Windows для этого устройства. Если длина пароля в политике Windows меньше указанного здесь значения, Kaspersky Small Office Security будет показывать уведомление о том, что вам надо увеличить минимальную длину пароля в политике Windows.

Основные возможности приложения

В этом разделе вы можете прочитать о том, как выполнить базовую настройку приложения, включающую настройку уведомлений и интерфейса, а также о том, как исправлять возникающие проблемы безопасности.

Анализ состояния защиты компьютера и устранение проблем безопасности

О появлении проблем в защите компьютера сигнализирует индикатор, расположенный в верхней части главного окна приложения. Зеленый цвет индикатора означает, что компьютер защищен, желтый цвет свидетельствует о наличии проблем в защите, красный – о серьезной угрозе безопасности компьютера. Проблемы и угрозы безопасности рекомендуется немедленно устранять.

Наиболее важные рекомендации отображаются в главном окне приложения. Каждая карточка рекомендаций содержит категорию проблемы.

Рекомендации по оценке защиты помогут вам оценить и улучшить защиту вашего компьютера, проведя вас через ключевые области безопасности. Из карточки рекомендаций Оценка защиты вы перейдете на страницу, где сможете выбрать темы защиты, которые вас больше всего интересуют, или отредактировать список тем. На следующем шаге вы увидите выбранные вами темы, а также статус соответствующих функций продукта. Функциональность, которая уже настроена, будет отображаться в зеленых блоках, а функциональность, которая еще не настроена, будет отображаться в серых блоках. Это упрощает просмотр областей безопасности, требующих внимания, и настройку недостающих функций.

Чтобы просмотреть полный список рекомендаций, откройте окно **Центр уведомлений** нажатием на кнопку **Подробнее**. В этом окне приведена подробная информация о состоянии защиты компьютера и предложены варианты действий для устранения проблем и угроз.

Проблемы в защите сгруппированы по категориям, к которым они относятся. Для каждой проблемы приведены действия, которые вы можете предпринять, чтобы решить проблему.

В разделе **Статус** отображается информация о состоянии защиты компьютера и статус лицензии. В случае обнаружения проблем, которые требуют исправления, напротив уведомления отображается кнопка **Исправить**, при нажатии на которую можно устранить возникшие проблемы безопасности.

В разделе **Советы** отображаются уведомления о действиях, которые рекомендуется выполнить для оптимизации работы приложения и более эффективного ее использования.

В разделе **Новости** отображаются новости кибербезопасности.

При нажатии на кнопку **Показать N игнорируемых советов** отображаются уведомления, к которым было применено действие **Игнорировать**. Проигнорированные уведомления не влияют на цвет индикатора защиты в главном окне приложения.

Как исправить проблемы безопасности компьютера

Чтобы исправить проблемы безопасности компьютера:

1. Откройте главное окно приложения.
2. По ссылке **Подробнее** в верхней части главного окна перейдите в окно **Центр уведомлений**.
3. Перейдите в раздел **Статус**. В этом разделе отображаются проблемы, связанные с безопасностью компьютера.
   - Выберите в списке проблему и нажмите на кнопку действия, например **Исправить**.
   - В раскрывающемся списке выберите вариант **Игнорировать**, если вы не хотите сейчас исправлять эту проблему. Вы можете просмотреть список проигнорированных уведомлений позднее, нажав на кнопку **Показать <N> игнорируемых уведомлений**.
4. Перейдите в раздел **Советы**. В этом разделе отображаются рекомендации, которые не обязательны к выполнению, однако помогут вам лучше оптимизировать работу с приложением и защиту компьютера.
   a. Выберите совет в списке.
   b. Нажмите на кнопку напротив предлагаемого действия, например, напротив совета **Хотите заблокировать навязчивые баннеры?** нажмите на кнопку **Включить**.

История действий приложения и подробный отчет

В главном окне вы можете посмотреть краткий обзор действий приложения за все время работы. Эта информация поможет вам лучше понимать, как именно приложение защищает ваше устройство и данные.

Чтобы посмотреть историю действий приложения:

1. Откройте главное окно приложения.

   В разделе **Главная** в блоке **История** отображается краткая история действий приложения.
2. Чтобы посмотреть подробную историю действий приложения, нажмите на кнопку **Посмотреть все**.

   Откроется окно с подробным описанием действий приложения и времени возникновения событий.
3. Чтобы посмотреть подробный отчет о работе приложения, нажмите на кнопку **Посмотреть отчет**.

   Будет выполнен переход в окно **Отчеты**.

Также вы можете посмотреть подробный отчет по кнопке **Отчеты** в разделе **Безопасность**. В окне **Отчеты** данные представлены в табличном виде. Для удобства просмотра отчетов вы можете выбирать различные варианты фильтрации записей.

Как настроить интерфейс приложения

Этот раздел содержит информацию о том, как настроить интерфейс приложения.

Как настроить уведомления приложения

Уведомления приложения, появляющиеся в области уведомлений панели задач, информируют о событиях, происходящих в процессе работы приложения и требующих вашего внимания. В зависимости от степени важности события уведомления могут быть следующих типов:

- *Критические* – информируют о событиях, имеющих первостепенную важность для обеспечения безопасности компьютера (например, об обнаружении вредоносного объекта или опасной активности в операционной системе). Окна критических уведомлений и всплывающих сообщений – красные.

- *Важные* – информируют о событиях, потенциально важных для обеспечения безопасности компьютера (например, об обнаружении возможно зараженного объекта или подозрительной активности в операционной системе). Окна важных уведомлений и всплывающих сообщений – желтые.

- *Информационные* – информируют о событиях, не имеющих первостепенной важности для обеспечения безопасности компьютера. Окна информационных уведомлений и всплывающих сообщений – зеленые. При появлении на экране уведомления следует выбрать один из предложенных в уведомлении вариантов действия. Оптимальный вариант – тот, который рекомендован специалистами "Лаборатории Касперского" по умолчанию. Уведомление может быть закрыто автоматически при перезагрузке компьютера, закрытии Kaspersky Small Office Security или в режиме Connected Standby в Windows 8. Уведомления компонента Предотвращение вторжений автоматически закрываются по истечении 500 секунд. Уведомления о запуске приложения автоматически закрываются по истечении 1 часа. При автоматическом закрытии уведомления Kaspersky Small Office Security выполнит действие, рекомендованное по умолчанию.

По ссылкам ниже вы можете прочитать о том, как настроить уведомления приложения.

Как настроить получение уведомлений

Чтобы создать правила уведомлений:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки интерфейса**.
4. В блоке **Уведомления** по ссылке **Настроить уведомления** перейдите в окно настройки уведомлений.
5. Слева в списке выберите компонент.

   В правой части окна отобразится список событий, которые могут произойти во время работы этого компонента.
6. Выберите в списке событие и установите флажки:

   - **Сохранять в локальном отчете**. При возникновении события информация о нем будет занесена в отчет, который хранится на локальном компьютере.
   - **Уведомлять на экране**. При возникновении события всплывающее уведомление отображается над значком приложения в области уведомлений панели задач.

   С помощью раскрывающегося списка в нижнем левом углу вы можете указать, какие уведомления вы хотите сохранять в локальный отчет:

   - **По умолчанию**. При выборе этого варианта в отчет сохраняются события на усмотрение специалистов "Лаборатории Касперского".
   - **Вручную**. Этот вариант выбирается автоматически, если вы настраиваете сохранение событий в отчет вручную.
   - **Критические**. При выборе этого варианта в отчете будут сохраняться события с уровнем важности **Критические события** (включая *События, связанные со сбоями в работе приложения* для элемента **Аудит системы** и компонента **Предотвращение вторжений**).
   - **Важные**. При выборе этого варианта в отчет будут сохраняться **Критические события** (включая *События, связанные со сбоями в работе приложения* для элемента **Аудит системы** и компонента **Предотвращение вторжений**) и **Предупреждения**.
   - **Информационные**. При выборе этого варианта в отчет будут сохраняться все события.

Уведомления обо всех изменениях, связанных с событием **Приложение работает в соответствии с местным законодательством и использует локальную инфраструктуру**, всегда отображаются на экране в области панели задач. Снятие флажка не влияет на изменение настройки.

[Как настроить получение информационных сообщений и специальных предложений от "Лаборатории Касперского"]

Если вы хотите получать информационные сообщения и специальные предложения от "Лаборатории Касперского":

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Перейдите в раздел **Настройки интерфейса**.
4. В блоке **Информационные материалы** выполните одно из следующих действий:

   - Установите флажок **Получать информационные и рекламные сообщения "Лаборатории Касперского"**, если вы хотите получать информацию о последних случаях мошенничества, взломах баз данных и масштабных утечках персональных данных.
   - Установите флажок **Отображать информацию о специальных предложениях на сайтах**, если вы хотите получать наиболее выгодные предложения при посещении сайтов "Лаборатории Касперского".
   - Установите флажок **Получать информационные и рекламные сообщения по истечении срока действия лицензии**, если вы хотите получать информационные сообщения от "Лаборатории Касперского" после истечения срока действия лицензии.

Как настроить сопровождение уведомлений звуковыми сигналами

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Перейдите в раздел **Настройки интерфейса**.
4. В блоке **Уведомления** установите флажок **Сопровождать уведомления звуковыми сигналами**.

   Изменить установленный по умолчанию звуковой сигнал на "визг свиньи" можно в окне **О приложении** с помощью сочетания клавиш **IDKFA**.

На операционной системе Microsoft Windows 10 звуковое сопровождение уведомлений не работает.

Как сменить тему оформления приложения

Смена темы оформления приложения доступна не во всех регионах.

Чтобы сменить тему оформления:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки интерфейса**.
4. В блоке **Тема оформления** установите флажок **Использовать альтернативную тему оформления**, если вы хотите использовать альтернативную тему оформления. По ссылке **Выбрать** и укажите путь к zip-архиву или папке, в котором содержатся файлы с альтернативной темой оформления.

Тема оформления будет применена после перезапуска приложения.

Как настроить значок приложения

В этом разделе вы можете прочитать о том, как настроить значок приложения на Рабочем столе и в области уведомлений.

Как сменить значок приложения

Чтобы сменить значок приложения:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки интерфейса**.
4. В разделе **Значок приложения** выберите один из вариантов.

   - **Стандартный значок**. При выборе этого варианта на рабочем столе и в области уведомлений будет отображаться стандартный значок приложения.
   - **Мидори Кума**. При выборе этого варианта на рабочем столе и в области уведомлений будет отображаться значок с изображением медведя Мидори Кума.

Если вы хотите вернуть традиционный значок приложения в виде буквы "K", это можно сделать в окне **О приложении** с помощью сочетания клавиш **IDDQD**. Чтобы изменения вступили в силу, требуется перезагрузить компьютер.

> В Windows 10 вам необходимо вручную **перезагрузить** компьютер, чтобы изменения вступили в силу. Если вы выключите/включите компьютер, изменения не будут применены.

Как настроить изменение значка в области уведомлений в зависимости от статуса защиты

Чтобы настроить изменение значка Kaspersky Small Office Security в области уведомлений в зависимости от статуса приложения:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки интерфейса**.
4. В блоке **Отображать состояние приложения в области уведомлений** выберите статус и установите флажок.

При переходе приложения в состояние, соответствующее выбранному статусу, значок приложения в области уведомлений будет меняться.

Как защитить доступ к управлению приложением с помощью пароля

На одном компьютере могут работать несколько пользователей с разным опытом и уровнем компьютерной грамотности. Неограниченный доступ разных пользователей к управлению приложением и его настройке может привести к снижению уровня защищенности компьютера.

Чтобы ограничить доступ к приложению, вы можете задать пароль администратора с именем `KLAdmin`. Этот пользователь имеет неограниченные права на управление и изменение настроек приложения, а также на назначение прав доступа к приложению другим пользователям. После того как вы создали пароль для `KLAdmin`, вы можете назначить разным пользователям или группам пользователей права доступа к приложению.

Чтобы создать пароль администратора `KLAdmin`:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки интерфейса**.
4. Переведите переключатель **Защита паролем** в положение **Вкл**.

5. В открывшемся окне заполните поля ввода **Имя пользователя** (рекомендованное значение KLAdmin), **Введите пароль** и **Подтвердите пароль**.

   Рекомендации по созданию надежного пароля:

   - Длина пароля: не менее 8 и не более 128 символов.
   - Пароль имеет хотя бы одну цифру.
   - Пароль содержит как прописные, так и строчные буквы.
   - Пароль должен содержать хотя бы один специальный символ (например: ! @ # $ % ^ & *).

6. Нажмите на кнопку **Сохранить**.

Забытый пароль восстановить нельзя. Если пароль забыт, для восстановления доступа к настройкам приложения потребуется обращение в Службу технической поддержки.

Пользователь `KLAdmin` может назначать разрешения для следующих пользователей и групп пользователей:

- Группа пользователей `Все`. В эту группу входят все пользователи операционной системы. Если вы выдаете разрешение на какое-либо действие для этой группы, то пользователям, входящим в эту группу, всегда будет разрешено выполнение этого действия, даже если это действие запрещено для конкретного пользователя или группы пользователей, входящих в группу `Все`. По умолчанию для группы `Все` запрещены все действия.
- `<пользователь системы>`. По умолчанию выбранному пользователю запрещены все действия. Это значит, что при попытке выполнения запрещенного действия будет запрошен ввод пароля для учетной записи `KLAdmin`.

Как добавить пользователя или группу пользователей

1. В разделе **Настройки интерфейса** в блоке **Отображать состояние приложения в области уведомлений** нажмите на кнопку **Добавить**.

   Откроется окно **Создание разрешений для пользователя или группы**.

2. По ссылке **Выбрать пользователя или группу** перейдите в окно выбора пользователя или группы пользователей операционной системы.
3. В поле ввода имени объекта укажите имя пользователя или группы пользователей (например, `Administrator`).
4. Нажмите на кнопку **OK**.
5. В окне **Создание разрешений для пользователя или группы** в блоке **Разрешения** установите флажки напротив действий, которые вы хотите разрешить этому пользователю или группе пользователей.

Как изменить разрешения для пользователя или группы пользователей

В разделе **Настройки интерфейса** в блоке **Отображать состояние приложения в области уведомлений** выберите пользователя или группу пользователей в списке и нажмите на кнопку **Изменить**.

Как разрешить какое-либо действие отдельному пользователю или группе пользователей

1. Перейдите в окно **Создание разрешений для пользователя или группы** для группы `Все` и снимите флажок, разрешающий это действие, если он установлен.
2. Перейдите в окно **Создание разрешений для пользователя или группы** для выбранного пользователя и установите флажок, разрешающий это действие.

Как запретить какое-либо действие отдельному пользователю или группе пользователей

1. Перейдите в окно **Создание разрешений для пользователя или группы** для группы `Все` и снимите флажок, разрешающий это действие, если он установлен.
2. Перейдите в окно **Создание разрешений для пользователя или группы** для выбранного пользователя и снимите флажок, разрешающий это действие.

При попытке выполнить какое-либо действие из списка в окне **Создание разрешений для пользователя или группы**, приложение запросит ввод пароля. В окне ввода пароля укажите имя пользователя и пароль от учетной записи текущего пользователя. Действие будет выполнено, если у указанной учетной записи есть разрешение на выполнение этого действия. В окне ввода пароля вы можете указать время, в течение которого пароль не будет запрашиваться повторно.

В окне ввода пароля язык ввода можно поменять только с помощью одновременного нажатия клавиш **ALT+SHIFT**. При использовании других комбинаций клавиш, даже если они установлены в операционной системе, смена языка ввода не происходит.

Как восстановить стандартные настройки приложения

Вы в любое время можете восстановить настройки приложения, рекомендуемые "Лабораторией Касперского". В результате восстановления настроек для всех компонентов защиты будет установлен уровень безопасности **Оптимальный**.

Чтобы восстановить стандартные настройки приложения:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Выберите раздел **Управление настройками**.
4. По ссылке **Восстановить** запустите мастер восстановления настроек.
5. Нажмите на кнопку **Далее**.

   В окне мастера отобразится процесс восстановления настроек работы приложения до тех, которые заданы специалистами "Лаборатории Касперского" по умолчанию.
6. После того как процесс восстановления стандартных настроек работы приложения будет завершен, нажмите на кнопку **Готово**.

Как применить настройки приложения на другом компьютере

Настроив приложение Kaspersky Small Office Security определенным образом, вы можете применить эти настройки на другом компьютере. В результате на обоих компьютерах приложение Kaspersky Small Office Security будет настроено одинаково.

Настройки приложения Kaspersky Small Office Security сохраняются в конфигурационном файле, который вы можете перенести с одного компьютера на другой.

Перенос настроек приложения Kaspersky Small Office Security с одного компьютера на другой производится в три этапа:

1. Сохранение настроек приложения Kaspersky Small Office Security в конфигурационном файле.
2. Перенос конфигурационного файла на другой компьютер (например, по электронной почте или на внешнем диске).
3. Импорт настроек из конфигурационного файла в приложение Kaspersky Small Office Security, установленное на другом компьютере.

Как экспортировать настройки

Чтобы экспортировать настройки Kaspersky Small Office Security:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. В окне **Настройка** выберите раздел **Управление настройками**.
4. Выберите элемент **Экспортировать**.
5. Откроется окно **Сохранение**.
6. Задайте имя конфигурационного файла и нажмите на кнопку **Сохранить**.

   Настройки приложения будут сохранены в конфигурационный файл.

Вы также можете экспортировать настройки приложения Kaspersky Small Office Security при помощи командной строки, используя команду: `avp.com EXPORT <имя_файла>`.

Адреса сайтов, которые вы добавили в Безопасные платежи, сохраняются при экспортировании настроек приложения Kaspersky Small Office Security только для текущего пользователя. При импортировании настроек на другом компьютере адреса сайтов не сохраняются.

Как импортировать настройки

Чтобы импортировать настройки в приложение Kaspersky Small Office Security, установленное на другом компьютере:

1. Откройте главное окно приложения Kaspersky Small Office Security, установленного на другом компьютере.
2. Нажмите на кнопку в нижней части окна.

   Откроется окно **Настройка**.
3. В окне **Настройка** выберите раздел **Управление настройками**.
4. Выберите элемент **Импортировать**.

   Откроется окно **Открыть**.
5. Укажите конфигурационный файл и нажмите на кнопку **Открыть**.

   Настройки будут импортированы в приложение Kaspersky Small Office Security, установленное на другом компьютере.

Как приостановить и возобновить защиту компьютера

Приостановка защиты означает выключение на некоторое время всех ее компонентов.

Во время приостановки защиты или выключения приложения Kaspersky Small Office Security действует функция контроля активности приложений, запущенных на вашем компьютере. Информация о результатах контроля активности приложений сохраняется в операционной системе. При следующем запуске или возобновлении защиты приложение Kaspersky Small Office Security использует эту информацию для защиты вашего компьютера от вредоносных действий, которые могли быть выполнены во время приостановки защиты или выключения приложения Kaspersky Small Office Security. Хранение информации о результатах контроля активности приложений не ограничено по времени. Эта информация удаляется в случае удаления приложения Kaspersky Small Office Security с вашего компьютера.

Чтобы приостановить защиту компьютера:

1. В контекстном меню значка Kaspersky Small Office Security в области уведомлений панели задач выберите пункт **Приостановить защиту**.

   Откроется окно **Приостановка защиты**.

2. В окне **Приостановка защиты** выберите период, по истечении которого защита будет включена:

   - **Приостановить на** – защита будет включена через интервал, выбранный в раскрывающемся списке ниже.
   - **Приостановить до перезапуска приложения** – защита будет включена после перезапуска приложения или перезагрузки операционной системы (при условии, что включен автоматический запуск приложения).
   - **Приостановить** – защита будет включена тогда, когда вы решите возобновить ее.

3. Нажмите на кнопку **Приостановить защиту** и подтвердите действие в открывшемся окне.

Как возобновить защиту компьютера

Чтобы возобновить защиту компьютера,

выберите пункт **Возобновить защиту** в контекстном меню значка Kaspersky Small Office Security в области уведомлений панели задач.

Поиск по функциональности приложения

Поиск по функциональности приложения доступен в заголовке главного окна. При нажатии на поле ввода вы будете перенаправлены в окно **Результаты поиска**.

Приложение осуществляет поиск:

- по прямому совпадению с введенной вами строкой, опечатки не учитываются.
- по всем наименованиям функций и настроек.

Результаты поиска выводятся в виде карточек, при нажатии на которые вы попадаете в соответствующую область интерфейса приложения.

Безопасность

Современные киберпреступники постоянно совершенствуются в попытках взломать ваши устройства. Каждый день появляются новые виды фишинга, приложения-вымогатели и другие способы мошенничества в интернете. Мы создали приложение Kaspersky Small Office Security, чтобы вы оставались на шаг впереди современных угроз. Посмотрите, какие инструменты защиты входят в него.

Чтобы узнать больше о технологиях кибербезопасности, используемых в приложении, нажмите на ссылку **Наши кибертехнологии** вверху страницы **Безопасность**.

Проверка компьютера

Во время проверки приложение ищет зараженные файлы и вредоносные приложения. Существует несколько типов сканирования, которые различаются по продолжительности и объему поиска. Вы можете приостановить, возобновить или остановить все типы проверок, за исключением Фоновой проверки.

- Полная проверка. Проверка всех областей компьютера. Требует много времени.
- Быстрая проверка. Проверка объектов, которые загружаются при старте операционной системы, а также системной памяти и загрузочных файлов. Не требует много времени.
- Выборочная проверка. Проверка выбранного файла или папки.
- Проверка внешних дисков. Проверка внешних дисков, например, жестких дисков и USB-флешек, подключенных к компьютеру.
- Проверка из контекстного меню. Проверка файлов через контекстное меню.
- Фоновая проверка. Проверка системной памяти, системного раздела, загрузочных секторов и объектов автозапуска, а также поиск руткитов.

  Эта функциональность недоступна, если приложение Kaspersky Small Office Security установлено на файловом сервере.

- Поиск уязвимостей в приложениях. Проверка компьютера на наличие уязвимостей в приложениях, через которые способны проникнуть вредоносные приложения.

После установки приложения мы рекомендуем выполнить полную проверку компьютера.

Как запустить полную проверку

Во время полной проверки по умолчанию приложение проверяет следующие объекты:

- системная память;
- объекты, которые загружаются при старте операционной системы;
- системное резервное хранилище;
- жесткие и внешние диски.

Рекомендуется выполнить полную проверку сразу после установки приложения на компьютер.

Чтобы запустить полную проверку:

1. Откройте главное окно приложения и перейдите в раздел **Безопасность**.
2. В блоке **Проверка** нажмите на кнопку **Выбрать проверку**.
   Откроется окно **Проверка**.
3. В окне **Проверка** выберите раздел **Полная проверка**.
4. В раскрывающемся списке рядом с кнопкой **Запустить** выберите действие по окончании проверки.
5. Нажмите на кнопку **Запустить**.

   Приложение начнет полную проверку компьютера.

Как запустить выборочную проверку

С помощью выборочной проверки вы можете проверить на вирусы и другие приложения, представляющие угрозу, файл, папку или диск.

Чтобы запустить выборочную проверку:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Безопасность**.
3. В блоке **Проверка** нажмите на кнопку **Выбрать проверку**.
   Откроется окно **Проверка**.
4. В окне **Проверка** выберите раздел **Выборочная проверка**.
5. Нажмите на кнопку **Выбрать** и укажите объект в открывшемся окне выбора файла или папки.
6. Нажмите на кнопку **Запустить**.

Как запустить быструю проверку

Во время быстрой проверки приложение по умолчанию проверяет следующие объекты:

- объекты, которые загружаются при старте операционной системы;
- системная память;
- загрузочные сектора диска.

Чтобы запустить быструю проверку:

1. Откройте главное окно приложения и выполните одно из следующих действий:
   - Перейдите в раздел **Главная** и нажмите на кнопку **Быстрая проверка**.
   - Перейдите в раздел **Безопасность**.
     1. В блоке **Проверка** нажмите на кнопку **Выбрать проверку**.
     2. Откроется окно **Проверка**.
     3. В окне **Проверка** выберите раздел **Быстрая проверка**.
     4. В разделе **Быстрая проверка** нажмите на кнопку **Запустить**.

Приложение начнет быструю проверку компьютера.

Как запустить проверку внешних дисков

Внешние диски, которые вы подключаете к компьютеру, могут содержать вирусы и другие приложения, представляющие угрозу. Приложение Kaspersky Small Office Security проверяет внешние диски, чтобы не допустить заражения вашего компьютера. Вы можете запускать проверку внешних дисков вручную или автоматически при подключении внешнего диска к компьютеру. По умолчанию автоматическая проверка внешних дисков включена.

Чтобы проверить внешний диск вручную:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Безопасность**.
3. В блоке **Проверка** нажмите на кнопку **Выбрать проверку**.

   Откроется окно **Проверка**.
4. В окне **Проверка** выберите раздел **Проверка внешних дисков**.

5. Перейдите в раздел Настройки проверки внешних дисков и выберите один из следующих вариантов:

   - **Быстрая проверка** (выбрано по умолчанию)

     Если выбран этот вариант, то после подключения внешнего устройства приложение Kaspersky Small Office Security проверяет только файлы определенных форматов, наиболее подверженные заражению, находящиеся в корневой папке подключенного устройства.

   - **Подробная проверка**

     Если вы выберете этот вариант, приложение Kaspersky Small Office Security будет проверять все файлы, расположенные во всех папках внешнего устройства.

6. Перейдите в раздел **Проверка внешних дисков**. В раскрывающемся списке выберите внешнее устройство (отображается в виде буквы латинского алфавита) и нажмите на кнопку **Запустить**.

Приложение начнет проверку подключенного устройства.

Как запустить проверку файла или папки из контекстного меню

Чтобы запустить проверку файла или папки из контекстного меню:

1. Правой клавишей мыши нажмите на файле или папке, которые нужно проверить.

2. В открывшемся контекстном меню выберите пункт **Проверить на вирусы**.

Приложение начнет проверку выбранного файла или папки.

В операционной системе Microsoft Windows 11 контекстное меню объекта нужно развернуть, чтобы в нем отображались команды приложения.

Как включить или выключить фоновую проверку

Фоновая проверка – это автоматический режим проверки без показа уведомлений. Такая проверка требует меньше ресурсов компьютера, чем другие виды проверок (например, полная проверка). В этом режиме приложение проверяет системную память, системные разделы, загрузочные секторы и объекты автозапуска, а также выполняет поиск руткитов.

Эта функциональность недоступна, если приложение Kaspersky Small Office Security установлено на файловом сервере.

Фоновая проверка запускается в следующих случаях:

- после обновления баз и модулей приложения;
- через 30 минут после запуска приложения;

- каждые шесть часов;
- если компьютер не используется в течение пяти и более минут (запущена экранная заставка).

Фоновая проверка прерывается при выполнении любого из следующих условий:

- Компьютер перешел в активный режим.
- Компьютер (ноутбук) перешел в режим питания от батареи.

Если фоновая проверка не выполнялась более десяти дней, проверка не прерывается. При выполнении фоновой проверки приложение не проверяет файлы, содержимое которых расположено в облачном хранилище OneDrive.

Чтобы включить или выключить фоновую проверку:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Безопасность**.
3. В блоке **Проверка** нажмите на кнопку **Выбрать проверку**.

   Откроется окно **Проверка**.
4. Нажмите на значок в блоке **Фоновая проверка**.

   Откроется окно **Настройки фоновой проверки**.
5. В окне **Настройки фоновой проверки** переведите переключать в положение **Вкл** или **Выкл**.

Как создать расписание проверки

Чтобы создать расписание проверки:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Безопасность**.
3. В блоке **Проверка** нажмите на кнопку **Выбрать проверку**.

   Откроется окно **Проверка**.
4. В окне **Проверка** выберите тип проверки и нажмите на значок .
5. В открывшемся окне по ссылке **Расписание проверки** перейдите в окно **Расписание проверки**.
6. В окне **Расписание проверки** в списке **Запускать проверку** выберите период, например **По дням**, и укажите время запуска проверки.

Создание расписания проверки недоступно для проверки из контекстного меню и фоновой проверки.

Как выполнить поиск уязвимостей в приложениях, установленных на вашем компьютере

В приложениях, установленных на вашем компьютере, могут быть уязвимости, через которые способны проникнуть вредоносные приложения. Проверка вашего компьютера поможет найти эти уязвимости и предотвратить заражение компьютера.

Приложение Kaspersky Small Office Security не обнаруживает уязвимости в OpenSSL приложениях.

Чтобы запустить поиск уязвимостей в приложениях:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Безопасность**.
3. В блоке **Проверка** нажмите на кнопку **Выбрать проверку**.

   Откроется окно **Проверка**.
4. В окне **Проверка** выберите раздел **Поиск уязвимостей в приложениях**.
5. Нажмите на кнопку **Запустить**.

Приложение начнет проверку вашего компьютера на наличие уязвимостей в приложениях.

Как исключить файл, папку или тип угрозы из проверки

Чтобы исключить файл, папку или тип угрозы из проверки:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки безопасности** → **Исключения и действия с найденными объектами**.
4. По ссылке **Настроить исключения** перейдите в окно **Исключения**.
5. Нажмите на кнопку **Добавить**.

6. Добавьте исключение одним из следующих способов:

   - Нажмите **Обзор** и выберите папку или файл, который вы хотите исключить из проверки. Нажмите на кнопку **Выбрать**.
   - В поле **Файл или папка** введите полное имя или маску имени файла или папки вручную.
   - В поле **Тип обнаруживаемого объекта** введите полное имя или маску имени типа угрозы по классификации детектируемых объектов "Лаборатории Касперского".
   - Заполните оба поля: **Файл или папка** и **Тип обнаруживаемого объекта**, чтобы приложение не проверяло в выбранном файле или папке указанный тип угрозы.
   - В поле **Хеш файла** укажите хеш сумму, если вы хотите, чтобы файлы исключались из проверки по хеш сумме.

7. Снимите флажки с компонентов защиты, для которых не будет действовать правило исключения. При желании укажите свой комментарий.
8. Выберите статус правила **Активно** и нажмите на кнопку **Добавить**.

Указанные объекты будут исключены из проверки.

Подробнее о настройках в окне Исключения и действия с найденными объектами

Проверка файлов в облачном хранилище OneDrive

На операционной системе Windows 10 RS3 и выше Kaspersky Small Office Security не проверяет файлы в облачном хранилище OneDrive. Если приложение обнаруживает такие файлы во время проверки, она показывает уведомление о том, что файлы в облачном хранилище не были проверены.

Следующие компоненты не проверяют файлы в облачном хранилище OneDrive:

- Полная проверка;
- Выборочная проверка;
- Быстрая проверка;
- Фоновая проверка.

Отчет о работе Kaspersky Small Office Security содержит список файлов в облачном хранилище OneDrive, пропущенных во время проверки.

Файлы, загруженные из облачного хранилища OneDrive на локальный компьютер, проверяются компонентами постоянной защиты. Если проверка файла происходит в отложенном режиме и файл был загружен обратно в облачное хранилище OneDrive до начала проверки, такой файл может быть пропущен при проверке.

При запуске приложений и скриптов компоненты Предотвращение вторжений и Мониторинг активности скачивают приложения из облачного хранилища OneDrive на локальный компьютер для проверки.

Чтобы файлы OneDrive отображались в проводнике, включите функцию Файлы по запросу в клиентском приложении OneDrive. При наличии подключения к интернету вы сможете использовать их как любые другие файлы на компьютере.

Обновление антивирусных баз и модулей приложения

Этот раздел содержит информацию об обновлении баз и модулей приложения.

Об обновлении антивирусных баз и модулей приложения

Пакет установки приложения включает в себя базы и модули приложения. С помощью этих баз:

- Приложение обнаруживает большинство угроз с помощью Kaspersky Security Network, для чего требуется подключение к интернету.
- Приложение обнаруживает рекламные приложения, приложения автодозвона и другие легальные приложения, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

Для полной защиты рекомендуется обновить антивирусные базы и модули приложения сразу после установки приложения.

Обновление баз и модулей приложения выполняется поэтапно:

1. Приложение запускает обновление баз и модулей приложения согласно указанным настройкам: автоматически, по расписанию или по вашему требованию. Приложения обращается к источнику обновлений, где хранится пакет обновлений антивирусных баз и модулей приложения. Для завершения установки пакета обновлений для модулей приложения потребуется перезагрузить компьютер.
2. Приложение сравнивает имеющиеся базы с базами, находящимися в источнике обновлений. Если базы отличаются, приложение скачивает отсутствующие части баз.

После этого приложение использует обновленные базы и модули приложения для проверки компьютера на вирусы и другие приложения, представляющие угрозу.

Источники обновлений

Вы можете использовать следующие источники обновлений:

- Серверы обновлений "Лаборатории Касперского".
- HTTP или FTP-сервер.
- Сетевая папка.

Особенности обновления антивирусных баз и модулей приложения

Обновление антивирусных баз и модулей приложения имеет следующие особенности и ограничения:

- Антивирусные базы устаревают по истечении одного дня и сильно устаревают по истечении семи дней.
- Для скачивания пакета обновлений с серверов обновлений "Лаборатории Касперского" требуется соединение с интернетом.
- Обновление антивирусных баз и модулей приложения недоступно в следующих случаях:
  - Истек срок действия лицензии, и не предусмотрен льготный период или режим ограниченной функциональности.
  - Используется высокоскоростное мобильное подключение к интернету. Это ограничение действует при работе в операционной системе Microsoft Windows 8 и выше, если выбран автоматический режим обновления или режим обновления по расписанию и установлено ограничение трафика при высокоскоростном мобильном подключении. Чтобы в этом случае выполнялось обновление антивирусных баз и модулей приложения, требуется снять флажок **Ограничивать трафик при лимитном подключении** в окне **Настройка → Настройки безопасности → Расширенные настройки → Настройки сети**.
  - Приложение используется по подписке от поставщика услуг, и вы приостановили подписку на сайте поставщика услуг.

Установка пакета исправлений

При получении пакета исправлений (патча) приложение устанавливает его автоматически. Для завершения установки пакета исправлений требуется перезагрузить компьютер. До перезагрузки компьютера значок приложения в области уведомлений имеет красный цвет, а в окне **Центр уведомлений** приложения отображается предложение перезагрузить компьютер.

Как запустить обновление баз и модулей приложения

По умолчанию базы и модули приложения обновляются в автоматическом режиме. Вам не нужно выполнять никаких действий. Если автоматическое обновление выключено, вы можете обновить базы и модули приложения вручную.

Чтобы запустить обновление баз и модулей приложения:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Безопасность**.
3. В блоке **Обновление антивирусных баз** нажмите на кнопку **Обновить**.

Предотвращение вторжений

С помощью приложения Kaspersky Small Office Security вы сможете снизить риски, связанные с использованием неизвестных приложений (например, риски заражения компьютера вирусами и другими приложениями, представляющими угрозу).

В состав приложения Kaspersky Small Office Security входят компоненты и инструменты, позволяющие проверить репутацию приложения и контролировать активность приложения на вашем компьютере.

О Предотвращении вторжений

Компонент Предотвращение вторжений предотвращает выполнение приложениями опасных для операционной системы действий, а также обеспечивает контроль доступа к ресурсам операционной системы (в том числе файловым ресурсам, расположенным на удаленных компьютерах) и вашим персональным данным.

Предотвращение вторжений отслеживает действия, которые совершают в операционной системе приложения, установленные на компьютере, и регулирует их на основании правил. Эти правила регламентируют подозрительную активность приложений, в том числе доступ приложений к защищаемым ресурсам (например, к файлам, папкам, ключам реестра, сетевым адресам).

При работе на 64-разрядных операционных системах недоступны для настройки права приложений на выполнение следующих действий:

- прямой доступ к физической памяти;
- управление драйверами принтера;
- создание службы;
- открытие службы для чтения;
- открытие службы для изменения;
- изменение конфигурации службы;
- управление службой;
- запуск службы;
- удаление службы;
- доступ к внутренним данным браузера;
- доступ к критическим объектам операционной системы;
- доступ к хранилищу паролей;
- установка прав отладчика;

- использование программных интерфейсов операционной системы;
- использование программных интерфейсов операционной системы (DNS);
- использование программных интерфейсов других приложений;
- изменение системных модулей (KnownDlls);
- запуск драйвера.

При работе на 64-разрядной Microsoft Windows 8 и Microsoft Windows 10 дополнительно недоступны для настройки права приложений на выполнение следующих действий:

- отправка оконных сообщений другим процессам;
- подозрительные операции;
- установка клавиатурных шпионов;
- перехват входящих событий потока;
- создание снимков экрана.

Сетевую активность приложений контролирует компонент Сетевой экран.

При первом запуске приложения на компьютере Предотвращение вторжений проверяет безопасность этого приложения и помещает в одну из групп ("Доверенные", "Недоверенные", "Сильные ограничения" или "Слабые ограничения"). Группа определяет правила, которые приложение Kaspersky Small Office Security применяет для контроля активности этого приложения.

Приложение Kaspersky Small Office Security помещает приложения в группы доверия ("Доверенные", "Недоверенные", "Сильные ограничения" или "Слабые ограничения"), только если включен компонент Предотвращение вторжений или Сетевой экран, а также когда включены оба эти компонента. Если оба эти компонента выключены, функциональность распределения приложений по группам доверия не работает.

Вы можете изменить правила контроля действий приложения вручную.

Правила, которые вы создаете для приложения, наследуются дочерними приложениями. Например, если вы запретили любую сетевую активность приложению cmd.exe, этот запрет будет распространятся на приложение notepad.exe, если оно было запущено с помощью cmd.exe. При опосредованном запуске приложения (если приложение не является дочерним по отношению к приложению, из которого оно запускается), правила унаследованы не будут.

Как изменить настройки Предотвращения вторжений

Чтобы изменить настройки Предотвращения вторжений:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.
   Откроется окно **Настройка**.
3. Выберите раздел **Настройки безопасности**.

4. Выберите компонент **Предотвращение вторжений**.

5. В окне **Настройки Предотвращения вторжений** по ссылке **Управление приложениями** перейдите в окно **Управление приложениями**.

6. Выберите нужное приложение в списке и двойным щелчком мыши по названию приложения откройте окно **Правила приложения**.

7. Чтобы настроить правила доступа приложения к ресурсам операционной системы, выполните следующие действия:

   a. На закладке **Файлы и системный реестр** выберите нужную категорию ресурсов.

   b. В графе с возможным действием над ресурсом (**Чтение**, **Запись**, **Удаление**, или **Создание**) нажатием на значок откройте меню и выберите в нем нужное значение (**Наследовать**, **Разрешить**, **Спрашивать пользователя**, или **Запретить**).

8. Чтобы настроить права приложения на выполнение различных действий в операционной системе, выполните следующие действия:

   a. На закладке **Права** выберите нужную категорию прав.

   b. В графе **Действие** нажатием на значок откройте меню и выберите в нем нужное значение (**Наследовать**, **Разрешить**, **Спрашивать пользователя** или **Запретить**).

9. Чтобы настроить права приложения на выполнение различных действий в сети, выполните следующие действия:

   a. На закладке **Сетевые правила** нажмите на кнопку **Добавить**.

      Откроется окно **Сетевое правило**.

   b. В открывшемся окне задайте нужные настройки правила и нажмите на кнопку **Сохранить**.

   c. Назначьте приоритет для нового правила. Для этого выделите правило и переместите его вверх или вниз по списку.

10. Чтобы исключить некоторые действия приложения из проверки, на закладке **Исключения** установите флажки для действий, которые не нужно контролировать.

11. Нажмите на кнопку **Сохранить**.

    Все исключения, созданные в правилах Предотвращения вторжений, доступны в окне настройки приложения Kaspersky Small Office Security в разделе **Исключения и действия с найденными объектами**.

Компонент Предотвращение вторжений будет отслеживать и ограничивать действия приложения в соответствии с настройками.

Проверка репутации приложения

Приложение Kaspersky Small Office Security позволяет проверять репутацию приложений у пользователей во всем мире. В состав репутации приложения входят следующие показатели:

- название производителя;
- информация о цифровой подписи (доступно при наличии цифровой подписи);

- информация о группе, в которую помещено приложение Предотвращением вторжений;
- количество пользователей Kaspersky Security Network, использующих приложение (доступно, если приложение отнесена к группе Доверенные в базе Kaspersky Security Network);
- время, когда приложение стало известно в Kaspersky Security Network;
- страны, в которых приложение наиболее распространено.

Проверка репутации приложения доступна, если вы согласились участвовать в Kaspersky Security Network.

Чтобы узнать репутацию приложения,

откройте контекстное меню исполняемого файла приложения и выберите пункт **Проверить репутацию в KSN**.

Откроется окно со сведениями о репутации приложения в Kaspersky Security Network.

Мониторинг сети

Мониторинг сети позволяет вам в реальном времени просматривать информацию о сетевой активности компьютера, блокировать сетевую активность, а также создавать сетевые и пакетные правила для приложений, установленных на вашем компьютере.

Чтобы перейти к настройке Мониторинга сети:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Безопасность**.
3. В блоке **Мониторинг сети** нажмите на кнопку **Посмотреть**.

Откроется окно Мониторинг сети.

В разделе **Сетевая активность** отображаются все активные на текущий момент сетевые соединения. Отображаются как входящие, так и исходящие соединения. По ссылке **Блокировать любую сетевую активность** вы можете заблокировать все сетевые соединения.

В разделе **Открытые порты** перечислены все открытые сетевые порты. В этом разделе вы также можете создавать сетевые и пакетные правила для приложений.

В разделе **Сетевой трафик** отображается объем входящего и исходящего сетевого трафика между вашим компьютером и другими компьютерами вашей сети.

В разделе **Заблокированные компьютеры** представлен список IP-адресов удаленных компьютеров, сетевую активность которых компонент Защита от сетевых атак заблокировал, обнаружив попытку сетевой атаки с этого IP-адреса.

Контроль работы пользователей на компьютере и в интернете

Этот раздел содержит информацию о том, как с помощью Kaspersky Small Office Security контролировать действия пользователей на компьютере и в интернете.

В этом разделе справки

Использование Веб-Контроля

Переход к настройке Веб-Контроля

Контроль использования компьютера

Контроль использования интернета

Контроль запуска игр и приложений

Контроль содержимого переписки

Просмотр отчета о действиях пользователя

Восстановление компьютера

Этот раздел содержит информацию о восстановлении операционной системы после заражения вредоносными приложениями.

О восстановлении операционной системы после заражения

Если вы подозреваете, что операционная система вашего компьютера была повреждена или изменена в результате действий вредоносных приложений или системного сбоя, используйте *мастер восстановления после заражения*, устраняющий следы пребывания в операционной системе вредоносных объектов. Специалисты "Лаборатории Касперского" рекомендуют также запускать мастер после лечения компьютера, чтобы убедиться, что все возникшие угрозы и повреждения устранены.

В ходе работы мастер проверяет наличие в операционной системе каких-либо изменений, к числу которых могут относиться блокировка доступа к сетевому окружению, изменение расширений файлов известных форматов, блокировка панели управления и тому подобное. Причины появления таких повреждений различны. Это могут быть активность вредоносных приложений, неправильная настройка операционной системы, системные сбои или применение неправильно работающих приложений – оптимизаторов операционной системы.

После исследования мастер анализирует полученную информацию с целью выявления в операционной системе повреждений, которые требуют немедленного вмешательства. По результатам исследования составляется список действий, которые следует выполнить, чтобы устранить повреждения. Мастер группирует действия по категориям с учетом серьезности обнаруженных проблем.

Восстановление операционной системы с помощью мастера восстановления

Чтобы запустить мастер восстановления после заражения:

1. Откройте главное окно приложения.
2. Выберите раздел **Безопасность** → **Устранение неполадок Windows**.
3. Нажмите на кнопку **Найти повреждения**.

   Откроется окно мастера восстановления после заражения.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется нажатием на кнопки **Назад** и **Далее**. Работа мастера завершается нажатием на кнопку **Готово**. Для прекращения работы мастера на любом этапе следует нажать на кнопку **Отмена**.

Рассмотрим подробнее шаги мастера.

Запуск восстановления операционной системы

a. Выберите один из двух вариантов работы мастера:

   - **Выполнить поиск повреждений, связанных с активностью вредоносных приложений**. Мастер выполнит поиск проблем и возможных повреждений.
   - **Отменить изменения**. Мастер отменит исправления ранее выявленных проблем и повреждений.

b. Нажмите на кнопку **Далее**.

Поиск проблем

Если вы выбрали вариант **Выполнить поиск повреждений, связанных с активностью вредоносных приложений**, мастер выполняет поиск проблем и возможных повреждений, которые следует исправить. По завершении поиска мастер автоматически переходит к следующему шагу.

Выбор действий для устранения повреждений

Все найденные на предыдущем шаге повреждения группируются в зависимости от опасности, которую они представляют. Для каждой группы повреждений специалисты "Лаборатории Касперского" предлагают набор действий, выполнение которых поможет устранить повреждения.

Всего выделено три группы:

- *Настоятельно рекомендуемые действия* помогут избавиться от повреждений, представляющих серьезную проблему. Рекомендуем вам устранить все повреждения из этой группы.
- *Рекомендуемые действия* направлены на устранение повреждений, которые могут представлять опасность. Повреждения из этой группы также рекомендуется устранить.
- *Дополнительные действия* предназначены для устранения неопасных в данный момент повреждений операционной системы, которые в дальнейшем могут поставить безопасность компьютера под угрозу.

Раскройте список выбранной группы, чтобы просмотреть повреждения, входящие в эту группу.

Чтобы мастер устранил какое-либо повреждение, установите флажок напротив названия повреждения. По умолчанию мастер устраняет повреждения из группы рекомендуемых и настоятельно рекомендуемых к устранению. Если вы не хотите устранять какое-либо повреждение, снимите флажок рядом с ним.

Настоятельно не рекомендуется снимать флажки, установленные по умолчанию, поскольку в результате этого действия безопасность вашего компьютера останется под угрозой.

Сформировав набор действий для выполнения мастером, нажмите на кнопку **Далее**.

Устранение повреждений

Мастер выполняет действия, выбранные на предыдущем шаге. Устранение повреждений может занять некоторое время. По завершении устранения повреждений мастер автоматически перейдет к следующему шагу.

Завершение работы мастера

Нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Об аварийном восстановлении операционной системы

Для аварийного восстановления операционной системы предназначено приложение Kaspersky Rescue Disk. Вы можете использовать Kaspersky Rescue Disk для проверки и лечения зараженного компьютера, который нельзя вылечить другим способом (например, с помощью антивирусных приложений).

Более подробную информацию об использовании Kaspersky Rescue Disk вы найдете на сайте Службы технической поддержки.

Как восстановить удаленный или вылеченный файл

Резервные копии файлов, которые были удалены или вылечены, помещаются в специальную папку на вашем компьютере, которая называется *Карантин*. Резервные копии файлов хранятся в специальном формате и не представляют опасности для вашего компьютера. Вы можете восстановить удаленный или вылеченный файл из резервной копии, которая хранится в Карантине.

Мы не рекомендуем восстанавливать удаленные и вылеченные файлы, поскольку они могут представлять угрозу для вашего компьютера.

Приложение не выполняет лечение приложений из Магазина Windows. Если в результате проверки такое приложение признано опасным, оно будет удалено с вашего компьютера. При удалении приложений из Магазина Windows приложение Kaspersky Small Office Security не создает резервные копии. Для восстановления таких объектов необходимо использовать средства восстановления операционной системы (подробную информацию можно получить из документации к операционной системе, установленной на вашем компьютере) либо обновить приложения через Магазин Windows.

Чтобы восстановить удаленный или вылеченный файл:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Безопасность**.

3. Нажмите на кнопку **Карантин** в правом верхнем углу окна приложения.

   Откроется окно **Карантин**.

4. В открывшемся окне **Карантин** выберите нужный файл в списке и нажмите на кнопку **Восстановить**.

Защита электронной почты

Этот раздел содержит информацию о том, как защитить электронную почту от спама, вирусов и других приложений, представляющих угрозу.

Настройка Почтового Антивируса

Приложение Kaspersky Small Office Security позволяет проверять сообщения электронной почты на наличие в них опасных объектов с помощью Почтового Антивируса. Почтовый Антивирус запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет почтовые сообщения, получаемые или отправляемые по протоколам POP3, SMTP, IMAP и NNTP (в том числе через защищенные соединения (SSL) по протоколам POP3, SMTP и IMAP). Кроме того, приложение может проверять вложения электронной почты, доступ к которым осуществляется через веб-почтовые клиенты.

По умолчанию Почтовый Антивирус проверяет как входящие, так и исходящие сообщения. При необходимости вы можете включить проверку только входящих сообщений.

Чтобы настроить Почтовый Антивирус:

1. Откройте главное окно приложения.

2. Нажмите на кнопку ⚙ в нижней части главного окна.

   Откроется окно **Настройка**.

3. Выберите раздел **Настройки безопасности**.

4. В окне **Настройки безопасности** выберите компонент Почтовый Антивирус.

   Будет выполнен переход в окно **Настройки Почтового Антивируса**.

5. Убедитесь, что переключатель в верхней части окна, включающий / выключающий Почтовый Антивирус, включен.

6. Выберите уровень безопасности:

   - **Оптимальный**. При установке этого уровня безопасности Почтовый Антивирус проверяет входящие и исходящие сообщения, вложенные архивы, а также выполняет эвристический анализ с уровнем детализации **Средний**.

   - **Низкий**. При установке этого уровня безопасности Почтовый Антивирус проверяет только входящие сообщения и не проверяет вложенные архивы.

   - **Предельный**. При установке этого уровня безопасности Почтовый Антивирус проверяет входящие и исходящие сообщения, вложенные архивы, а также выполняет эвристический анализ с уровнем детализации **Глубокий**.

7. В блоке **Действие при обнаружении угрозы** выберите действие, которое Почтовый Антивирус будет выполнять при обнаружении зараженного объекта (например, лечить).

8. Если вы хотите проверять вложения электронной почты в веб-почтовых клиентах, выберите вариант **Проверять веб-почтовые клиенты** в разделе **Встраивание в операционную систему**. Функция фильтрации вложений также работает для веб-почтовых клиентов.

Если угрозы в почтовом сообщении не были обнаружены или зараженные объекты были успешно вылечены, почтовое сообщение становится доступным для работы. Если зараженный объект вылечить не удалось, Почтовый Антивирус переименовывает или удаляет объект из сообщения и помещает в тему сообщения уведомление о том, что оно обработано приложением Kaspersky Small Office Security. В случае удаления объекта приложение Kaspersky Small Office Security создает его резервную копию и помещает на карантин.

При переходе на более новую версию приложения настроенные пользователем настройки Почтового Антивируса не сохраняются. Новая версия приложения будет использовать установленные по умолчанию настройки Почтового Антивируса.

Если во время проверки приложение обнаружило в тексте сообщения пароль к архиву, пароль будет использован для проверки содержания этого архива на наличие вредоносных приложений. Пароль при этом не сохраняется. При проверке архива выполняется его распаковка. Если во время распаковки архива произошел сбой в работе приложения, вы можете вручную удалить файлы, которые при распаковке сохраняются по следующему пути: %systemroot%\temp. Файлы имеют префикс PR.

Участие в Kaspersky Security Network

Чтобы повысить эффективность защиты вашего компьютера, приложение Kaspersky Small Office Security использует облачную защиту. Облачная защита реализуется с помощью инфраструктуры Kaspersky Security Network, использующей данные, полученные от пользователей во всем мире.

Kaspersky Security Network (KSN) – это облачная база знаний "Лаборатории Касперского", которая содержит информацию о репутации приложений и сайтов. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложения Kaspersky Small Office Security на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Участие пользователей в Kaspersky Security Network позволяет "Лаборатории Касперского" оперативно получать информацию о новых угрозах и их источниках, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний. Участие в Kaspersky Security Network обеспечивает вам доступ к данным о репутации приложений и сайтов.

Если вы участвуете в Kaspersky Security Network, вы в автоматическом режиме отправляете в "Лабораторию Касперского" информацию о конфигурации вашей операционной системы и времени запуска и завершения процессов приложения Kaspersky Small Office Security.

Если вы работаете в соответствии с условиями Общего регламента по защите данных (GDPR), прочтите эту статью.

Как включить и выключить участие в Kaspersky Security Network

Участие в Kaspersky Security Network является добровольным. Вы можете включить или выключить использование Kaspersky Security Network (KSN) во время установки приложения Kaspersky Small Office Security и / или в любой момент после установки.

Чтобы включить или выключить участие в Kaspersky Security Network:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки безопасности** → **Kaspersky Security Network**.

   В открывшемся окне **Kaspersky Security Network** отобразятся сведения о Kaspersky Security Network и настройки участия в Kaspersky Security Network.
4. Включите или выключите участие в Kaspersky Security Network с помощью переключателя в верхней части окна:

   - Если вы хотите участвовать в Kaspersky Security Network, переведите переключатель в положение **Вкл**.

     Откроется окно с текстом Положения о Kaspersky Security Network. Если вы согласны с условиями положения, нажмите на кнопку **Я согласен**.
   - Если вы не хотите участвовать в Kaspersky Security Network, переведите переключатель в положение **Выкл**.

В некоторых версиях приложения Kaspersky Small Office Security вместо информации о Kaspersky Security Network в окне **Kaspersky Security Network** отображается **Положении о Kaspersky Security Network**.

Чтобы принять Положение о Kaspersky Security Network:

1. Нажмите на кнопку **Принять** в блоке **Положение о Kaspersky Security Network**.

   Откроется Положение о Kaspersky Security Network. Это положение позволяет специалистам "Лаборатории Касперского" своевременно получать информацию об угрозах, обнаруженных на вашем компьютере, о запускаемых приложениях и о скачиваемых подписанных приложениях, а также информацию об операционной системе для улучшения вашей защиты.
2. Если вы принимаете условия положения, нажмите на кнопку **Принять**.

Чтобы отказаться от Положения о Kaspersky Security Network,

нажмите на кнопку **Отказаться** в блоке **Положение о Kaspersky Security Network**.

Как проверить подключение к Kaspersky Security Network

Подключение к Kaspersky Security Network может отсутствовать по следующим причинам:

- Вы не участвуете в Kaspersky Security Network.
- Ваш компьютер не подключен к интернету.
- Текущий статус ключа не позволяет осуществить подключение к Kaspersky Security Network. Например, подключение к KSN может отсутствовать по следующим причинам:
  - Приложение не активировано.
  - Срок действия лицензии или подписки истек.

Выявлены проблемы, связанные с лицензионным ключом (например, ключ попал в список запрещенных ключей).

Чтобы проверить подключение к Kaspersky Security Network:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.

   Выберите раздел **Настройки безопасности** → **Kaspersky Security Network**.

В окне **Kaspersky Security Network** отобразится статус подключения к Kaspersky Security Network.

В некоторых случаях "Лаборатория Касперского" может вводить временные ограничения на запросы репутации файлов из Kaspersky Security Network. В случае действия временных ограничений на запрос информации из Kaspersky Security Network отображается соответствующее уведомление.

Защита с помощью аппаратной виртуализации

В этом разделе вы узнаете, как вы можете защитить свой компьютер с помощью аппаратной виртуализации.

О защите с помощью аппаратной виртуализации

Приложение Kaspersky Small Office Security, установленное в 64-разрядной операционной системе Microsoft Windows 8, Microsoft Windows 8.1 или Microsoft Windows 10, использует технологию гипервизора для дополнительной защиты от сложных вредоносных приложений, которые могут похищать ваши персональные данные с помощью буфера обмена и фишинга.

Защита с помощью аппаратной виртуализации включена по умолчанию. Если защита была выключена вручную, вы можете включить ее в окне настройки приложения.

Функциональность защиты с помощью аппаратной виртуализации (гипервизора) в Kaspersky Small Office Security имеет следующие ограничения в 64-разрядных операционных системах Microsoft Windows 8, Microsoft Windows 8.1 или Microsoft Windows 10:

- Функциональность недоступна при запуске гипервизора сторонним приложением, например, приложения для виртуализации компании VMware™. После завершения работы гипервизора стороннего приложения функциональность защиты от создания снимков экрана снова становится доступной.
- Функциональность недоступна, если центральный процессор вашего компьютера не поддерживает технологию аппаратной виртуализации. Уточнить, поддерживает ли процессор вашего компьютера технологию аппаратной виртуализации, можно в технической документации для вашего компьютера или на сайте производителя процессора.
- Функциональность недоступна, если в момент запуска защищенного режима браузера обнаружен работающий гипервизор стороннего приложения, например, приложения компании VMware.
- Функциональность недоступна, если на вашем компьютере выключена аппаратная виртуализация. Уточнить, как включить аппаратную виртуализацию на вашем компьютере, можно в технической документации для вашего компьютера или на сайте производителя процессора.
- Функциональность недоступна, если на операционной системе Microsoft Windows 10 включен режим Device Guard.
- Функциональность недоступна, если на операционной системе Microsoft Windows 10 включен режим Virtualization Based Security (VBS).

Как включить защиту с помощью аппаратной виртуализации

Чтобы включить защиту с помощью аппаратной виртуализации:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки приватности** → **Защита ввода данных**.
4. Установите флажок **Использовать аппаратную виртуализацию, если она доступна**. Флажок отображается в 64-разрядной версии Windows 8, Windows 8.1 и Windows 10.
5. Установите флажок **Использовать расширенные возможности аппаратной виртуализации**, если вы хотите, чтобы аппаратная виртуализация включалась при запуске операционной системы.

   Доступность данной опции зависит от того, установлен ли на компьютере загрузочный гипервизор, а также от параметров работы драйверов Kaspersky Small Office Security.

Если на вашем компьютере выключена аппаратная виртуализация, защита с помощью аппаратной виртуализации не работает.

Защита с помощью Antimalware Scan Interface (AMSI)

Этот раздел содержит информацию о том, что сторонние приложения, например Microsoft Office, могут отправлять в приложение Kaspersky Small Office Security скрипты для проверки через интерфейс Antimalware Scan Interface (AMSI), а также о том, как выключить защиту с помощью AMSI в приложении Kaspersky Small Office Security.

О защите с помощью Antimalware Scan Interface

Antimalware Scan Interface (AMSI) позволяет стороннему приложению с поддержкой AMSI отправлять объекты в приложение Kaspersky Small Office Security для дополнительной проверки (например, скрипты PowerShell) и получать результаты проверки этих объектов. Сторонними приложениями могут быть, например, приложения Microsoft Office. Подробнее об интерфейсе AMSI см. в *документации Microsoft*.

С помощью Antimalware Scan Interface можно только обнаруживать угрозу и уведомлять стороннее приложение об обнаруженной угрозе. Стороннее приложение после уведомления об угрозе не дает выполнить вредоносные действия (например, завершает работу).

Приложение Kaspersky Small Office Security может отклонить запрос от стороннего приложения, например, если это приложение превысило максимальное количество запросов за промежуток времени. В этом случае приложение Kaspersky Small Office Security показывает уведомление о том, что запрос был отклонен. При получении такого уведомления вам не требуется выполнять никаких действий.

Защита с помощью Antimalware Scan Interface доступна на операционных системах Windows 10 Home / Pro / Education / Enterprise и Windows 11 Home / Pro / Enterprise.

Как включить защиту с помощью Antimalware Scan Interface

Чтобы включить защиту с помощью Antimalware Scan Interface:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки безопасности** → **AMSI-защита**.
4. В блоке **Проверка скриптов** установите флажок **Проверять скрипты с помощью Antimalware Scan Interface (AMSI)**.

Как исключить скрипт из проверки с помощью Antimalware Scan Interface

Чтобы исключить скрипт из проверки с помощью Antimalware Scan Interface:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки безопасности** → **AMSI-защита**.
4. В блоке **Проверка скриптов** установите флажок **Проверять скрипты с помощью Antimalware Scan Interface (AMSI)**.
5. По ссылке **Настроить исключения** перейдите в окно **Исключения**.
6. В окне **Исключения** нажмите на кнопку **Добавить**.

   Откроется окно **Добавление нового исключения**.
7. В поле **Файл или папка** укажите папку, в которой расположен скрипт.
8. В поле **Объект** укажите название скрипта.

   Вы также можете добавлять в исключения файлы одного типа с помощью маски.
9. В разделе **Компоненты защиты** установите флажок напротив компонента Файловый Антивирус.
10. Выберите статус **Активно**.

Проверка указанного объекта не будет выполняться с помощью Antimalware Scan Interface.

Производительность

Если ваше устройство тормозит или зависает, вы не одиноки! Бывает, что приложения не хотят запускаться, а браузер не отвечает в самый нужный момент. Это может происходить по разным причинам. Мы поможем вам разобраться, что именно вызвало эти проблемы, и устранить их.

Обновление приложений

Этот раздел содержит информацию о том, как с помощью приложения Kaspersky Small Office Security вы можете обновлять приложения, установленные на вашем компьютере.

Об обновлении приложений

Если вы давно не обновляли приложения на своем компьютере, эти приложения могут иметь уязвимости. Такими уязвимостями могут воспользоваться злоумышленники, чтобы нанести вред вашему компьютеру или данным.

Обновление установленных приложений повышает безопасность вашего компьютера. С помощью Kaspersky Small Office Security вы можете искать обновления для установленных приложений, а также скачивать и устанавливать последние обновления.

Kaspersky Small Office Security подразделяет обновления приложений на два типа:

- *Важные* – это обновления, которые устраняют уязвимости установленных приложений и повышают безопасность вашего компьютера.
- *Рекомендуемые* – это обновления, которые улучшают функциональность и / или вносят изменения в установленные приложения.

Kaspersky Small Office Security регулярно выполняет поиск обновлений. Когда Kaspersky Small Office Security находит новое обновление для установленного на компьютере приложения, Kaspersky Small Office Security показывает всплывающее уведомление в области уведомлений. Информация о наличии, количестве и типе доступных обновлений отображается в Центре уведомлений. Из Центра уведомлений вы можете перейти к просмотру, скачиванию и установке доступных обновлений.

Вы также можете запустить поиск обновлений для приложений вручную.

По умолчанию Kaspersky Small Office Security автоматически скачивает и устанавливает все обновления для известных приложений, если для этого от вас не требуется принимать новое лицензионное соглашение. Если Kaspersky Small Office Security установлен на файловом сервере, обновления для приложений автоматически не скачиваются.

В операционной системе Windows 8 и более поздних версиях Kaspersky Small Office Security прерывает автоматическое скачивание обновлений для приложений, если используется лимитное подключение к интернету. Скачивание обновлений возобновляется после восстановления безлимитного подключения. Если вы запустили обновление вручную, Kaspersky Small Office Security скачает его независимо от того, лимитное подключение вы используете или нет.

Приложения, которые вы не хотите обновлять или для которых не хотите устанавливать отдельные обновления, Kaspersky Small Office Security помещает в список исключений. Вы можете просматривать и изменять список исключений.

Как изменить настройки Обновления приложений

Чтобы изменить настройки Обновления приложений:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки производительности**.
4. Нажмите на кнопку **Автоматический поиск обновлений**.

   Откроется окно **Настройки Обновления приложений**.
5. Если вы не хотите, чтобы Kaspersky Small Office Security автоматически скачивал и устанавливал обновления приложений, для которых не требуется принимать новое лицензионное соглашение, снимите флажок **Автоматически скачивать и устанавливать обновления, если не требуется принимать новое лицензионное соглашение**.

   По умолчанию флажок установлен.
6. В блоке **Искать обновления для приложений** выберите, какие обновления приложений будет скачивать и устанавливать Kaspersky Small Office Security:

   - Выберите вариант **Важные обновления, которые повышают безопасность компьютера**, чтобы приложение Kaspersky Small Office Security устанавливало только важные обновления, которые устраняют уязвимости приложений и повышают безопасность вашего компьютера.
   - Выберите вариант **Все обновления для известных приложений**, чтобы Kaspersky Small Office Security устанавливал все обновления приложений.

Поиск обновлений для приложений

Чтобы запустить поиск обновлений для приложений:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Производительность**.
3. В блоке **Обновление приложений** нажмите на кнопку **Найти обновления**.

Запустится поиск обновлений для приложений.

Как настроить режим поиска обновлений

Чтобы настроить режим поиска обновлений для установленных приложений:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки производительности**.
4. Нажмите на кнопку **Автоматический поиск обновлений**.

   Откроется окно **Настройки Обновления приложений**.
5. В блоке **Обновление** установите флажок **Включить поиск обновлений для приложений**.
6. По ссылке **Задать расписание** перейдите в окно **Режим поиска обновлений**.
7. В раскрывающемся списке **Искать обновления** выберите один из следующих пунктов:

   - **Автоматически**. Если вы выберете этот пункт, приложение Kaspersky Small Office Security будет выполнять поиск обновлений для приложений минимум раз в сутки согласно внутренним настройкам приложения.
   - **По дням** / **Еженедельно** / **Ежемесячно**. Если вы выберете один из этих пунктов, приложение Kaspersky Small Office Security будет запускать поиск обновлений по заданному вами расписанию, с точностью до минуты. При выборе одного из этих вариантов доступен список **Отложить запуск после старта приложения на N минут**.

   Следующие параметры из раскрывающегося списка **Искать обновления** больше недоступны и будут заменены на **Автоматически** после обновления приложения: **Вручную**, **По минутам**, **По часам**, **В указанное время**, **После запуска приложения**, и **После каждого обновления**.
8. Установите флажок **Запускать поиск обновлений на следующий день, если компьютер был выключен**, чтобы запускать поиск после включения компьютера в случае пропуска запланированного времени поиска. Если флажок не установлен, приложение будет запускать поиск обновлений только в заданное по расписанию время, когда компьютер включен.
9. Нажмите на кнопку **Сохранить**, чтобы сохранить настройки.

Просмотр списка обновлений для приложений

Список обновлений формируется в зависимости от местоположения пользователя. Приложение Kaspersky Small Office Security скрывает обновления, которые недоступны для загрузки в текущем регионе.

Приложение Kaspersky Small Office Security регулярно выполняет поиск обновлений для приложений, установленных на вашем компьютере. Информацию о количестве и типе доступных обновлений для приложений вы можете посмотреть в Центре уведомлений.

Чтобы просмотреть список, сформированный в результате поиска обновлений приложений:

1. Откройте главное окно приложения.
2. Нажмите на кнопку **Подробнее** в верхней части окна.

   Откроется окно **Центр уведомлений**.
3. В разделе **Статус** в строке с сообщением о найденных обновлениях для приложений нажмите на кнопку **Показать**.

   Откроется окно **Обновление приложений**, которое содержит список найденных обновлений для приложений.
4. Если вы хотите обновить все приложения, которые отображаются в списке, нажмите на кнопку **Обновить все** (доступно не во всех регионах).
5. Если вы хотите принять решение по каждому приложению, которую предлагается обновить, выполните одно из следующих действий:

   - Нажмите на кнопку **Обновить** в строке с приложением, если хотите обновить это приложение.

     Перед обновлением приложений рекомендуется ознакомиться с его лицензионными соглашениями. Лицензионные соглашения доступны в раскрывающемся списке **Лицензионные соглашения**. По умолчанию язык лицензионного соглашения соответствует языку, заданному в интерфейсе приложения. Если лицензионное соглашение на языке интерфейса приложения недоступно, его текст будет представлен на языке интерфейса приложения Kaspersky Small Office Security. В остальных случаях текст лицензионного соглашения будет представлен на английском языке или первом доступном языке, если нет текста на английском.

   - По кнопке ⌄ откройте меню и выберите элемент **Не обновлять это приложение**, если хотите, чтобы приложение Kaspersky Small Office Security не уведомляло вас о появлении обновлений для выбранного приложения.

     Выбранное приложение будет перенесено в список исключений. Приложение Kaspersky Small Office Security не будет уведомлять о появлении новых обновлений для этого приложения.

   - По кнопке ⌄ откройте меню и выберите элемент **Пропустить это обновление**, если хотите, чтобы приложение Kaspersky Small Office Security не уведомляло вас о выбранном обновлении.

     Выбранное обновление приложения будет перемещено в список исключений. Приложение Kaspersky Small Office Security уведомит вас о появлении нового обновления для этого приложения.

   - По кнопке ⌄ откройте меню и выберите элемент **Открыть сайт производителя**, если хотите вручную скачать и установить обновление для выбранного приложения.

     В браузере, заданном в операционной системе по умолчанию, откроется сайт компании-производителя приложения. На сайте вы можете ознакомиться с обновлением и скачать его вручную.

Интерфейс окна, Обновление приложений и просмотр Лицензионных соглашений могут отличаться в зависимости от языка локализации приложения Kaspersky Small Office Security.

Удаление обновления или приложения из списка исключений

Просматривая список обновлений для приложений, вы можете пропускать как уведомления об отдельных обновлениях, так и уведомления обо всех обновлениях для определенных приложений. Приложение Kaspersky Small Office Security помещает такие обновления и приложения в список исключений.

Чтобы удалить обновление или приложение из списка исключений:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки производительности**.
4. Нажмите на кнопку **Автоматический поиск обновлений**.

   Откроется окно **Настройки Обновления приложений**.
5. По ссылке **Исключения** перейдите в окно **Исключения**.

   В списке **Исключения** содержатся приложения и обновления, для которых вы указали, что их не надо обновлять, и отдельные обновления приложений, которые вы не установили.
6. Выберите в списке обновление или приложение и нажмите на кнопку **Удалить**.

При следующем поиске обновлений приложение Kaspersky Small Office Security уведомит вас о наличии обновлений для приложений, которые вы удалили из списка исключений.

Резервное копирование данных

Этот раздел содержит информацию о резервном копировании данных.

О резервном копировании данных

Резервное копирование данных необходимо для защиты ваших данных от потери в результате выхода из строя или кражи оборудования, случайного удаления или потери в результате действий злоумышленников.

Чтобы выполнить резервное копирование данных, требуется создать и запустить задачу резервного копирования. Задача может быть запущена автоматически, по заданному расписанию, или вручную. С помощью приложения вы можете просматривать информацию о выполнении этих задач.

Сохранять резервные копии данных рекомендуется на внешних дисках или в Облачном хранилище. Данные резервных копий зашифрованы.

Приложение Kaspersky Small Office Security не может создавать полную копию диска с активной операционной системой Microsoft Windows.

Для создания резервных копий приложение Kaspersky Small Office Security позволяет использовать следующие типы хранилищ:

- локальный диск;
- внешний диск (например, внешний жесткий диск);
- сетевой диск;
- Облачное хранилище.

Особенности создания задач с учетом прав доступа пользователя

Задачи резервного копирования создаются с учетом прав доступа пользователя к файлам на локальном компьютере.

Если у вас нет прав локального администратора на компьютере, вам доступны только созданные вами задачи. Если у вас есть права локального администратора на этом компьютере, вам видны все задачи резервного копирования, но вы не можете изменять задачи, созданные другими пользователями.

Задачи резервного копирования, созданные ранее без учета прав доступа к файлам, доступны всем пользователям компьютера. Однако при изменении таких задач они будут выполняться с учетом прав доступа пользователя, который изменил задачу.

О восстановлении данных с учетом прав доступа пользователя

Если у вас нет прав локального администратора на компьютере, вы можете восстанавливать данные только из созданных вами задач резервного копирования и только в папки, на доступ к которым у вас есть права. Если у вас есть права локального администратора на этом компьютере, вы можете восстанавливать данные из любой задачи резервного копирования в любую папку.

Общий размер копируемых файлов в папке может превышать размер самой папки, если эта папка включает ссылки на другие папки (например, при копировании папки Документы также будут копироваться папки Видео, Музыка и Изображения, если ссылки на эти папки есть в папке Документы).

О резервном копировании данных в OneDrive

При резервном копировании файлов в папке OneDrive на вашем компьютере приложение Kaspersky Small Office Security действует по-разному в зависимости от того, скачан ли облачный файл в папку OneDrive:

- Если файл есть и в облаке, и в папке OneDrive на вашем компьютере, приложение Kaspersky Small Office Security делает резервную копию этого файла.
- Если файла нет в облаке, но есть в папке OneDrive на вашем компьютере, Kaspersky Small Office Security делает резервную копию этого файла.
- Если файл отображается в папке OneDrive, но хранится только в облаке и не хранится на вашем компьютере, приложение Kaspersky Small Office Security не делает резервную копию этого файла.

Как создать задачу резервного копирования

Чтобы создать задачу резервного копирования:

1. Откройте главное окно приложения Kaspersky Small Office Security.
2. Выберите раздел **Производительность**.
3. В блоке **Резервное копирование** нажмите на кнопку **Создать копию**, чтобы запустить мастер создания резервной копии.

   Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется нажатием кнопки **Далее**. Чтобы вернуться назад, нажмите на название предыдущего шага вверху страницы. Для прекращения работы мастера на любом шаге следует нажать на кнопку **Отмена**.

   Если вы прервете создание задачи резервного копирования, вам будет предложено сохранить черновик. Чтобы сохранить черновик, необходимо выбрать хотя бы одну папку на первом шаге мастера. Затем черновик появится в списке задач резервного копирования в окне **Резервное копирование**.

   Рассмотрим подробнее шаги мастера.

Шаг 1. Выбор файлов и папок для резервного копирования

На шаге **Выберите папки** вы можете указать папки и файлы, резервную копию которых хотите создать. Для этого перетащите нужную папку в окно **Выберите папки** или выберите папку, нажав на кнопку **Выберите папку**, чтобы открыть окно **Выберите папку**. В окне **Выберите папку** вы можете выбрать папку из дерева или указать путь к папке в текстовом поле вручную.

> Приложение Kaspersky Small Office Security не создает резервные копии файлов, расположенных в папках "Рабочий стол" и "Мои документы", если эти папки находятся на сетевом диске.

Чтобы добавить еще папки, нажмите на кнопку **Добавить папку** в правом верхнем углу страницы. Чтобы удалить папку с этой страницы, наведите курсор на нужную папку и нажмите на кнопку корзины.

После добавления папки вы можете выбрать файлы, резервную копию которых хотите создать. Чтобы просмотреть список файлов в папке, дважды щелкните по нужной папке. Чтобы включить или исключить из резервной копии определенные файлы, вы можете использовать флажки рядом с файлами. Если вам нужно найти конкретный файл в списке, используйте опцию **Поиск**.

Если вам нужно отсортировать файлы по типу, чтобы выполнить быструю настройку, нажмите **Аудио**, **Изображения**, **Документы**, **Финансовые документы**, **Видео**, или **Файлы других типов**.

Шаг 2. Выбор хранилища резервных копий

На шаге **Выберите хранилище**, вы можете настроить хранилище или указать существующее хранилище:

- **Облачные хранилища**. Выберите **Dropbox**, если вы хотите хранить резервные копии в Облачном хранилище Dropbox. Обратите внимание, что перед использованием Облачное хранилище Dropbox необходимо активировать. При создании резервной копии с использованием Облачного хранилища, приложение Kaspersky Small Office Security не создает резервные копии тех типов данных, на которые наложены ограничения правилами использования Dropbox.

- **Сетевые диски**. Если вы хотите хранить резервные копии на сетевом диске, выберите нужный сетевой диск нажав на кнопку **Добавить**.

- **Локальные и внешние диски**. Если вы хотите хранить резервные копии на локальном или внешнем диске, выберите нужный диск в списке.

- **У меня уже есть хранилище**. Если у вас уже есть хранилище, укажите его, нажав на кнопку **Подключить**.

Для безопасности данных рекомендуется использовать Облачное хранилище или создавать хранилища резервных копий на внешних дисках.

Как добавить сетевой диск в качестве хранилища

Чтобы добавить сетевой диск:

1. В секции **Сетевые диски** в окне **Выберите хранилище** нажмите на кнопку **Добавить**, чтобы открыть диалог **Добавление сетевого диска** и выбрать желаемый сетевой диск.

2. Предоставьте необходимую информацию для подключения к сетевому диску.

3. Нажмите на кнопку **Добавить**.

Как добавить локальный или внешний диск в качестве хранилища

Чтобы установить локальный или внешний диск в качестве хранилища резервных копий, выберите диск из списка в секции **Локальные и внешние диски** в окне **Выберите хранилище**.

Шаг 3. Создание расписания резервного копирования

На шаге **Настройте расписание** вы можете указать следующие параметры:

- Задайте имя задачи резервного копирования.
- Выберите **Запускать копирование вручную**, если хотите запускать задачу вручную.
- Задайте расписание запуска задачи резервного копирования, если хотите, чтобы задача запускалась автоматически.
    - Выберите опцию **Запускать копирование автоматически** и задайте интервал времени для запуска задачи (например, **Каждую неделю**), день недели и время выполнения задачи.
    - Укажите имя пользователя и пароль вашей учетной записи Windows на этом компьютере. Данные учетной записи Windows требуются для получения прав доступа к файлам во время резервного копирования. Если вы вошли в операционную систему под доменной учетной записью, для создания задачи резервного копирования укажите имя пользователя и пароль от вашей доменной учетной записи.
    - Установите флажок **Запускать при включении компьютера, если в указанное время он был выключен**, если вы хотите, чтобы приложение запускало резервное копирование при первой возможности после включения компьютера. Например, если резервное копирование запланировано на каждые выходные и компьютер был выключен, резервное копирование будет выполнено после включения компьютера в будний день. Если флажок снят, резервное копирование выполняется согласно расписанию, без повторных попыток в случае неудачного запуска резервного копирования.
    - Установите флажок **Запускать резервное копирование при подключении внешнего диска**, если вы хотите запускать резервное копирование при подключении внешнего диска к вашему компьютеру.

Обратите внимание на следующие особенности работы с задачами резервного копирования:

- Если вы создаете задачу резервного копирования по расписанию, вам необходимо указать данные вашей учетной записи на этом компьютере.
- Если вы создаете задачу резервного копирования по требованию, вам не нужно указывать данные вашей учетной записи на этом компьютере.
- Если вы изменяете задачу по требованию на задачу по расписанию, вам необходимо указать данные вашей учетной записи на этом компьютере.

Шаг 4. Настройка хранилища резервных копий

На шаге **Настройте хранилище** вы можете указать параметры хранения файлов:

Во время каждой сессии резервного копирования приложение проверяет, изменился ли файл со времени предыдущего резервного копирования. Если файл изменился, приложение создает в хранилище новую версию своей резервной копии. Предыдущая версия резервной копии также сохраняется в хранилище. Вы можете ограничить количество версий резервных копий. Установите флажок **Ограничить количество копий одного файла, если этот файл изменился несколько раз** и в поле **Количество последних копий одного файла** укажите количество версий резервных копий одного файла, которые необходимо сохранять. Резервная копия может иметь до 999 версий.

Также вы можете ограничить срок хранения каждой версии резервной копии файла. Старые версии резервных копий файла будут автоматически удалены. Последняя сохраненная версия резервной копии файла будет храниться неопределенно долго. Чтобы ограничить срок хранения, установите флажок **Удалять старые копии файла после указанного времени. Последняя, самая новая копия будет храниться бессрочно**, чтобы указать количество дней или недель, в течение которых должна храниться каждая версия файла резервной копии. Максимальное количество дней или недель — 999.

При желании вы можете указать пароль, который защитит ваши резервные копии от несанкционированного доступа. Чтобы это сделать нажмите **Настроить** в секции **Пароль** и задайте пароль.

Пароль будет применен ко всем резервным копиям в этом хранилище. Пароль не может быть изменен позже. Если вы забудете пароль, вы не сможете восстановить файлы из резервных копий в этом хранилище.

Приложение запрашивает у вас ввод пароля в следующих случаях:

- Когда вы первый раз создаете хранилище резервных копий на локальном диске или на внешнем диске (например, флеш-накопителе). При создании последующих задач резервного копирования на локальный диск или этот внешний диск, приложение уже не будет запрашивать ввод пароля. Будет использоваться пароль, заданный вами ранее.

  Если вы скопируете локальное хранилище резервных копий на внешний диск и подключите этот внешний диск к другому компьютеру, приложение попросит вас ввести пароль для копирования или восстановления данных из этого хранилища.

- Когда вы подключаете внешний диск к компьютеру. Приложение проверяет внешний диск и просит вас ввести пароль в случае обнаружения хранилища резервных копий на этом внешнем диске.

Если ваше хранилище резервных копий находится на компьютере, на котором приложение Kaspersky Small Office Security повреждено или не установлено, вы можете использовать Kaspersky Restore Utility, чтобы восстановить файлы из резервных копий или получить доступ к секретным папкам. Для этого вам необходимо скопировать утилиту в это хранилище выбрав флажок **Копировать утилиту Kaspersky Restore Utility в хранилище** в секции **Kaspersky Restore Utility**.

После настройки хранилища резервных копий нажмите на кнопку **Запустить**, чтобы немедленно запустить задачу резервного копирования, или нажмите на кнопку **Сохранить и закрыть**, если вы хотите запустить эту задачу позже вручную или по расписанию.

Завершение работы мастера

Процесс настройки хранилища может занять некоторое время. На этом шаге вы будете перенаправлены в окно **Резервное копирование**, где вы увидите список задач резервного копирования.

Как запустить или возобновить задачу резервного копирования

Чтобы запустить задачу резервного копирования:

1. Откройте главное окно приложения Kaspersky Small Office Security.
2. Выберите раздел **Производительность**.
3. В блоке **Резервное копирование** нажмите на кнопку **Посмотреть мои копии**.
4. В открывшемся окне выберите задачу резервного копирования и нажмите на кнопку **Запустить**.

   Запустится задача резервного копирования.

Если у вас есть черновик задачи резервного копирования и вы хотите его завершить, выполните следующие действия:

1. Откройте главное окно приложения Kaspersky Small Office Security.
2. Выберите раздел **Производительность**.
3. В блоке **Резервное копирование** нажмите на кнопку **Посмотреть мои копии**.
4. Выберите черновик незавершенной задачи резервного копирования.

   Блок задачи отображает список выполненных и незавершенных шагов.
5. Нажмите на кнопку **Настроить**, чтобы завершить работу мастера.

Восстановление данных из резервной копии

Чтобы восстановить данные из резервной копии:

1. Откройте главное окно приложения.
2. Выберите раздел **Производительность**.
3. В блоке **Резервное копирование** нажмите на кнопку **Посмотреть мои копии**.

   Откроется окно **Резервное копирование**.

   - Нажмите на опцию **Посмотреть файлы** в раскрывающемся меню рядом с выбранной задачей резервного копирования.
   - Нажмите на ссылку **Мои хранилища**, затем в открывшемся окне нажмите на кнопку **Посмотреть файлы** напротив нужного хранилища.
4. Если при создании резервной копии был задан пароль, укажите этот пароль в окне **Введите пароль для доступа к резервным копиям в хранилище**. Откроется окно **Выберите файлы для восстановления**.
5. Чтобы отсортировать и восстановить файлы определенных типов, выберите эти типы файлов вверху страницы.
6. Хранилище может содержать копии файлов, которые были удалены, и вы можете восстановить удаленный файл из резервной копии. Установите флажок **Не показывать копии удаленных файлов**, если вы предпочитаете не видеть резервные копии удаленных файлов.

7. Затем выполните одно из следующих действий:

    - Если вы хотите восстановить все данные, установите флажок **Все данные**.
    - Если вы хотите восстановить только некоторые папки, установите флажки рядом с нужными папками.
    - Если вы хотите восстановить только определенные файлы, установите флажки рядом с нужными файлами в графе **Имя**.

8. В раскрывающемся списке **Дата копирования** выберите дату и время создания нужных резервных копий.
9. Нажмите на кнопку **Выбрать**. Откроется окно **Выберите файлы для восстановления**.
10. Выберите один из двух вариантов:

    - **Исходная папка**. Приложение восстановит данные в исходную папку.
    - **Указанная папка**. Приложение восстановит данные в указанную папку. Нажмите на кнопку **Выбрать**, чтобы выбрать папку, в которую вы хотите восстановить данные.

11. В раскрывающемся списке **При совпадении имен файлов** выберите действие, которое должно выполнять приложение, если имя восстанавливаемого файла совпадает с именем файла, находящегося в указанной для восстановления папке:

    - **спрашивать** – Приложение Kaspersky при совпадении имен файлов предлагает выбрать один из вариантов: заменить файл резервной копией, сохранить оба файла или не восстанавливать этот файл.
    - **заменить файл резервной копией** – приложение Kaspersky Small Office Security удаляет существующий файл и помещает на его место файл, восстановленный из резервной копии.
    - **сохранить оба файла** – приложение Kaspersky Small Office Security оставляет существующий файл без изменений и сохраняет файл, восстановленный из резервной копии, под новым именем в этой же папке.
    - **не восстанавливать этот файл** – Приложение Kaspersky Small Office Security оставляет существующий файл без изменений, не восстанавливая одноименный файл из резервной копии.

12. Нажмите на кнопку **Восстановить файлы**.

    Выбранные для восстановления файлы будут восстановлены из резервной копии и сохранены в указанной папке.

Восстановление данных из FTP-хранилища

Приложение Kaspersky Small Office Security не поддерживает резервное копирование по FTP. Для восстановления резервных копий из FTP-хранилища, созданных в других приложениях "Лаборатории Касперского", воспользуйтесь следующей инструкцией.

Чтобы восстановить резервные копии из FTP-хранилища:

1. Откройте главное окно приложения.
2. Выберите раздел **Производительность**.

3. В блоке **Резервное копирование** нажмите на кнопку **Посмотреть мои копии**.

   Откроется окно **Резервное копирование**.

4. По ссылке **Мои хранилища** перейдите в окно **Хранилища**.

5. Откройте в проводнике папку FTP-хранилища.

6. Скопируйте данные, включая файл `storage.xml`, на локальный диск (например, C:\<название папки>).

7. В окне **Хранилища** напротив FTP-хранилища нажмите на кнопку **Удалить хранилище**.

8. В окне подтверждения удаления нажмите на кнопку **Удалить**.

   FTP хранилище будет удалено.

9. В окне **Хранилища** нажмите на кнопку **Подключить мое хранилище**.

10. В окне **Подключение хранилища** перейдите в раздел **Локальный диск** и с помощью кнопки **Обзор** укажите путь к папке с резервными копиями, которые вы скопировали на локальный диск из FTP-хранилища.

11. В окне **Хранилища** напротив подключенного хранилища нажмите на кнопку **Посмотреть файлы**.

12. Следуйте стандартной процедуре восстановления.

Восстановление данных из резервной копии с помощью Kaspersky Restore Utility

Утилита восстановления Kaspersky Restore Utility используется для работы с данными в хранилище резервных копий и данными в секретных папках на компьютере, на котором удалено или повреждено приложение "Лаборатории Касперского". По умолчанию после установки приложения утилита находится в папке Kaspersky Restore Utility, расположенной в папке установки приложения. Чтобы использовать утилиту на компьютере, на котором не установлено или повреждено приложение "Лаборатории Касперского", утилиту требуется скопировать на внешний диск.

Для запуска утилиты восстановления Kaspersky Restore Utility необходимы права локального администратора.

Для запуска Restore Utility на Windows 11 убедитесь, что на вашем компьютере установлен файл *VC_redist.x86.exe*. Подробнее см. в статье базы знаний Microsoft.

Как запустить утилиту восстановления

Чтобы запустить утилиту восстановления:

1. Откройте внешний диск, на который была скопирована утилита.
2. Запустите файл *restore_tool.exe* расположенный в папке Restore Utility.
3. Откроется главное окно утилиты восстановления, в котором вы можете выбрать, к чему вы хотите восстановить доступ:
   - **Резервная копия**. Нажав эту кнопку, вы сможете указать местоположение хранилища резервных копий или вам будет предложено выбрать хранилище по умолчанию, настроенное в приложении. Вы также можете указать другой путь к хранилищу.
   - **Секретная папка**. Нажав эту кнопку, вы сможете указать местоположение секретной папки.

Как открыть хранилище резервных копий с помощью утилиты восстановления

Чтобы открыть хранилище с помощью утилиты восстановления:

1. Запустите утилиту восстановления.
2. В открывшемся окне нажмите на кнопку **Резервная копия**.
3. Утилита автоматически определяет путь к хранилищу резервных копий, если оно создано на локальном диске *C:*.
4. Если хранилище резервных копий находится на другом диске, нажмите на кнопку **Выбрать другое хранилище**.
5. В открывшемся окне нажмите на кнопку **Выбрать** и укажите путь к хранилищу резервных копий.
6. Нажмите на кнопку **Выбрать**.

Как открыть секретную папку с помощью утилиты восстановления

Чтобы открыть секретную папку с помощью утилиты восстановления:

1. Запустите утилиту восстановления.
2. В открывшемся окне нажмите на кнопку **Секретная папка**.
3. Выберите секретную папку из списка и нажмите **Выбрать**.
4. В окне **Секретные папки, к которым восстанавливается доступ** нажмите на кнопку **Открыть**, чтобы получить доступ к папке.
5. Введите пароль, чтобы разблокировать секретную папку.
6. Теперь вы можете открыть секретную папку в Проводнике.

Как восстановить данные из резервной копии

Чтобы восстановить данные из резервной копии:

1. Запустите утилиту восстановления.
2. В открывшемся окне нажмите на кнопку **Резервная копия**.
3. В главном окне утилиты восстановления выполните следующие действия:
   a. В раскрывающемся списке **Резервная копия** выберите необходимую вам резервную копию.
   b. В раскрывающемся списке **Дата копирования** выберите дату и время создания нужных резервных копий.
4. Выберите файлы и папки, которые нужно восстановить. Для этого установите флажки рядом с нужными папками в списке.

   Используйте кнопку рядом с полем **Поиск**, чтобы переключаться между структурой папок и списком файлов.
5. Нажмите на кнопку **Восстанавливаем файлы**.

   Откроется окно **Выбор папки для восстановленных файлов**.
6. В открывшемся окне выберите место сохранения восстановленных файлов.
   - **Исходная папка**. Выберите этот вариант, если вы хотите восстановить данные в исходную папку.
   - **Указанная папка**. Выберите этот вариант, если вы хотите выбрать папку для восстановления данных. Чтобы выбрать папку для восстановления данных, нажмите на кнопку **Обзор**.
7. В раскрывающемся списке **При совпадении имен файлов** выберите действие, которое должно выполнять приложение, если в папке, куда требуется поместить восстановленный файл, уже находится файл с таким же именем:
   - **спрашивать** – Приложение Kaspersky при совпадении имен файлов предлагает выбрать один из вариантов: заменить файл резервной копией, сохранить оба файла или не восстанавливать этот файл.
   - **заменить файл резервной копией** – приложение Kaspersky Small Office Security удаляет существующий файл и помещает на его место файл, восстановленный из резервной копии.
   - **сохранить оба файла** – приложение Kaspersky Small Office Security оставляет существующий файл без изменений и сохраняет файл, восстановленный из резервной копии, под новым именем в этой же папке.
   - **не восстанавливать этот файл** – Приложение Kaspersky Small Office Security оставляет существующий файл без изменений, не восстанавливая одноименный файл из резервной копии.
8. Нажмите на кнопку **Восстановить файлы**.

   Откроется окно **Восстанавливаем файлы**. В окне отображается информация о процессе восстановления резервных копий файлов. Вы можете остановить восстановление с помощью кнопки **Остановить**.

   Будут восстановлены нужные резервные копии выбранных файлов.

Об Облачном хранилище

Приложение Kaspersky Small Office Security позволяет сохранять резервные копии ваших данных в Облачном хранилище, используя веб-сервис Dropbox.

Для использования Облачного хранилища требуется:

- Убедиться, что компьютер подключен к интернету.
- Создать учетную запись на сайте поставщика услуг хранения данных в облаке.
- Активировать Облачное хранилище.

Вы можете использовать одну и ту же учетную запись Dropbox для сохранения в единое Облачное хранилище резервных копий данных с разных устройств, на которых установлено приложение Kaspersky Small Office Security.

Объем Облачного хранилища определяется поставщиком услуг хранения данных онлайн, веб-сервисом Dropbox. Более подробную информацию об условиях использовании веб-сервиса вы можете получить на сайте Dropbox.

При копировании файлов в хранилище Dropbox, приложение Kaspersky Small Office Security не учитывает регистр в названии файла и / или названии пути к этому файлу. При попытке создания резервных копий файлов, названия и / или пути которых отличаются только регистром, приложение Kaspersky Small Office Security создает только одну резервную копию, так как в Dropbox возникает конфликт регистров.

Как активировать Облачное хранилище

Чтобы активировать Облачное хранилище:

1. Откройте главное окно приложения Kaspersky Small Office Security.
2. Выберите раздел **Производительность**.
3. В блоке **Резервное копирование** нажмите на кнопку **Создать копию**, чтобы запустить мастер создания резервной копии.
4. В окне выбора папки укажите папку и файлы, резервную копию которых хотите создать.
5. В окне выбора хранилища выберите **Dropbox** в блоке **Облачные хранилища** и нажмите на кнопку **Войти**.

   Для создания Облачного хранилища требуется подключение к интернету.

   Откроется окно входа в учетную запись Dropbox.

6. В открывшемся окне выполните одно из следующих действий:

   - Если вы не зарегистрированы на сайте Dropbox, пройдите процедуру регистрации.
   - Если вы зарегистрированы на сайте Dropbox, войдите в учетную запись Dropbox.

7. Для завершения активации Облачного хранилища подтвердите, что Kaspersky Small Office Security может использовать вашу учетную запись Dropbox для резервного копирования данных и восстановления данных из резервной копии. Kaspersky Small Office Security будет помещать резервные копии данных в отдельную папку, которая создается в папке хранения приложений Dropbox.

   После завершения активации Облачного хранилища откроется окно выбора хранилища. Онлайн-хранилище будет доступно для выбора. Для активированного Облачного хранилища отображается объем занятого пространства и объем свободного пространства, доступного для записи информации.

При копировании файлов в хранилище Dropbox, приложение Kaspersky Small Office Security не учитывает регистр в названии файла и / или названии пути к этому файлу. При попытке создания резервных копий файлов, названия и / или пути которых отличаются только регистром, приложение Kaspersky Small Office Security создает только одну резервную копию, так как в Dropbox возникает конфликт регистров.

Текущая активность

Если вы заметили, что ваш компьютер зависает или подтормаживает, вы можете перейти в окно **Активность приложений**, в котором отображаются запущенные приложения и активные процессы, и завершить работу приложения или приложений, которые потребляют слишком много ресурсов компьютера.

Чтобы просмотреть текущую активность и / или завершить работу приложения:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Производительность**.
3. В блоке **Текущая активность** нажмите на кнопку **Посмотреть всю активность**.

   Откроется окно **Активность приложений** на закладке **Работающие**.

4. В списке приложений выберите то, которое потребляет больше всего ресурсов процессора (графа **Процессор**) и / или оперативной памяти (графа **Память**), и нажмите на кнопку **Завершить процесс**.

Работа приложения будет завершена.

Режим "Не беспокоить"

В режиме "Не беспокоить" приложение Kaspersky Small Office Security не показывает всплывающие уведомления о событиях, произошедших на вашем компьютере, когда вы общаетесь по видеосвязи, смотрите фильм, активно используете установленные приложения и клавиатуру. Также в режиме "Не беспокоить" могут быть приостановлены некоторые автоматически запущенные задачи или отложено выполнение запланированных задач, чтобы избежать излишнего потребления ресурсов компьютера.

Чтобы включить режим "Не беспокоить" в настройках приложения (автоматический):

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки производительности** → **Оптимизация производительности компьютера**.
4. Установите флажок **Режим "Не беспокоить"**.

Чтобы включить режим "Не беспокоить" вручную:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Производительность**.
3. В блоке **Режим "Не беспокоить"** выберите количество часов из раскрывающегося списка и нажмите на кнопку **Включить**.

   Также вы можете включить режим "Не беспокоить", нажав **Включить режим "Не беспокоить** в контекстном меню значка приложения.

Режим "Не беспокоить" можно активировать вручную, если в настройках приложения не настроен автоматический запуск этой функции.

После выхода из режима "Не беспокоить" приложение покажет вам в области уведомлений панели задач сообщение о событии, которое произошло, пока вы были заняты. Если событий было несколько, нажмите на кнопку **Посмотреть**, чтобы перейти в **Центр уведомлений** и посмотреть все события.

Вы также можете посмотреть все события за последние три дня в окне **Центр уведомлений** на закладке **Статус** в разделе **Уведомления**.

Пока включен Режим сосредоточенной работы или режим "Не беспокоить", также не будут показаны уведомления приложений Kaspersky Secure Connection и Kaspersky Password Manager, установленных на этом же устройстве.

Функциональность Безопасное VPN-соединение доступна не во всех регионах.

Подробнее о показе уведомлений вы можете прочитать в разделе справки Как настроить уведомления приложения.

Как сохранить ресурсы операционной системы

При одновременной работе Kaspersky Small Office Security и некоторых приложений в полноэкранном режиме иногда могут возникать следующие неудобства:

- работа приложения замедляется из-за недостатка системных ресурсов;
- окна уведомлений Kaspersky Small Office Security отвлекают.

Чтобы не изменять настройки Kaspersky Small Office Security вручную перед каждым переходом в полноэкранный режим, вы можете использовать Режим сосредоточенной работы. Если Режим сосредоточенной работы включен и вы работаете с приложением в полноэкранном режиме, Kaspersky Small Office Security не запускает задачи проверки и обновления, не отображает уведомления.

Чтобы включить Режим сосредоточенной работы в настройках приложения (автоматический):

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки производительности** → **Оптимизация производительности компьютера**.
4. Установите флажок **Режим сосредоточенной работы**.

Чтобы включить Режим сосредоточенной работы вручную:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Производительность**.
3. В блоке **Режим сосредоточенной работы** выберите количество часов из выпадающего списка и нажмите на кнопку **Включить**.

   Также вы можете включить Режим сосредоточенной работы, нажав **Включить режим сосредоточенной работы** в контекстном меню значка приложения.

Режим сосредоточенной работы можно активировать вручную, если в настройках приложения не настроен автоматический запуск этой функции.

Пока включен Режим сосредоточенной работы или режим "Не беспокоить", также не будут показаны уведомления приложений Kaspersky Secure Connection и Kaspersky Password Manager, установленных на этом же устройстве.

Функциональность Безопасное VPN-соединение доступна не во всех регионах.

Экономия заряда батареи

Эта функция доступна только для ноутбуков.

Когда режим экономии заряда батареи включен, приложение Kaspersky Small Office Security откладывает выполнение задач проверки и обновления, для которых задан запуск по расписанию. По мере необходимости вы можете самостоятельно запускать задачи проверки и обновления.

Включить или выключить режим экономии заряда батареи вы также можете в окне **Оптимизация производительности компьютера**, установив или сняв флажок **Экономия заряда батареи**.

Оптимизация нагрузки на операционную систему

Проверка компьютера с помощью приложения Kaspersky Small Office Security может потребовать значительных системных ресурсов. Чтобы оптимизировать нагрузку на систему, в приложении Kaspersky Small Office Security предусмотрена возможность запуска задач проверки (системной памяти, системного раздела, объектов автозапуска) и обновления баз в то время, когда компьютер заблокирован или включена экранная заставка. Эта дополнительная настройка позволяет повысить безопасность компьютера, не снижая производительность в то время, когда вы используете его.

Если компьютер работает от аккумулятора, приложение Kaspersky Small Office Security не будет выполнять задачи во время простоя компьютера, чтобы продлить время его работы.

Чтобы оптимизировать нагрузку на операционную систему:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки производительности** → **Оптимизация производительности компьютера**.
4. Установите флажок **Откладывать выполнение задач проверки компьютера при высокой нагрузке на центральный процессор и дисковые системы**.

Приватность

Утечка личных данных, сбор информации о ваших действиях и показ вам навязчивой рекламы – это лишь неполный список проблем, которые могут омрачить ваше пребывание в интернете. Управление своими данными и любыми следами, которые вы оставляете в интернете, становится вопросом первой необходимости. Узнайте, как приложение Kaspersky Small Office Security помогает защитить вашу приватность.

Безопасное VPN-соединение

В некоторых регионах, использование приложения Kaspersky Secure Connection может регулироваться местным законодательством. Вы можете использовать Kaspersky Secure Connection только в соответствии с его назначением и без нарушения местного законодательства.

Этот раздел содержит информацию о том, как безопасно подключаться к сетям Wi-Fi и устанавливать безопасное VPN-соединение.

О безопасном подключении к сетям Wi-Fi

Функциональность Безопасное VPN-соединение доступна не во всех регионах.

Общественные сети Wi-Fi могут быть недостаточно защищены, например, если сеть Wi-Fi использует уязвимый протокол шифрования или слабый пароль. Когда вы совершаете покупки в интернете через незащищенные сети Wi-Fi, ваши пароли и другие конфиденциальные данные передаются в открытом текстовом виде. Злоумышленники могут перехватить ваши конфиденциальные данные, например, узнать номер вашей банковской карты и получить доступ к деньгам.

Чтобы обезопасить себя при работе в небезопасных сетях Wi-Fi, вы можете включить Безопасное VPN-соединение через специально выделенный сервер, расположенный в указанном вами регионе. Данные с сайта сначала поступают на выделенный сервер, и только после этого данные передаются на ваше устройство по зашифрованному безопасному VPN-соединению.

Чтобы использовать компонент Безопасное VPN-соединение, вам нужно запустить приложение Kaspersky Secure Connection. Kaspersky Secure Connection устанавливается совместно с приложением Kaspersky Small Office Security.

Компонент Безопасное VPN-соединение предоставляет следующие преимущества:

- Безопасная работа с платежными системами и сайтами бронирования. Злоумышленники не могут перехватить номер вашей банковской карты, когда вы совершаете онлайн-платеж, бронируете гостиницу или берете в аренду автомобиль.
- Защита вашей секретной информации. Никто не сможет определить IP-адрес вашего компьютера и ваше местоположение.
- Защита вашей персональной информации. Никто не может перехватить и прочитать вашу переписку в социальных сетях.

Безопасное VPN-соединение можно также использовать для других типов сетевых подключений: например, локальное подключение к интернету или подключение через USB-модем.

По умолчанию Kaspersky Secure Connection не предлагает включать безопасное VPN-соединение, если подключение к сайту выполняется по протоколу HTTPS.

Смена локации при посещении сайтов банков, платежных систем, сайтов бронирования, а также социальных сетей, чатов и почтовых сайтов может приводить к срабатыванию систем фрод-мониторинга (систем, предназначенных для оценки финансовых транзакций в интернете на предмет мошеннических операций).

Использование Безопасного VPN-соединения может регулироваться местным законодательством. Вы можете использовать Безопасное VPN-соединение только в соответствии с его назначением и без нарушения местного законодательства.

Как включить безопасное VPN-соединение

Функциональность Безопасное VPN-соединение доступна не во всех регионах.

Безопасное VPN-соединение устанавливается с помощью приложения Kaspersky Secure Connection. Вы можете запускать Kaspersky Secure Connection из меню **Пуск** (в операционной системе Microsoft Windows 7 и ниже), с начального экрана (в операционной системе Microsoft Windows 8 и выше) или из окна приложения Kaspersky Small Office Security.

Чтобы запустить Kaspersky Secure Connection из окна приложения Kaspersky Small Office Security:

1. Откройте главное окно приложения Kaspersky Small Office Security.
2. Перейдите в раздел **Приватность**.
3. В блоке **Безопасное VPN-соединение** нажмите на кнопку **Использовать**.

   Откроется главное окно приложения Kaspersky Secure Connection.

Подробную информацию о работе Kaspersky Secure Connection вы можете получить в справке для этого приложения.

Защита от сбора данных в интернете

Этот раздел содержит информацию о том, как с помощью приложения Kaspersky Small Office Security защитить вас от сбора информации о ваших действиях в интернете.

О защите от сбора данных в интернете

Когда вы находитесь в интернете, сайты с помощью сервисов отслеживания собирают информацию о ваших действиях в интернете. Сервисы отслеживания используют полученную информацию для анализа ваших действий и могут применять результаты анализа, например, для показа вам соответствующей рекламной информации.

Компонент *Защита от сбора данных в интернете* предназначен для защиты от сбора информации о ваших действиях в интернете.

В *режиме обнаружения* компонент Защита от сбора данных в интернете обнаруживает и подсчитывает попытки сбора данных, записывая информацию об этом в отчет. Режим обнаружения включен по умолчанию, сбор данных разрешен на всех сайтах.

В *режиме блокировки* компонент Защита от сбора данных в интернете обнаруживает и блокирует попытки сбора данных, информацию о них записывает в отчет. В этом режиме сбор данных запрещен на всех сайтах, кроме:

- сайтов, которые вы добавили в исключения;
- сайтов "Лаборатории Касперского" и ее партнеров;
- сайтов, о которых "Лаборатории Касперского" известно, что их работоспособность может быть нарушена в результате блокировки.

Счетчик заблокированных попыток сбора данных отображает общее количество блокировок по всему сайту в зависимости от того, сколько страниц сайта открыто в браузере. Если в браузере открыта одна страница, считаются только заблокированные попытки сбора данных на этой странице сайта. Если в браузере открыто несколько страниц одного сайта, считаются заблокированные попытки сбора данных на всех страницах сайта, открытых в браузере.

Вы можете управлять компонентом Защита от сбора данных в интернете в интерфейсе Kaspersky Small Office Security или с помощью расширения Kaspersky Protection в браузере.

Защита от сбора данных в интернете имеет следующие ограничения:

- Приложение не блокирует сбор данных сервисом отслеживания из категории "Социальные сети", если вы находитесь на сайте соответствующей социальной сети.
- Если веб-страницу, на которой выполнена попытка сбора данных, не удалось определить, то Kaspersky Small Office Security не блокирует такую попытку сбора данных и не отображает информацию о ней.
- Если веб-страницу, на которой выполнена попытка сбора данных, удалось определить, но не удалось сопоставить ни с одной веб-страницей, открытой в браузере, то Kaspersky Small Office Security применяет то действие, которое задано в настройках Защиты от сбора данных в интернете (запрещает или разрешает сбор данных). Приложение отображает информацию о попытке сбора данных в отчетах, но не включает эту информацию в статистику Защиты от сбора данных, отображаемую в браузере.

Эта функциональность недоступна, если приложение Kaspersky Small Office Security установлено на файловом сервере.

Запрет на сбор данных

Чтобы запретить сбор данных:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Приватность**.
3. Выберите компонент **Защита от сбора данных в интернете** и нажмите на значок .

   Откроется окно **Настройки Защиты от сбора данных в интернете**.
4. Если компонент выключен, включите его, установив переключатель в верхней части окна в положение **Вкл**.
5. Выберите вариант **Запретить сбор данных**.

   Приложение Kaspersky Small Office Security будет блокировать попытки сбора данных на всех сайтах, кроме исключений.
6. Если вы хотите запретить или разрешить сбор данных в зависимости от категорий сервисов отслеживания:

   a. По ссылке **Категории и исключения** перейдите в окно **Категории и исключения**.

   b. По умолчанию сбор данных запрещен всем категориям сервисов отслеживания и всем социальным сетям. Снимите флажки напротив категорий сервисов отслеживания и социальных сетей, которым вы хотите разрешить сбор данных.

Разрешение на сбор данных на всех сайтах

Чтобы разрешить сбор данных на всех сайтах:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Приватность**.
3. Выберите компонент **Защита от сбора данных в интернете** и нажмите на значок .

   Откроется окно **Настройки Защиты от сбора данных в интернете**.
4. Если компонент выключен, включите его, установив переключатель в верхней части окна в положение **Вкл**.
5. Выберите вариант **Только собирать статистику**.

   Приложение Kaspersky Small Office Security будет обнаруживать и подсчитывать попытки сбора данных о ваших действиях в интернете, не блокируя их. Результаты работы компонента вы сможете посмотреть в отчете.

Разрешение на сбор данных в виде исключения

В виде исключения вы можете разрешить сбор данных о своих действиях на отдельных сайтах.

Чтобы разрешить сбор данных в виде исключения:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Приватность**.
3. Выберите компонент **Защита от сбора данных в интернете** и нажмите на значок .

   Откроется окно **Настройки Защиты от сбора данных в интернете**.
4. Если компонент выключен, включите его, установив переключатель в верхней части окна в положение **Вкл**.
5. Выберите вариант **Запретить сбор данных**.

   Приложение Kaspersky Small Office Security будет блокировать попытки сбора данных на всех сайтах, кроме исключений.
6. По умолчанию в виде исключения разрешен сбор данных на сайтах "Лаборатории Касперского" и ее партнеров. Если вы хотите запретить сбор данных на этих сайтах, снимите флажок **Разрешить сбор данных на сайтах "Лаборатории Касперского" и ее партнеров**.

7. По умолчанию в виде исключения разрешен сбор данных на сайтах, о которых "Лаборатории Касперского" известно, что их работоспособность может быть нарушена в результате блокировки. Если вы хотите запретить сбор данных на этих сайтах, снимите флажок **Разрешить сбор данных на несовместимых сайтах**.

   Kaspersky Small Office Security обновляет список несовместимых сайтов по мере устранения проблем совместимости.

8. Если вы хотите указать собственные исключения, выполните следующие действия:

   a. По ссылке **Категории и исключения** перейдите в окно **Категории и исключения**.

   b. По ссылке **Исключения** перейдите в окно **Исключения Защиты от сбора данных в интернете**.

   c. Нажмите на кнопку **Добавить**.

   d. В открывшемся окне укажите адрес сайта, на котором вы хотите разрешить сбор данных, и нажмите на кнопку **OK**.

      Указанный сайт будет добавлен в список исключений.

Вы также можете разрешить сбор данных на отдельном сайте при его посещении в браузере.

Просмотр отчета о попытках сбора данных в интернете

Чтобы просмотреть отчет о попытках сбора данных в интернете:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Приватность**.
3. Выберите компонент **Защита от сбора данных в интернете** и нажмите на значок .

   Откроется окно **Настройки Защиты от сбора данных в интернете**.

   Если компонент выключен, включите его, установив переключатель в верхней части окна в положение **Вкл**.

В окне отображается сводный отчет с информацией о попытках сбора данных о ваших действиях в интернете.

Вы также можете просматривать отчет о попытках сбора данных в браузере или в отчете о работе приложения.

Управление защитой от сбора данных в браузере

Вы можете управлять компонентом Защита от сбора данных в интернете непосредственно в браузере:

- включать компонент, если он выключен;
- просматривать статистику обнаруженных попыток сбора данных;

- переходить в окно настройки Защиты от сбора данных в интернете;
- запрещать или разрешать сбор данных.

Чтобы получить доступ к управлению компонентом Защита от сбора данных в интернете,

нажмите на кнопку **Kaspersky Protection** в панели инструментов браузера.

В открывшемся меню отображается информация о работе компонента и элементы управления им.

Менеджер паролей

В некоторых регионах использование приложения Kaspersky Password Manager может регулироваться местным законодательством. Вы можете использовать Kaspersky Password Manager только в соответствии с его назначением и без нарушения местного законодательства.

Приложение Kaspersky Password Manager предназначено для безопасного хранения и синхронизации паролей между вашими устройствами. Kaspersky Password Manager нужно устанавливать независимо от Kaspersky Small Office Security.

После установки вы можете запускать Kaspersky Password Manager из меню **Пуск** (в операционных системах Microsoft Windows 7, Microsoft Windows 10), с начального экрана (в операционных системах Microsoft Windows 8, Microsoft Windows 8.1) или из окна Kaspersky Small Office Security.

Установка и запуск приложения Kaspersky Password Manager недоступны, если Kaspersky Small Office Security установлен на файловом сервере.

Как запустить Kaspersky Password Manager из окна Kaspersky Small Office Security

Чтобы запустить Kaspersky Password Manager, если он уже установлен:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Приватность**.
3. В блоке **Безопасность паролей** нажмите на кнопку **Начать**.

   Откроется окно приложения для защиты паролей Kaspersky Password Manager.

Как скачать и установить Kaspersky Password Manager

Чтобы скачать и установить приложения для защиты паролей Kaspersky Password Manager,

1. Откройте главное окно приложения.
2. Перейдите в раздел **Приватность**.
3. В блоке **Безопасность паролей** нажмите на кнопку **Посмотреть**.

   Вы перейдете на страницу, где вы сможете скачать Kaspersky Password Manager. Для установки Kaspersky Password Manager следуйте стандартной процедуре установки приложений на компьютер.

Информацию о работе с приложением Kaspersky Password Manager смотрите в *Справке Kaspersky Password Manager*.

В некоторых регионах приложение Kaspersky Password Manager может быть недоступно. Если ранее вы установили приложение Kaspersky Password Manager, мы рекомендуем сохранить ваши пароли до того, как будет выполнен переход на Kaspersky Small Office Security.

Безопасные платежи

Этот раздел содержит информацию о том, как вы можете защитить свои финансовые операции и покупки в интернете с помощью приложения Kaspersky Small Office Security.

О защите финансовых операций и покупок в интернете

Для защиты конфиденциальных данных, которые вы вводите на сайтах банков и платежных систем (например, номера банковской карты, пароли для доступа к интернет-банкам), а также для предотвращения кражи платежных средств при проведении платежей онлайн, приложение Kaspersky Small Office Security предлагает открывать такие сайты в защищенном режиме браузера. Если вы выбрали вариант открытия сайта без использования защищенного режима браузера, в течение следующих 50 минут приложение Kaspersky Small Office Security не будет предлагать вам открыть этот сайт в защищенном режиме браузера.

Защищенный режим браузера – это специальный режим работы браузера, который используется для защиты ваших данных при работе на сайтах банков или платежных систем. Защищенный режим браузера запускается в изолированной среде, чтобы другие приложения не могли внедриться в процесс защищенного режима браузера. Приложение Kaspersky Small Office Security создает специальные профили браузеров Mozilla Firefox и Google Chrome, чтобы установленные сторонние расширения не могли повлиять на работу защищенного режима браузера. Приложение не влияет на ваши данные, которые браузеры могут сохранять в созданных профилях.

При переходе в защищенный режим браузера вам будет предложено скопировать данные, настройки и плагины из основного браузера. После завершения переноса данных, приложение Kaspersky Small Office Security не будет производить синхронизацию данных между основным браузером и защищенным режимом браузера. По этой причине стоит учитывать, что, например, при удалении данных из основного браузера, информация в защищенном режиме браузера сохранится. В этом случае данные из защищенного режима браузера необходимо удалить отдельно.

Если вы используете браузеры Microsoft Edge на базе Chromium, Google Chrome, Mozilla Firefox, Internet Explorer или Opera на базе Chromium, защищенный режим браузера запускается в новом окне.

Приложение использует расширение Kaspersky Protection для включения ряда функций защищенного режима браузера.

Браузеры, не соответствующие программным требованиям, не работают в защищенном режиме браузера. Вместо таких браузеров в защищенном режиме запускается Microsoft Edge на базе Chromium или браузер, заданный в настройках приложения.

Запуск защищенного режима браузера невозможен при следующих условиях:

- снят флажок **Включить самозащиту** в окне **Настройки самозащиты** в разделе настроек **Настройки безопасности → Самозащита**;
- в браузере выключено выполнение JavaScript.

Возможности защищенного режима браузера

При работе в защищенном режиме браузера приложение предоставляет защиту от следующих видов угроз:

- Недоверенные модули. Проверка на наличие недоверенных модулей выполняется при каждом переходе на сайт банка или платежной системы.
- Руткиты. Приложение сканирует систему на наличие руткитов при запуске защищенного режима браузера.
- Недействительные сертификаты сайтов банков или платежных систем. Проверка сертификатов выполняется при переходе на сайт банка или платежной системы. Проверка сертификатов выполняется по базе скомпрометированных сертификатов.

Состояние защищенного режима браузера

Когда вы открываете сайт в защищенном режиме браузера, вокруг окна браузера появляется рамка. Цвет рамки сигнализирует о статусе защиты.

Рамка и информационная панель в нижней части окна браузера могут отображать следующие цветовые обозначения:

- Зеленый цвет рамки. Указывает на успешное завершение всех проверок. Вы можете продолжить работу в защищенном режиме браузера. Если у вас все еще есть какие-либо проблемы, нажмите кнопку конверта на информационной панели.

- Желтый цвет рамки. Означает, что проверки выявили проблемы безопасности, которые необходимо устранить, или некоторые компоненты защиты отключены. Список проблем безопасности будет отображен в правом нижнем углу окна браузера. Вы можете выполнить предлагаемые действия или закрыть эти уведомления.

  Приложение может обнаружить следующие угрозы и проблемы безопасности:

  - Недоверенный модуль. Требуется проверка компьютера и лечение.
  - Руткит. Требуется проверка компьютера и лечение.
  - Недействительный сертификат сайта банка или платежной системы.
  - Самозащита отключена.

  > Если вы не устраните обнаруженные угрозы, безопасность сеанса подключения к сайту банка или платежной системы не гарантируется. События, связанные с запуском и работой защищенного режима браузера с пониженной защитой, записываются в журнал событий Windows.

  Следующие компоненты защиты могут быть отключены:

  - Мониторинг активности
  - Защита от сетевых атак
  - Интернет-защита

- Красный цвет рамки. Означает, что Файловый Антивирус выключен. В правом нижнем углу окна браузера появится предупреждающее сообщение. Вы можете включить Файловый Антивирус или закрыть предупреждение.

О защите от создания снимков экрана

Приложение Kaspersky Small Office Security блокирует несанкционированное создание снимков экрана приложениями-шпионами, защищая ваши данные при работе с защищаемыми сайтами. Защита от создания снимков экрана включена по умолчанию. Защита от снимков экрана работает, даже если выключена аппаратная виртуализация.

О защите данных буфера обмена

Приложение Kaspersky Small Office Security блокирует несанкционированный доступ приложений к буферу обмена во время проведения платежных операций, предотвращая кражу данных злоумышленниками. Блокировка действует только в случае попыток недоверенных приложений получить несанкционированный доступ к буферу обмена. Если вы вручную копируете данные из окна одного приложения в окно другого приложения (например, из Блокнота в окно текстового редактора), доступ к буферу обмена разрешен.

Защита буфера обмена не работает, если на вашем компьютере выключена аппаратная виртуализация.

Если защищенный режим браузера запущен на операционной системе Microsoft Windows 10, приложение Kaspersky Small Office Security блокирует работу приложений универсальной платформы Windows с буфером обмена.

Как изменить настройки Безопасных платежей

Чтобы настроить Безопасные платежи:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки приватности**.
4. Нажмите на кнопку **Безопасные платежи**.

   В окне отобразятся настройки компонента Безопасные платежи.
5. Включите компонент Безопасные платежи с помощью переключателя в верхней части окна.
6. В блоке **При первом обращении к сайтам банков или платежных систем** выберите действие, которое будет выполнять приложение, когда вы впервые открываете в браузере сайт банка или платежной системы:

   - Выберите **Открывать в защищенном режиме браузера**, если хотите, чтобы приложение открывало сайт в защищенном режиме браузера.
   - Выберите **Спрашивать пользователя**, если хотите, чтобы при обращении к сайту приложение спрашивало у вас, открывать ли сайт в защищенном режиме браузера.
   - Выберите **Не открывать в защищенном режиме браузера**, если хотите, чтобы приложение не открывало сайт в защищенном режиме браузера.
7. В блоке **Дополнительно** в раскрывающемся списке **Для перехода к сайтам из окна Безопасных платежей использовать** выберите браузер, который приложение будет запускать в защищенном режиме браузера, когда вы переходите к сайту банка или платежной системы из окна Безопасных платежей.

   Вы можете выбрать один из браузеров, установленных на вашем компьютере, или использовать браузер, заданный в операционной системе по умолчанию.

Как настроить Безопасные платежи для определенного сайта

Чтобы настроить Безопасные платежи для определенного сайта:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Приватность**.

3. Перейдите в раздел **Безопасные платежи** и нажмите на кнопку **Посмотреть сайты**.

   Откроется окно **Безопасные платежи**.

4. По ссылке **Добавить вручную** откройте поля для добавления информации о сайте.

5. В поле **Веб-адрес** введите адрес сайта, который нужно открывать в защищенном режиме браузера.

   Перед адресом сайта должен быть указан протокол HTTPS (например, https://example.com), по умолчанию используемый в защищенном режиме браузера.

6. Выберите способ запуска защищенного режима браузера при открытии этого сайта:

   - Если вы хотите, чтобы сайт каждый раз открывался в защищенном режиме браузера, выберите вариант **Открывать в защищенном режиме браузера**.
   - Если вы хотите, чтобы приложение Kaspersky Small Office Security запрашивало, какое действие выполнять при открытии сайта, выберите вариант **Спрашивать пользователя**.
   - Если вы хотите выключить Безопасные платежи для этого сайта, выберите вариант **Не открывать в защищенном режиме браузера**.

7. Введите название или описание этого сайта в текстовое поле **Описание (необязательно)**.

8. Нажмите на кнопку **Добавить**.

Сайт отобразится в списке.

Как отправить отзыв о работе Безопасных платежей

Вы можете отправить в "Лабораторию Касперского" отзыв о работе компонента Безопасные платежи или сообщить о проблеме, возникшей при работе с компонентом.

Как отправить отзыв

Чтобы отправить отзыв о работе с Безопасными платежами:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Приватность**.
3. Перейдите в раздел **Безопасные платежи** и нажмите на кнопку **Посмотреть сайты**.

   Откроется окно **Безопасные платежи**.
4. По ссылке **Оставить отзыв** откройте окно, в котором вы можете написать отзыв о работе с Безопасными платежами.
5. Оцените работу Безопасных платежей по 5-балльной шкале, выбрав от 1 до 5 звезд.
6. Если вы хотите добавить к вашему отзыву комментарий, введите текст комментария в поле **Подробнее**.
7. Нажмите на кнопку **Отправить**.

Как сообщить о проблеме

Чтобы сообщить о проблеме с защищенным режимом браузера:

1. Нажмите на значок конверта в правом нижнем углу окна браузера в защищенном режиме браузера.

   Откроется окно, в котором вы можете сообщить о проблеме в работе Безопасных платежей.

2. В раскрывающемся списке выберите пункт, наиболее точно описывающий возникшую у вас проблему:

   - **Не использую**. Выберите этот элемент, если вы не используете или решили отказаться от использования Безопасных платежей.
   - **Медленно открывается сайт**. Выберите этот элемент, если сайт работает медленнее, чем в браузере, запущенном в обычном режиме.
   - **Защищенный режим браузера включается не тогда, когда нужно**. Выберите этот элемент, если в защищенном режиме браузера открываются сайты, не требующие использования Безопасных платежей.
   - **Не получается авторизоваться на сайте**. Выберите этот элемент, если при попытках авторизоваться на сайте, открытом в защищенном режиме браузера, возникают ошибки.
   - **Не открывается или неправильно отображается сайт**. Выберите этот элемент, если сайты не открываются в защищенном режиме браузера или отображаются с ошибками / искажениями.
   - **Сертификаты сайта проверяются с ошибками**. Выберите этот элемент, если при проверке сертификатов сайта появляются сообщения об ошибках.
   - **Невозможно сделать снимок экрана, если включен защищенный режим браузера**. Выберите этот элемент, если в защищенном режиме браузера не создаются скриншоты.
   - **Ошибки во время ввода данных с клавиатуры или из буфера обмена**. Выберите этот элемент, если во время ввода данных в защищенном режиме браузера возникают ошибки.
   - **Не печатается страница, открытая в защищенном режиме браузера**. Выберите этот элемент, если вы не можете распечатать открытую страницу сайта.
   - **Появляется предупреждение о том, что не установлены важные обновления операционной системы**. Выберите этот элемент, если при запуске защищенного режима браузера появляется сообщение "Не установлены важные обновления операционной системы".
   - **Защищенный режим браузера включается в другом браузере**. Выберите этот элемент, если защищенный режим браузера открывается не в том браузере, в котором вы его запустили.
   - **Работает с ошибками**. Выберите этот элемент, если при работе защищенного режима браузера возникают ошибки.
   - **Другая причина**. Выберите этот элемент, если ваша проблема не относится к указанным в других пунктах.

3. Если вы хотите сообщить в "Лабораторию Касперского" дополнительную информацию о вашей проблеме, введите ее в текстовое поле.

4. Нажмите на кнопку **Отправить**.

Если не удается отправить отзыв (например, отсутствует соединение с интернетом), приложение Kaspersky Small Office Security сохраняет отзыв на вашем компьютере. Отзывы хранятся в открытом виде в течение 30 дней.

Вы можете отправить до 10 отзывов о работе с Безопасными платежами в сутки.

Вы также можете отправить отзыв при отключении компонента Безопасные платежи. Отзыв при отключении компонента вы можете отправить один раз в месяц.

Контроль камеры и микрофона

Приложение Kaspersky Small Office Security защищает вашу камеру и микрофон от несанкционированного доступа, если включен компонент Контроль камеры и микрофона. Вы можете заблокировать все приложения или получать уведомления, когда приложение пытается получить доступ к этим устройствам. Правила доступа зависят от уровня доверия приложения, а уведомления позволяют вам реагировать в режиме реального времени, разрешая или запрещая доступ.

Если в настройках компонента включены уведомления, приложение Kaspersky Small Office Security оповещает вас о попытках какого-либо приложения получить доступ к вашей камере или микрофону. Уведомление включает в себя следующие параметры:

- **Разрешить**. Приложение будет добавлено в список приложений, которым разрешен доступ к камере или микрофону без дополнительных уведомлений.
- **Запретить**. Приложение будет добавлено в список заблокированных приложений.
- Если вы решите заблокировать микрофон или камеру и микрофон, вы получите уведомление о том, что микрофон будет заблокирован при следующей попытке подключения приложения. Чтобы немедленно заблокировать микрофон, нажмите на кнопку **Закрыть принудительно**, которая завершит процесс приложения без сохранения.
- Для настройки параметров доступа нажмите на три точки, а затем выберите вариант **Настроить Контроль камеры и микрофона**.
- Чтобы настроить правила приложения, нажмите на три точки, а затем выберите вариант **Настроить правила приложения**.
- Чтобы скрыть уведомление, нажмите кнопку закрытия.

О доступе приложений к камере и микрофону

Злоумышленники могут пытаться следить за вами с помощью камеры или подслушать ваши разговоры, получив доступ к микрофону. Приложение Kaspersky Small Office Security защищает вашу камеру и микрофон от несанкционированного доступа, если включен компонент Контроль камеры и микрофона. В настройках компонента вы можете запретить всем приложениях доступ к камере и микрофону или попросить уведомлять вас при попытке какого-либо приложения получить доступ к камере и микрофону.

Если компонент включен, но полный запрет на доступ к камере и микрофону не выбран, доступ предоставляется в зависимости от того, в какую группу доверия входит приложение, запрашивающее доступ. Блокируется доступ приложениям, которые входят в группы доверия "Сильные ограничения" и "Недоверенные".

Вы можете разрешить доступ приложениям к камере или микрофону, входящим в группы "Сильные ограничения" и "Недоверенные", в окне настройки Предотвращения вторжений. Если доступ к камере или микрофону пытается получить приложение, входящее в группу доверия "Слабые ограничения", приложение Kaspersky Small Office Security предоставляет доступ и уведомляет вас об этом, если в настройках компонента вы выбрали показ уведомления.

Уведомление не отображается, если на вашем компьютере есть приложения, запущенные в полноэкранном режиме.

Особенности работы приложения Kaspersky Small Office Security с камерой

Приложение Kaspersky Small Office Security по умолчанию разрешает доступ к камере приложениям, для которых требуется ваше разрешение, если графический интерфейс приложения находится в процессе загрузки, выгрузки или не отвечает, и вы не можете вручную разрешить доступ.

Функциональность защиты доступа к камере имеет следующие особенности и ограничения:

- Приложение Kaspersky Small Office Security контролирует видео и статические изображения, полученные в результате обработки данных камеры.
- Приложение Kaspersky Small Office Security контролирует аудиосигнал, если он является частью видеопотока, получаемого с камеры.
- Приложение Kaspersky Small Office Security контролирует только веб-камеры, подключаемые по интерфейсу USB или IEEE1394 и отображаемые в Диспетчере устройств Windows как Устройства обработки изображений (Imaging Device).

Ознакомиться со списком поддерживаемых камер вы можете по ссылке.

Чтобы защита от несанкционированного доступа к камере работала, должен быть включен компонент Предотвращение вторжений.

Защита доступа к камере имеет ограничения, если приложение установлено на операционной системе Microsoft Windows 10 Anniversary Update (RedStone 1).

Особенности работы приложения Kaspersky Small Office Security с микрофоном

Функциональность защиты микрофона имеет следующие особенности:

- Для работы функциональности необходимо, чтобы был включен компонент Предотвращение вторжений.
- При изменении настроек доступа приложения к устройствам записи звука (например, приложению было запрещено получение аудиосигнала в окне настроек Предотвращения вторжений), чтобы приложение перестало получать аудиосигнал, требуется перезапуск этого приложения.
- Приложение Kaspersky Small Office Security защищает доступ только к встроенным микрофонам и внешним микрофонам. Другие устройства передачи звука не поддерживаются.
- Приложение Kaspersky Small Office Security разрешает приложению получение аудиосигнала и не показывает никаких уведомлений, если приложение начало получать аудиосигнал до запуска приложения Kaspersky Small Office Security, или если вы поместили приложение в группу "Недоверенные" или "Сильные ограничения" после того, как приложение начало получать аудиосигнал.
- В некоторых случаях приложение Kaspersky Small Office Security определяет, что какое-либо приложение обращается к микрофону, хотя фактически микрофон к устройству не подключен.

Приложение Kaspersky Small Office Security не гарантирует защиту аудиосигнала, передаваемого с таких устройств, как DSLR-камеры, портативные видеокамеры, экшн-камеры.

Как изменить настройки доступа приложений к камере или микрофону

Чтобы изменить настройки доступа приложений к камере или микрофону:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.
   Откроется окно **Настройка**.
3. В разделе **Настройки приватности** выберите компонент **Контроль камеры и микрофона**.

4. В блоке **Настройки камеры** выберите один из вариантов действия:

   - **Запретить всем приложениям подключаться к камере**. Доступ к камере будет запрещен всем приложениям, установленным на вашем компьютере.

   - **Запрашивать подтверждение подключаться к камере**. Приложениям, которым разрешен доступ по умолчанию, будет предоставляться доступ к камере. При этом будет показано уведомление о том, что камеру использует определенное приложение.

     - **Разрешенные приложения**. При нажатии на эту ссылку открывается список приложений, имеющих доступ к камере без каких-либо уведомлений. Чтобы исключить приложение из списка, выберите его и нажмите **Удалить из списка**.

     - **Запрещенные приложения**. При нажатии на эту ссылку открывается список приложений, для которых доступ к камере заблокирован. Чтобы исключить приложение из списка, выберите его и нажмите **Удалить из списка**.

   Эта настройка недоступна, если выбран вариант действия **Запретить всем приложениям подключаться к камере**.

5. В блоке **Настройки микрофона** выберите один из вариантов действия:

   - **Запретить всем приложениям подключаться к микрофону**. Доступ к микрофону будет запрещен всем приложениям, установленным на вашем компьютере.

   - **Запрашивать подтверждение подключаться к микрофону**. Приложениям, которым разрешен доступ по умолчанию, будет предоставляться доступ к микрофону. При этом будет показано уведомление о том, что микрофон использует определенное приложение.

     - **Разрешенные приложения**. При нажатии на эту ссылку открывается список приложений, имеющих доступ к микрофону без каких-либо уведомлений. Чтобы исключить приложение из списка, выберите его и нажмите **Удалить из списка**.

     - **Запрещенные приложения**. При нажатии на эту ссылку открывается список приложений, для которых доступ к микрофону заблокирован. Чтобы исключить приложение из списка, выберите его и нажмите **Удалить из списка**.

   Эта настройка недоступна, если выбран вариант действия **Запретить всем приложениям подключаться к микрофону**.

Как разрешить или запретить доступ избранного приложения к камере

Чтобы разрешить или запретить доступ приложения к камере:

1. Откройте главное окно приложения.

2. Перейдите в раздел **Безопасность**.

3. Выберите компонент **Предотвращение вторжений**.

4. По ссылке **Управлять приложениями** перейдите в окно **Управление приложениями**.

5. Выберите приложение в списке, которому вы хотите разрешить доступ к устройствам записи звука, и откройте окно **Правила приложения** двойным щелчком мыши.

6. В окне **Правила приложения** перейдите на закладку **Права**.

7. В списке категорий прав выберите пункт **Изменение операционной системы → Подозрительные изменения в операционной системе**.

8. Выберите элемент **Доступ к камере**.

9. В графе **Действие** выберите пункт **Разрешить** или **Запретить**.

10. Нажмите на кнопку **Сохранить**.

Если выбран вариант **Запретить всем приложениям подключаться к камере**, доступ приложения к камере блокируется независимо от группы доверия и настроенного вручную разрешения.

Как разрешить или запретить доступ избранного приложения к микрофону

Чтобы разрешить или запретить доступ приложения к микрофону:

1. Откройте главное окно приложения.

2. Перейдите в раздел **Безопасность**.

3. Выберите компонент **Предотвращение вторжений**.

4. По ссылке **Управлять приложениями** перейдите в окно **Управление приложениями**.

5. Выберите приложение в списке, которому вы хотите разрешить доступ к микрофону, и откройте окно **Правила приложения** двойным щелчком мыши.

6. В окне **Правила приложения** перейдите на закладку **Права**.

7. В списке категорий прав выберите пункт **Изменение операционной системы → Подозрительные изменения в операционной системе → Доступ к устройствам записи звука**.

8. В графе **Действие** выберите пункт **Разрешить** или **Запретить**.

9. Если вы хотите получать уведомления о том, что приложению был запрещен или разрешен доступ к аудиосигналу, в графе **Действие** нажмите на значок и выберите пункт **Записывать в отчет**.

10. Нажмите на кнопку **Сохранить**.

Если выбран вариант **Запретить всем приложениям подключаться к микрофону**, доступ приложения к микрофону блокируется независимо от группы доверия и настроенного вручную разрешения.

Обнаружение сталкерских и других приложений

Некоторые легальные приложения могут использоваться злоумышленниками для кражи ваших данных и слежки за вами. Большинство этих приложений являются полезными, и многие пользователи применяют их. Среди таких приложений – IRC-клиенты, приложения автодозвона, приложения для загрузки файлов, мониторы активности компьютерных систем, утилиты для работы с паролями, интернет-серверы служб FTP, HTTP или Telnet.

Однако если злоумышленники получат доступ к таким приложениям или внедрят их на вашем компьютере, они смогут использовать некоторые их функции для кражи персональных данных и совершения других противоправных действий.

Ниже вы можете ознакомиться с разными типами программного обеспечения, которое может быть использовано злоумышленниками.

Тип	Название	Описание
Client-IRC	Клиенты интернет-чатов	Пользователи устанавливают эти приложения, чтобы общаться в ретранслируемых интернет-чатах (Internet Relay Chats). Злоумышленники используют их для распространения вредоносных приложений.
Dialer	Приложения автодозвона	Позволяют устанавливать телефонные соединения через модем в скрытом режиме. Злоумышленники могут использовать этот тип программного обеспечения для звонков с устройства пользователя, после выполнения которых жертвы могут понести материальные убытки.
Downloader	Приложения-загрузчики	Позволяют загружать файлы с веб-страниц в скрытом режиме. С помощью таких приложений злоумышленники могут загрузить вредоносное программное обеспечение на ваш компьютер.
Monitor	Приложения-мониторы	Позволяют наблюдать за активностью на компьютере, на котором установлены (видеть, какие приложения работают, и как они обмениваются данными с приложениями на других компьютерах). Могут быть использованы злоумышленниками для слежки за устройством пользователя.
PSWTool	Восстановители паролей	Позволяют просматривать и восстанавливать забытые пароли. С этой же целью их скрыто внедряют на компьютеры пользователей злоумышленники.
RemoteAdmin	Приложения удаленного администрирования	Широко используются системными администраторами; позволяют получать доступ к интерфейсу удаленного компьютера, чтобы наблюдать за ним и управлять им. С этой же целью злоумышленники скрыто внедряют их на компьютеры пользователей для наблюдения за удаленными компьютерами и управления ими. Легальные приложения удаленного администрирования отличаются от троянских приложений удаленного администрирования Backdoor. Троянские приложения обладают функциями, которые позволяют им самостоятельно проникать в систему и устанавливать себя; легальные приложения этих функций не имеют.
Server-FTP	FTP-серверы	Выполняют функции FTP-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу FTP.
Server-Proxy	Прокси-серверы	Выполняют функции прокси-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы от его имени рассылать спам.
Server-Telnet	Telnet-серверы	Выполняют функции Telnet-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу Telnet.
Server-Web	Веб-серверы	Выполняют функции веб-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу HTTP.
RiskTool	Инструменты для работы на локальном компьютере	Дают пользователю дополнительные возможности при работе на своем компьютере (позволяют скрывать на своем компьютере файлы или окна активных приложений, закрывать активные процессы). К этой группе относятся майнеры, которые могут быть установлены скрыто от пользователя и потреблять большое количество ресурсов компьютера. Все описанные выше действия могут использоваться злоумышленниками для сокрытия или затруднения обнаружения внедрённого вредоносного программного обеспечения.

Тип	Название	Описание
NetTool	Сетевые инструменты	Дают пользователю компьютера, на котором установлены, дополнительные возможности при работе с другими компьютерами в сети (позволяют перезагружать их, находить открытые порты, запускать установленные на них приложения). Все перечисленные выше действия могут быть использованы в злонамеренных целях.
Client-P2P	Клиенты пиринговых сетей	Позволяют работать в пиринговых (Peer-to-Peer) сетях. Могут использоваться злоумышленниками для распространения вредоносных приложений.
Client-SMTP	SMTP-клиенты	Отправляют сообщения электронной почты в скрытом режиме. Злоумышленники внедряют их на компьютер пользователя, чтобы от его имени рассылать спам.
WebToolbar	Веб-панели инструментов	Добавляют в интерфейс других приложений панели инструментов для использования поисковых систем. Часто распространяется с помощью вредоносных или рекламных программ.

Вы можете включить защиту от сталкерских и других приложений, которые могут быть использованы злоумышленниками, и мы предупредим вас, если обнаружим такие приложения.

Чтобы включить защиту от сталкерских и других приложений

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Перейдите в раздел **Настройки безопасности** → **Исключения и действия с найденными объектами**.
4. В разделе **Сталкерские и другие приложения** установите флажки:

   - **Обнаруживать сталкерские приложения**

     Для защиты от приложений, с помощью которых злоумышленники могут получить доступ к вашему местоположению и переписке, а также информации о том, какие сайты и соцсети вы посещаете.

   - **Обнаруживать легальные приложения, которые злоумышленники могут использовать для нанесения вреда компьютеру или вашим данным**

     Для защиты от приложений, с помощью которых злоумышленники могут загрузить вредоносное программное обеспечение на ваш компьютер или использовать ресурсы вашего компьютера в своих целях. Kaspersky Small Office Security не обнаруживает приложения удаленного администрирования, которые считаются доверенными.

Если данные флажки не установлены, вы можете получать уведомления о некоторых приложениях из таблицы выше, поскольку они включены в специальные категории и обрабатываются по умолчанию вне зависимости от настроек приложения, например: RemoteAdmin, PSWTool, Monitor.

Анти-Баннер

Этот раздел содержит информацию о том, как с помощью приложения Kaspersky Small Office Security защитить вас от рекламных баннеров в интернете.

Об Анти-Баннере

Для защиты от баннеров в интернете предназначен компонент Анти-Баннер. Анти-Баннер блокирует отображение баннеров на просматриваемых вами сайтах и в интерфейсе некоторых компьютерных приложений. Анти-Баннер блокирует баннеры из списка известных баннеров, который входит в состав баз Kaspersky Small Office Security. Вы можете управлять блокировкой баннеров через интерфейс Kaspersky Small Office Security или непосредственно в браузере.

По умолчанию баннеры разрешены на сайтах из списка **Сайты "Лаборатории Касперского"**. Список составляется специалистами "Лаборатории Касперского" и включает в себя сайты "Лаборатории Касперского" и сайты партнеров компании, на которых размещена реклама "Лаборатории Касперского". Вы можете просмотреть список, а также выключить использование этого списка, если считаете нужным блокировать баннеры на сайтах "Лаборатории Касперского" и ее партнеров.

Счетчик заблокированных баннеров отображает общее количество блокировок по всему сайту в зависимости от того, сколько страниц сайта открыто в браузере. Если в браузере открыта одна страница, считаются только блокировки на этой странице сайта. Если в браузере открыто несколько страниц одного сайта, считаются заблокированные баннеры на всех страницах сайта, открытых в браузере.

Информация о работе Анти-Баннера доступна в отчетах.

Анти-Баннер имеет следующие ограничения:

Анти-Баннер имеет следующие ограничения:

- Некоторые сайты определяют, что реклама на их страницах блокируется, и не показывают контент до тех пор, пока пользователь не выключит блокировщик рекламы. Чтобы просмотреть содержимое такого сайта, вам нужно добавить адрес этого сайта в исключения.
- Если веб-страницу, на которой расположен баннер, не удалось определить, то приложение Kaspersky Small Office Security не блокирует такой баннер и не отображает информацию о нем.
- Если веб-страницу, на которой расположен баннер, удалось определить, но не удалось сопоставить ни с одной веб-страницей, открытой в браузере, то приложение Kaspersky Small Office Security запрещает или разрешает отображение баннера с учетом информации о веб-странице, которую удалось определить. Приложение отображает информацию о баннере в отчетах, но не включает эту информацию в статистику Анти-Баннера, отображаемую в браузере.
- В статистике Анти-Баннера, отображаемой в браузере, могут учитываться баннеры, заблокированные при предыдущих загрузках веб-страницы, в том числе баннеры, заблокированные ранее и загруженные повторно.
- В статистике Анти-Баннера, отображаемой в браузере, не учитываются баннеры, заблокированные в динамическом содержимом страницы после загрузки сайта.
- В связи с тем, что некоторые функции Java Script не поддерживаются браузером Internet Explorer, Kaspersky Small Office Security не может заблокировать некоторые баннеры в этом браузере.

Эта функциональность недоступна, если приложение Kaspersky Small Office Security установлено на файловом сервере.

Как включить компонент Анти-Баннер

По умолчанию компонент Анти-Баннер выключен. Вы можете включить его в приложении Kaspersky Small Office Security или с помощью расширения Kaspersky Protection в браузере.

Как включить Анти-Баннер в приложении Kaspersky Small Office Security

Чтобы включить компонент Анти-Баннер в приложении Kaspersky Small Office Security:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.
   Откроется окно **Настройка**.
3. Выберите раздел **Настройки приватности**.
4. Выберите компонент Анти-Баннер.
   Откроется окно **Настройки Анти-Баннера**.
5. Включите компонент с помощью переключателя в верхней части окна.

Как включить Анти-Баннер в окне браузера

Чтобы включить компонент Анти-Баннер в окне браузера:

1. Нажмите на кнопку **Kaspersky Protection** в панели инструментов браузера.
2. В раскрывшемся меню в блоке **Анти-Баннер** нажмите на кнопку **Включить**.

После включения или выключения Анти-Баннера необходимо перезагрузить веб-страницу в браузере, чтобы изменения вступили в силу.

Запрет баннеров

Анти-Баннер блокирует на сайтах баннеры из списка известных баннеров, который входит в состав баз приложения Kaspersky Small Office Security. Если баннер на веб-странице отображается, несмотря на работающий Анти-Баннер, это может означать, что баннер не входит в список известных баннеров. Вы можете самостоятельно запретить отображение этого баннера.

Чтобы запретить баннер, нужно добавить его в список запрещенных баннеров. Вы можете сделать это непосредственно на веб-странице или в приложении Kaspersky Small Office Security.

Если баннер находится на сайте из списка сайтов с разрешенными баннерами, вы не можете запретить отображение этого баннера.

Как запретить баннер, находясь на веб-странице

Чтобы запретить баннер, находясь на веб-странице:

1. Убедитесь, что в браузере установлено и включено расширение Kaspersky Protection.
2. Если Анти-Баннер выключен, включите его:
   a. Нажмите на кнопку **Kaspersky Protection** в панели инструментов браузера.
   b. В раскрывшемся меню в блоке **Анти-Баннер** нажмите на кнопку **Включить**.
3. Наведите курсор мыши на баннер, который вы хотите запретить, и нажмите на правую клавишу мыши.
4. В появившемся контекстном меню выберите пункт **Добавить в Анти-Баннер**.
   Откроется окно **Добавление запрещенного баннера**.
5. В окне **Добавление запрещенного баннера** нажмите на кнопку **Добавить**.
   Адрес баннера будет добавлен в список запрещенных баннеров.
6. Обновите веб-страницу в браузере, чтобы баннер перестал отображаться.

При последующих переходах на эту веб-страницу баннер не будет отображаться.

Как запретить баннер в приложении Kaspersky Small Office Security

Чтобы запретить баннер в приложении Kaspersky Small Office Security:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки приватности**.
4. Выберите компонент Анти-Баннер.

   Откроется окно **Настройки Анти-Баннера**.
5. Включите компонент Анти-Баннер с помощью переключателя в верхней части окна.
6. В окне **Настройки Анти-Баннера** по ссылке **Запрещенные баннеры** перейдите в окно **Запрещенные баннеры**.
7. В окне **Запрещенные баннеры** нажмите на кнопку **Добавить**.
8. В открывшемся окне в поле **Маска веб-адреса (URL)** введите адрес или маску адреса баннера.
9. В качестве статуса для этого баннера укажите **Активно**.
10. Нажмите на кнопку **OK**.

    Приложение Kaspersky Small Office Security будет блокировать указанный баннер.

Разрешение баннеров

Вы можете разрешить как отдельный баннер, так и все баннеры на указанном вами сайте.

Как разрешить отдельный баннер

Чтобы разрешить отдельный баннер:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки приватности**.
4. Выберите компонент Анти-Баннер.

   Откроется окно **Настройки Анти-Баннера**.
5. Включите компонент Анти-Баннер с помощью переключателя в верхней части окна.
6. В окне **Настройки Анти-Баннера** по ссылке **Сайты с разрешенными баннерами** перейдите в окно **Сайты с разрешенными баннерами**.
7. В окне **Сайты с разрешенными баннерами** нажмите на кнопку **Добавить**.
8. В открывшемся окне в поле **Сайт** введите адрес или маску адреса баннера.
9. Выберите статус **Активно**.
10. Нажмите на кнопку **OK**.

Приложение не будет блокировать указанный баннер.

Если баннер добавлен в список разрешенных баннеров, но на сайте баннер находится внутри рекламного блока, свойства которого приводят к его блокировке Анти-Баннером, такой баннер будет заблокирован вместе с рекламным блоком.

Как разрешить все баннеры на сайте

Чтобы разрешить все баннеры на сайте:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки приватности**.
4. Выберите компонент Анти-Баннер.

   Откроется окно **Настройки Анти-Баннера**.
5. Включите компонент Анти-Баннер с помощью переключателя в верхней части окна.
6. В окне **Настройки Анти-Баннера** по ссылке **Сайты с разрешенными баннерами** перейдите в окно **Сайты с разрешенными баннерами**.
7. В окне **Сайты с разрешенными баннерами** нажмите на кнопку **Добавить**.
8. В открывшемся окне в поле **Сайт** введите веб-адрес, например, `example.com`.
9. Выберите статус **Активно**.
10. Нажмите на кнопку **OK**.

    Сайт будет добавлен в список сайтов с разрешенными баннерами. Kaspersky Small Office Security не блокирует баннеры на сайтах из этого списка, даже если баннер добавлен в список запрещенных баннеров.

Как настроить фильтры Анти-Баннера

Чтобы настроить фильтры Анти-Баннера:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки приватности**.
4. Выберите компонент Анти-Баннер.

   Откроется окно **Настройки Анти-Баннера**.
5. Включите компонент Анти-Баннер с помощью переключателя в верхней части окна.

6. По ссылке **Список фильтров** перейдите в окно **Список фильтров**.

7. В окне **Список фильтров** выполните настройку фильтров:

   - **Рекомендуемые**. В эту группу входят базовый и языковой фильтр, соответствующий вашему региону. Эти фильтры включены по умолчанию.

   - **Тематические**. В эту группу входят два фильтра:

     - **Виджеты социальных сетей**. Включите этот фильтр, если вы хотите блокировать на сайтах социальных сетей такие кнопки как "Нравится" или "Поделиться".

     - **Нежелательные элементы**. Включите этот фильтр, если вы хотите блокировать всплывающие сообщения, окна и прочие элементы, не относящиеся к сайту.

   - **Языковые дополнения**. В этой группе фильтров вы можете выбрать язык. Приложение будет блокировать баннеры на сайтах указанного языка.

Как управлять Анти-Баннером в браузере

Вы можете управлять компонентом Анти-Баннер непосредственно в браузере с помощью расширения Kaspersky Protection.

Расширение Kaspersky Protection позволяет выполнять следующие действия:

- включать и выключать компонент;
- просматривать статистику заблокированных баннеров;
- переходить в окно настройки Анти-Баннера;
- просматривать информацию о том, запрещены или разрешены баннеры на сайте, открытом в браузере, и управлять отображением баннеров на сайте.

Как управлять компонентом Анти-Баннер через расширение Kaspersky Protection

Чтобы получить доступ к управлению компонентом Анти-Баннер через расширение Kaspersky Protection,

нажмите на кнопку **Kaspersky Protection** в панели инструментов браузера.

В открывшемся меню отображается информация о работе компонента и элементы управления им.

Блокировщик скрытых установок

Бывает, что вы устанавливаете приложение, а потом обнаруживаете, что вместе с этим приложением установились еще несколько дополнительных приложений, которые вы не запрашивали. Знакомая ситуация? Такие приложения устанавливаются незаметно и могут спамить вас рекламой и даже изменять браузер по умолчанию.

Включите **Блокировщик скрытых установок**, чтобы навсегда забыть об этой проблеме. Блокировщик скрытых установок будет сам снимать флажки с приложений, предлагаемых к дополнительной установке, чтобы вам не приходилось делать это вручную.

Также вы можете включить Блокировщик скрытых установок в окне настройки Менеджера приложений.

Для этого установите флажок **Во время установки приложений автоматически снимать флажки установки дополнительных приложений. Предупреждать при попытке установить дополнительные приложения**.

Удалять рекламные приложения

Раздражает реклама? Приложение Kaspersky Small Office Security удаляет с вашего компьютера приложения, которые показывают рекламу в браузерах и на рабочем столе. Помимо рекламы мы также удалим за вас приложения автодозвона и упакованные файлы, которые могут содержать вирусы и другие угрозы. Включите функцию **Удалять рекламные приложения**, чтобы никогда больше не видеть навязчивую рекламу.

Чтобы удалить рекламные приложения:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Приватность**.
3. Включите функцию **Удалять рекламные приложения**.

Как изменить настройки Менеджера приложений

Чтобы изменить настройки Менеджера приложений:

1. Откройте главное окно приложения.
2. Выберите раздел **Приватность**.
3. В блоке **Блокировщик скрытых установок** нажмите на кнопку .
   Будет выполнен переход в окно **Настройки Менеджера приложений**.

4. В блоке настроек **Блокировщик скрытых установок** установите флажок **Во время установки приложений автоматически снимать флажки установки дополнительных приложений. Предупреждать при попытке установить дополнительные приложения**, чтобы запретить установку дополнительного программного обеспечения при установке новых приложений. Если при установке нового приложения будут предотвращены нежелательные действия, приложение Kaspersky Small Office Security уведомит вас об этом.

   Если флажок **Во время установки приложений автоматически снимать флажки установки дополнительных приложений. Предупреждать при попытке установить дополнительные приложения** снят после того, как вы уже запустили установку какого-либо приложения, блокировщик скрытых установок продолжит свою работу в рамках текущей установки. Флажки напротив приложений, предлагаемых к дополнительной установке, будут сняты, а сами дополнительные приложения не будут устанавливаться. При последующей установке приложений эта функциональность работать не будет. Дополнительные приложения будут устанавливаться совместно с основным.

5. Установите флажок **Не отображать шаги установки, которые могут содержать рекламу или предложения об установке дополнительных приложений**, чтобы запретить показ шагов установки, содержащих рекламу, во время установки на компьютер новых приложений. Если такие шаги установки будут удалены, приложение Kaspersky Small Office Security уведомит вас об этом.

Секретная папка

Этот раздел содержит информацию о том, как вы можете защитить данные с помощью секретных папок.

О секретной папке

Для защиты ваших конфиденциальных данных от несанкционированного доступа предназначены секретные папки. *Секретная папка* – это хранилище данных на вашем компьютере, которое вы можете открывать или закрывать с помощью известного только вам пароля. Для изменения файлов, хранящихся в секретной папке, требуется ввести пароль. Если вы ввели неверный пароль 10 раз подряд, доступ к секретной папке блокируется на один час.

Если вы потеряете или забудете пароль, восстановить данные будет невозможно.

Для создания секретной папки в приложении Kaspersky Small Office Security используется алгоритм шифрования данных AES XTS с эффективной длиной ключа 56 бит.

Если на вашем компьютере используется файловая система FAT32, вы можете создавать секретные папки объемом не более 4 ГБ.

Как поместить файлы в секретную папку

Чтобы поместить файлы в секретную папку:

1. Откройте главное окно приложения Kaspersky Small Office Security.
2. Перейдите в раздел **Приватность**.
3. В блоке **Секретная папка** выполните одно из следующих действий:

Если у вас еще нет секретной папки

1. Нажмите на кнопку **Создать папку**.
2. В окне **Секретная папка** нажмите на кнопку **Добавить** и выберите файлы в Проводнике или перетащите файлы в окно приложения Kaspersky Small Office Security.

   Выбранные файлы отобразятся в окне **Секретная папка**.
3. Нажмите на кнопку **Продолжить**.
4. Введите название секретной папки и укажите ее расположение или используйте значения этих настроек по умолчанию.
5. Укажите размер секретной папки.
6. Для получения быстрого доступа к секретной папке установите флажок **Создать ярлык папки на рабочем столе**.
7. Нажмите на кнопку **Продолжить**.
8. Заполните поля **Пароль для доступа к секретной папке** и **Подтверждение пароля** и нажмите на кнопку **Продолжить**.
9. Выберите действие с исходными копиями файлов вне секретной папки:
   - Чтобы удалить исходные копии файлов вне секретной папки, нажмите на кнопку **Удалить**.
   - Чтобы сохранить исходные копии файлов вне секретной папки, нажмите на кнопку **Пропустить**.
10. Нажмите на кнопку **Готово**.

    В списке секретных папок отобразится созданная вами секретная папка.
11. Чтобы закрыть секретную папку, нажмите на кнопку **Закрыть**.

    Данные в закрытой секретной папке будут доступны только после ввода пароля.

Если у вас уже есть секретная папка

1. По ссылке **У меня уже есть секретная папка** перейдите в окно **Секретная папка**.
2. В окне **Секретная папка** выберите нужную секретную папку и нажмите на кнопку **Открыть**.
3. Введите пароль доступа к секретной папке и нажмите на кнопку **Открыть в Проводнике**.

   Секретная папка откроется в Проводнике.
4. Перетащите нужные файлы в секретную папку.
5. Закройте окно Проводника.
6. В приложении Kaspersky Small Office Security в окне **Секретная папка** нажмите на кнопку **Закрыть**.

При добавлении в секретную папку файлов с одинаковыми названиями, написанными в разных регистрах, один из таких файлов может быть недоступен при попытке открытия секретной папки. Чтобы избежать потери данных, мы рекомендуем добавлять такие файлы в разные секретные папки или поменять названия файлов на полностью уникальные.

Как получить доступ к файлам, хранящимся в секретной папке

Чтобы получить доступ к файлам, хранящимся в секретной папке:

1. Откройте главное окно приложения Kaspersky Small Office Security.
2. Перейдите в раздел **Приватность**.
3. В блоке **Секретная папка** нажмите на кнопку **У меня уже есть секретная папка**.

   Откроется окно **Секретная папка**.
4. Нажмите на кнопку **Открыть** рядом с секретной папкой.
5. Введите пароль и нажмите на кнопку **Открыть в Проводнике**.

Файлы, сохраненные в секретной папке, отобразятся в окне Проводника. Вы можете внести необходимые изменения в файлы, или добавить новые файлы, и снова закрыть секретную папку.

Начиная с версии Kaspersky Small Office Security 8, при переименовании секретной папки появляется ошибка при попытке открытия такой секретной папки. Чтобы этого избежать, мы рекомендуем открыть секретную папку, которую вы хотите переименовать, извлечь ваши данные и создать новую секретную папку с этими данными, назвав ее другим именем.

Чтобы открыть секретные папки, созданные в предыдущей версии приложения, вам нужно выполнить конвертацию секретных папок старого формата в новый формат. Приложение предложит вам выполнить конвертацию при попытке открыть секретную папку в Kaspersky Small Office Security.

Конвертация секретных папок в новый формат зависит от размера секретных папок и может занимать значительное время.

Если при удалении Kaspersky Small Office Security в окне **Сохранить следующие данные на этом компьютере для повторного использования** флажок **Настройки работы приложения** снят, а флажок **Секретная папка** установлен, при последующей установке текущей или новой версии Kaspersky Small Office Security секретные папки нужно будет добавить вручную по ссылке **У меня уже есть папка** в окне **Секретная папка**.

Если вы не установили последнее обновление для Kaspersky Small Office Security, при обновлении на новую версию секретные папки, созданные в предыдущей версии приложения, могут быть недоступны.

Уничтожитель файлов

Дополнительная безопасность персональных данных обеспечивается защитой от несанкционированного восстановления удаленной информации злоумышленниками.

В состав приложения Kaspersky Small Office Security входит инструмент для удаления данных без возможности восстановления обычными программными средствами.

Приложение Kaspersky Small Office Security позволяет удалять данные без возможности восстановления со следующих носителей информации:

- Локальные диски. Удаление возможно, если у вас есть права на запись и удаление информации.
- Внешние диски или другие устройства, которые распознаются как внешние диски (например, дискеты, карты памяти, USB-карты или мобильные телефоны). Удаление данных с карт памяти возможно, если на них механически не включен режим защиты от записи.

Вы можете удалять те данные, доступ к которым разрешен под вашей учетной записью. Перед удалением данных требуется убедиться, что эти данные не используются работающими приложениями.

Чтобы удалить данные без возможности восстановления:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Приватность**.
3. В блоке **Уничтожитель файлов** нажмите на кнопку **Выбрать файлы**.

   Откроется окно **Уничтожитель файлов**.
4. Нажмите на кнопку **Обзор** и в открывшемся окне **Выберите файлы для удаления** выберите папку или файл для удаления без возможности восстановления.

   Удаление системных файлов может вызвать сбои в работе операционной системы.

5. В раскрывающемся списке **Метод удаления данных** выберите нужный метод удаления данных.

Для удаления данных с SSD- и USB-устройств рекомендуется применять методы **Быстрое удаление (рекомендуется)** или **ГОСТ Р 50739-95, Россия**. Остальные методы удаления могут нанести вред SSD- или USB-устройству.

- **Быстрое удаление (рекомендуется)**. Процесс удаления состоит из двух циклов перезаписи данных: записи нулей и псевдослучайных чисел. Основное достоинство этого алгоритма – скорость выполнения. Быстрое удаление позволяет предотвратить восстановление данных с помощью стандартных утилит восстановления.
- **ГОСТ Р 50739-95, Россия**. Алгоритм проводит один цикл перезаписи данных псевдослучайными числами и защищает от восстановления данных стандартными средствами. Этот алгоритм соответствует второму классу защищенности из шести по классификации Государственной технической комиссии.
- **Алгоритм Брюса Шнайера**. Процесс состоит из семи циклов перезаписи данных. Метод отличается от немецкого VSITR последовательностью перезаписи. Этот усовершенствованный метод удаления информации считается одним из наиболее надежных.
- **Стандарт VSITR, Германия**. Проводятся семь циклов перезаписи данных. Алгоритм считается надежным, но его выполнение занимает значительное время.
- **Стандарт NAVSO P-5239-26 (MFM), США** и **Стандарт NAVSO P-5239-26 (RLL), США**. Используются три цикла перезаписи данных. Стандарты различаются последовательностью перезаписи информации.
- **Стандарт 5250.22-M, США**. Используются три цикла перезаписи. Этот стандарт применяется Министерством обороны США.

6. Нажмите на кнопку **Удалить**.

7. В открывшемся окне подтверждения удаления нажмите на кнопку **Удалить**.

Файлы, используемые сторонним приложением, не могут быть удалены.

Удаление следов активности

При работе на компьютере действия пользователя регистрируются в операционной системе. При этом сохраняется следующая информация:

- данные о введенных пользователем поисковых запросах и посещенных сайтах;
- сведения о запуске приложений, открытии и сохранении файлов;
- записи в системном журнале Microsoft Windows;
- другая информация о действиях пользователя.

Сведения о действиях пользователя, содержащие конфиденциальные данные, могут оказаться доступными злоумышленникам и посторонним лицам.

В состав приложения входит:

- Мастер устранения следов активности пользователя, очищающий следы активности пользователей в операционной системе.
- Мастер восстановления настроек отменит изменения, которые были сделаны в результате предыдущей работы мастера устранения следов активности. Этот вариант действия доступен, если в результате предыдущей работы мастера следы активности были устранены.

Чтобы запустить мастер устранения следов активности:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Приватность**.
3. В блоке **Удаление следов активности** нажмите на кнопку **Найти**.
4. Затем вас попросят закрыть все окна браузера и продолжить.
5. Мастер выполняет поиск следов активности на вашем компьютере. Это может занять некоторое время. По завершении поиска мастер автоматически переходит к следующему шагу.
6. Если вам необходимо включить автоматическое удаление следов активности, переведите переключатель **Автоматическое удаление следов активности** в положение **Вкл**, создайте расписание сеансов очистки и укажите свою учетную запись Windows и пароль.
7. В блоке **Выберите действия** укажите, какие данные необходимо удалить, и нажмите на кнопку **Сохранить и удалить** или на кнопку **Удалить**, если вы не меняли список действий.

   Для просмотра действий, включенных в группу, раскройте список выбранной группы. Чтобы мастер выполнил какое-либо действие, установите флажок напротив названия действия. По умолчанию выполняются все рекомендуемые и настоятельно рекомендуемые действия. Если вы не хотите выполнять какое-либо действие, снимите флажок рядом с ним.

   > Настоятельно не рекомендуется снимать флажки, установленные по умолчанию, поскольку в результате этого действия безопасность вашего компьютера останется под угрозой.

8. Мастер выполняет действия, выбранные на предыдущем шаге. Удаление следов активности может занять некоторое время. Для устранения некоторых следов активности может потребоваться перезагрузка компьютера, о чем мастер вас уведомит.

Чтобы запустить мастер восстановления настроек:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Приватность**.
3. В блоке **Удаление следов активности** нажмите на кнопку **Восстановить настройки**.
4. Мастер выполняет поиск измененных настроек. Это может занять некоторое время. По завершении поиска мастер автоматически переходит к следующему шагу.

5. Выберите, какие настройки необходимо восстановить, и нажмите на кнопку **Восстановить**.

6. После этого вы получите уведомление о завершении операции. Выполнение операции может занять некоторое время. Для устранения некоторых следов активности может потребоваться перезагрузка компьютера, о чем мастер вас уведомит.

Защита персональных данных в интернете

Этот раздел содержит информацию о том, как сделать работу в интернете безопасной и защитить ваши данные от кражи.

О защите персональных данных в интернете

С помощью Kaspersky Small Office Security вы можете защитить от кражи свои персональные данные:

- пароли, имена пользователя и другие регистрационные данные;
- номера счетов и банковских карт.

В состав Kaspersky Small Office Security входят компоненты и инструменты, позволяющие защитить ваши персональные данные от кражи злоумышленниками, использующими такие методы как фишинг и перехват данных, вводимых с клавиатуры.

Для защиты от фишинга предназначен Анти-Фишинг, включенный в состав компонентов Интернет защита. Включите эти компоненты, чтобы обеспечить максимально эффективную защиту от фишинга.

Для защиты от перехвата данных, введенных с клавиатуры, предназначена Экранная клавиатура и защита ввода данных с аппаратной клавиатуры.

Для удаления информации о действиях пользователя на компьютере предназначен мастер устранения следов активности.

Для защиты данных при использовании сервисов интернет-банкинга и при оплате покупок в интернет-магазинах предназначены функции Безопасных платежей и Безопасного VPN-соединения.

> Функциональность Безопасное VPN-соединение доступна не во всех регионах.

Для защиты от пересылки персональных данных через интернет предназначен один из инструментов Веб-Контроля.

Об Экранной клавиатуре

При работе в интернете часто возникают ситуации, когда необходимо указать персональные данные, а также имя пользователя и пароль. Это происходит, например, при регистрации на сайтах, совершении покупок в интернет-магазинах, использовании интернет-банкинга.

В таких случаях существует опасность перехвата персональных данных с помощью аппаратных перехватчиков или клавиатурных шпионов – приложений, регистрирующих нажатие клавиш. Экранная клавиатура позволяет избежать перехвата данных, вводимых с клавиатуры.

Эта функциональность недоступна, если приложение Kaspersky Small Office Security установлено на файловом сервере.

Многие приложения-шпионы обладают функциями снятия снимков экрана, которые автоматически передаются злоумышленнику для последующего анализа и извлечения персональных данных пользователя. Экранная клавиатура защищает вводимые персональные данные от перехвата посредством снятия снимков экрана.

Экранная клавиатура имеет следующие особенности:

- На клавиши Экранной клавиатуры нужно нажимать с помощью мыши.
- В отличие от настоящей клавиатуры, на Экранной клавиатуре невозможно одновременно нажать несколько клавиш. Поэтому, чтобы использовать комбинации клавиш (например, **ALT**+**F4**), нужно сначала нажать на первую клавишу (например, **ALT**), затем на следующую (например, **F4**), а затем повторно нажать на первую клавишу. Повторное нажатие заменяет отпускание клавиши на настоящей клавиатуре.
- На Экранной клавиатуре язык ввода переключается с помощью того же сочетания клавиш, которое установлено в настройках операционной системы для обычной клавиатуры. При этом на вторую клавишу нужно нажимать правой клавишей мыши (например, если в настройках операционной системы для переключения языка ввода задана комбинация **LEFT ALT**+**SHIFT**, то на клавишу **LEFT ALT** нужно нажимать левой клавишей мыши, а на клавишу **SHIFT** нужно нажимать правой клавишей мыши).

Использование Экранной клавиатуры имеет следующие ограничения:

- Экранная клавиатура защищает от перехвата персональных данных только при работе с браузерами Microsoft Edge на базе Chromium, Mozilla Firefox, Google Chrome и Opera на базе Chromium. При работе с другими браузерами Экранная клавиатура не защищает вводимые персональные данные от перехвата.
- Экранная клавиатура не может защитить ваши персональные данные в случае взлома сайта, требующего ввода таких данных, поскольку в этом случае информация попадет непосредственно в руки злоумышленников.
- Экранная клавиатура не предотвращает снятие снимков экрана с помощью нажатия клавиши **Print Screen** и других комбинаций клавиш, заданных в настройках операционной системы.
- Приложение Kaspersky Small Office Security не защищает от создания снимков экрана в операционной системе Microsoft Windows 8 и 8.1 (только 64-разрядные), если открыто окно Экранной клавиатуры, но не запущен процесс защищенного режима браузера.

В списке выше перечислены основные ограничения, которые имеет функциональность защиты ввода данных. Полный перечень ограничений приводится в статье на сайте Службы технической поддержки "Лаборатории Касперского". В статье перечислены ограничения на защиту ввода с аппаратной клавиатуры в Kaspersky Internet Security, эти ограничения распространяются и на Экранную клавиатуру в Kaspersky Small Office Security.

Как открыть Экранную клавиатуру

Открыть Экранную клавиатуру можно следующими способами:

- из панели инструментов браузеров Microsoft Edge на базе Chromium, Mozilla Firefox, Google Chrome или Opera на базе Chromium;
- с помощью значка быстрого вызова Экранной клавиатуры в полях ввода на сайтах;

  Отображение значка быстрого вызова в полях ввода на сайтах можно настроить.

  При использовании Экранной клавиатуры приложение Kaspersky Small Office Security отключает функцию автозаполнения полей ввода на сайтах.

- с помощью комбинации клавиш аппаратной клавиатуры.

Запуск Экранной клавиатуры из панели инструментов браузера

Чтобы открыть Экранную клавиатуру из панели инструментов браузеров Microsoft Edge на базе Chromium, Mozilla Firefox, Google Chrome или Opera на базе Chromium:

1. Нажмите на кнопку **Kaspersky Protection** в панели инструментов браузера.
2. В раскрывшемся меню выберите пункт **Экранная клавиатура**.

Запуск Экранной клавиатуры с помощью аппаратной клавиатуры

Чтобы открыть Экранную клавиатуру с помощью аппаратной клавиатуры,

нажмите комбинацию клавиш **CTRL**+**ALT**+**SHIFT**+**P**.

Экранная клавиатура не запускается при нажатии на эту комбинацию клавиш, если эта комбинация клавиш уже зарегистрирована в другом приложении, например, Microsoft Word.

Как настроить отображение значка Экранной клавиатуры

Чтобы настроить отображение значка быстрого вызова Экранной клавиатуры в полях ввода на сайтах:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки приватности**.

4. В окне **Настройки приватности** нажмите на кнопку **Защита ввода данных**.

   В окне отобразятся настройки защиты ввода данных.

5. В блоке **Экранная клавиатура** установите флажок **Открывать Экранную клавиатуру по комбинации клавиш CTRL+ALT+SHIFT+P**.

6. Если вы хотите, чтобы значок вызова Экранной клавиатуры отображался в полях ввода на всех сайтах, установите флажок **Показывать значок быстрого вызова в полях ввода**.

7. Если вы хотите, чтобы значок вызова Экранной клавиатуры отображался только при открытии сайтов определенных категорий, установите флажки для категорий сайтов, на которых нужно отображать значок вызова Экранной клавиатуры в полях ввода.

   Значок вызова Экранной клавиатуры будет отображаться при открытии сайта, относящегося к какой-либо из выбранных категорий.

8. Если вы хотите включить или выключить отображение значка вызова Экранной клавиатуры на определенном сайте, выполните следующие действия:

   a. В блоке **Экранная клавиатура** по ссылке **Настройка исключений** перейдите в окно **Исключения для Экранной клавиатуры**.

   b. В нижней части окна нажмите на кнопку **Добавить**.

   c. Откроется окно для добавления исключения для Экранной клавиатуры.

   d. Введите адрес сайта в поле **Маска веб-адреса**.

   e. В блоке **Область применения** укажите, где должен отображаться (или не отображаться) значок вызова Экранной клавиатуры: на указанной странице или на всех страницах сайта.

   f. В блоке **Значок Экранной клавиатуры** укажите, должен ли отображаться или нет значок вызова Экранной клавиатуры.

   g. Нажмите на кнопку **OK**.

      Указанный сайт появится в списке в окне **Исключения для Экранной клавиатуры**.

При открытии указанного сайта значок вызова Экранной клавиатуры будет отображаться в полях ввода в соответствии с настройками.

О защите ввода данных с аппаратной клавиатуры

Защита ввода данных с аппаратной клавиатуры позволяет избежать перехвата данных, которые вы вводите с клавиатуры на сайтах. Чтобы защита ввода данных с аппаратной клавиатуры работала, в браузере должно быть активировано расширение Kaspersky Protection. Вы можете настроить защиту ввода данных с клавиатуры на разных сайтах. После того как защита ввода данных с клавиатуры настроена, рядом с полем, в котором установлен курсор, отображается всплывающее сообщение о том, что защита ввода данных с клавиатуры включена. По умолчанию защита ввода данных включена для всех категорий сайтов, кроме сайтов категории "Общение в сети".

Эта функциональность недоступна, если приложение Kaspersky Small Office Security установлено на файловом сервере.

Ограничения защиты ввода данных

Защита ввода данных в Kaspersky Small Office Security имеет следующие ограничения:

- Защита ввода данных с аппаратной клавиатуры не работает в браузерах, запущенных в приложении Sandboxie.
- Защита ввода данных с аппаратной клавиатуры не может защитить ваши персональные данные в случае взлома сайта, требующего ввода таких данных, поскольку в этом случае информация попадет непосредственно в руки злоумышленников. Защита работает только в браузерах: Microsoft Edge на базе Chromium, Mozilla Firefox, Mozilla Firefox ESR, Google Chrome и Opera на базе Chromium при установленном и включенном расширении Kaspersky Protection.
- Защита работает только для страниц, удовлетворяющих условиям:
  - Страница находится в списке URL-адресов или категории страниц, для которых необходима защита ввода данных с аппаратной клавиатуры.
  - Страница открыта в защищенном режиме браузера.
  - Страница не находится в списке исключений URL-адресов.
  - Страница содержит поле для ввода пароля, при этом в настройках приложения установлен флажок **Поля ввода паролей на всех сайтах**.
  - Чтобы проверить, установлен ли флажок, перейдите в раздел **Настройки приватности** → **Настройки Защиты ввода данных** → блок **Защита ввода данных с аппаратной клавиатуры**.
- Защита работает только для полей, удовлетворяющих условиям:
  - Поле ввода однострочное, соответствует HTML-тегу <input>.
  - Поле ввода не скрытое: значение атрибута type не равно hidden, в CSS-стилях у поля display не установлено значение none.
  - Поля ввода не являются полями типа submit, radio, checkbox, button, image.
  - Поле ввода не должно быть только для чтения (readOnly).
  - Поле ввода должно быть доступно для ввода (получать фокус).
  - Если поле имеет атрибут максимальной длины (maxlength), минимальное количество вводимых символов должно быть больше трех.
- Защита не работает в следующих случаях:
  - Ввод осуществляется с применением технологии IME.
  - Поле ввода не является полем ввода пароля.

После установки Kaspersky Small Office Security и до первой перезагрузки компьютера приложение не перехватывает первый введенный пользователем символ (в любом приложении).

Как изменить настройки защиты ввода данных с аппаратной клавиатуры

Чтобы настроить защиту ввода данных с аппаратной клавиатуры:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. Перейдите в раздел **Настройки приватности**.
4. Нажмите на кнопку **Защита ввода данных**.

   Откроется окно **Настройки Защиты ввода данных**.
5. В нижней части окна в блоке **Защита ввода данных с аппаратной клавиатуры** установите флажок **Защищать ввод данных с аппаратной клавиатуры**.
6. Установите флажки для категорий сайтов, на которых нужно защищать ввод данных с аппаратной клавиатуры.
7. Если вы хотите включить или выключить защиту ввода данных с клавиатуры на определенном сайте, выполните следующие действия:

   a. Откройте окно **Исключения для Экранной клавиатуры** по ссылке **Настройка исключений**.

   b. В открывшемся окне нажмите на кнопку **Добавить**.

   c. Откроется окно для добавления исключения для аппаратной клавиатуры.

   d. В открывшемся окне введите адрес сайта в поле **Маска веб-адреса**.

   e. Выберите один из вариантов защиты ввода данных на этом сайте: **Применить к указанной странице** или **Применить ко всему сайту**.

   f. Выберите действие защиты ввода данных на этом сайте: **Защищать** или **Не защищать**.

   g. Нажмите на кнопку **ОК**.

Указанный сайт появится в списке в окне **Исключения для Экранной клавиатуры**. При открытии указанного сайта будет действовать защита ввода данных в соответствии с настройками.

Проверка безопасности сайта

Kaspersky Small Office Security позволяет проверить безопасность сайта, прежде чем вы перейдете по ссылке на этот сайт. Для проверки сайтов используется компонент *Проверка ссылок* (недоступен на файловом сервере).

Компонент Проверка ссылок проверяет ссылки на веб-странице открытой в любом из поддерживаемых браузеров. Рядом с проверенной ссылкой приложение Kaspersky Small Office Security отображает один из следующих значков:

– если веб-страница, которая открывается по ссылке, безопасна по данным "Лаборатории Касперского";

– если нет информации о безопасности веб-страницы, которая открывается по ссылке;

– если веб-страница, которая открывается по ссылке, по данным "Лаборатории Касперского" может быть использована злоумышленниками для нанесения вреда компьютеру или вашим данным;

– если веб-страница, которая открывается по ссылке, по данным "Лаборатории Касперского" может быть заражена или взломана;

– если веб-страница, которая открывается по ссылке, опасна по данным "Лаборатории Касперского".
При наведении курсора мыши на значок отображается всплывающее окно с более подробным описанием ссылки.

По умолчанию Kaspersky Small Office Security проверяет ссылки только в результатах поиска. Вы можете включить проверку ссылок на любом сайте.

Чтобы настроить проверку ссылок на сайтах:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. В разделе **Базовая защита** выберите подраздел **Интернет-защита**.

   В окне отобразятся настройки Интернет-защиты.
4. По ссылке **Расширенная настройка** раскройте блок дополнительных настроек Интернет-защиты.
5. В блоке **Проверка ссылок** установите флажок **Проверять ссылки**.
6. Чтобы Kaspersky Small Office Security проверял содержимое всех сайтов, выберите вариант **На всех сайтах, кроме указанных**.
7. Если необходимо, укажите веб-страницы, которым вы доверяете, в окне **Исключения**. Окно открывается по ссылке **Настроить исключения**, Kaspersky Small Office Security не будет проверять содержимое указанных веб-страниц.

8. Чтобы Kaspersky Small Office Security проверял содержимое только определенных веб-страниц, выполните следующие действия:

   a. Выберите вариант **Только на указанных сайтах**.

   b. По ссылке **Настроить проверяемые сайты** перейдите в окно **Проверяемые сайты**.

   c. Нажмите на кнопку **Добавить**.

   d. Введите адрес веб-страницы, содержимое которой необходимо проверять.

   e. Выберите статус проверки веб-страницы (*Активно* – Kaspersky Small Office Security проверяет содержимое веб-страницы).

   f. Нажмите на кнопку **ОК**.

   Указанная веб-страница появится в списке в окне **Проверяемые сайты**. Kaspersky Small Office Security будет проверять ссылки на этой веб-странице.

9. Если вы хотите указать дополнительные настройки проверки ссылок, в окне **Дополнительные настройки Интернет-защиты** в блоке **Проверка ссылок** по ссылке **Настроить проверку ссылок** откройте окно **Проверка ссылок**.

10. Чтобы Kaspersky Small Office Security предупреждал о безопасности ссылок на всех веб-страницах, в блоке **Проверяемые ссылки** выберите вариант **Любые ссылки**.

11. Чтобы Kaspersky Small Office Security отображал информацию о принадлежности ссылки к определенной категории содержимого сайтов (например, *Нецензурная лексика*), выполните следующие действия:

    a. Установите флажок **Отображать информацию о категориях содержимого сайтов**.

    b. Установите флажки напротив категорий содержимого сайтов, информацию о которых необходимо отображать в комментарии.

Kaspersky Small Office Security будет проверять ссылки на указанных веб-страницах и отображать информации о категориях ссылок в соответствии с настройками.

Как изменить настройки защищенных соединений

Защищенные соединения – это соединения, которые устанавливаются по протоколам SSL и TLS. По умолчанию приложение Kaspersky Small Office Security выполняет проверку таких соединений по запросу компонентов защиты, таких как Почтовый Антивирус, Безопасные платежи, Проверка ссылок, Защита от сбора данных в интернете, Интернет-защита и Анти-Баннер.

Чтобы изменить настройки защищенных соединений:

1. Откройте главное окно приложения.

2. Нажмите на кнопку ⚙ в нижней части главного окна.

   Откроется окно **Настройка**.

3. Перейдите в раздел **Настройки безопасности**.

4. В блоке **Расширенные настройки** нажмите на кнопку **Настройки сети**.

5. В окне **Настройки сети** перейдите в раздел **Проверка защищенных соединений**.

6. Выберите вариант действия при подключении к сайтам по защищенному соединению:

   - **Не проверять защищенные соединения**. Kaspersky Small Office Security не проверяет защищенные соединения.

   - **Проверять защищенные соединения по запросу компонентов защиты**. Kaspersky Small Office Security проверяет защищенные соединения, только если на это будет запрос от компонента Проверка ссылок. Этот вариант действия выбран по умолчанию.

   - **Всегда проверять защищенные соединения**. Kaspersky Small Office Security всегда проверяет защищенные соединения.

   По ссылке **Показать сертификаты** открывается окно со списком доверенных сертификатов, которые используются популярными сайтами. Сертификаты добавляются в этот список, если при посещении какого-либо сайта вы нажимаете на кнопку **Добавить в доверенные и продолжить** в уведомлении приложения Kaspersky Small Office Security. После добавления сертификата в список, сайт будет считаться доверенным. Вы можете добавить или удалить сертификаты в окне **Доверенные корневые сертификаты** с помощью кнопок **Добавить** или **Удалить**.

   Если у вас на компьютере несколько учетных записей, и один из пользователей принял новый сертификат, для других пользователей он также будет добавлен в список доверенных сертификатов.

7. Выберите вариант действия, если возникают ошибки при проверке защищенных соединений:

   - **Игнорировать**. Если выбран этот вариант, Kaspersky Small Office Security разрывает соединение с сайтом, на котором возникла ошибка проверки защищенного соединения.

   - **Спрашивать**. Если выбран этот вариант, при возникновении ошибки проверки защищенного соединения с сайтом, Kaspersky Small Office Security показывает уведомление, в котором вы можете выбрать вариант действия:

     - **Игнорировать**. Если выбран этот вариант, Kaspersky Small Office Security разрывает соединение с сайтом, на котором возникла ошибка проверки.

     - **Разрешать и добавлять домен в исключения**. Если выбран этот вариант, Kaspersky Small Office Security добавляет адрес сайта в список доверенных адресов. Kaspersky Small Office Security не проверяет защищенные соединения на сайтах, которые входят в список доверенных адресов. Такие сайты можно посмотреть по ссылке **Настроить доверенные адреса**.

     Этот вариант выбран по умолчанию.

   - **Разрешать и добавлять домен в исключения**. Если выбран этот вариант, Kaspersky Small Office Security добавляет сайт в список доверенных адресов. Kaspersky Small Office Security не проверяет защищенные соединения на сайтах, которые входят в список доверенных адресов. Такие сайты отображаются в окне **Доверенные адреса**, которое можно открыть по ссылке **Настроить доверенные адреса**.

8. По ссылке **Настроить доверенные адреса** откройте окно **Доверенные адреса** и выполните следующие действия:

   a. Нажмите на кнопку **Добавить**, чтобы добавить сайт в список исключений из проверки защищенных соединений.

   b. Укажите доменное имя сайта в поле **Доменное имя**.

   c. Нажмите на кнопку **Добавить**.

      Kaspersky Small Office Security не будет проверять защищенное соединение с этим сайтом. Обратите внимание, что добавление сайта в список доверенных адресов означает, что функциональность проверки этого сайта такими компонентами, как Безопасные платежи, Проверка ссылок, Защита от сбора данных в интернете, Интернет-защита и Анти-Баннер, может быть ограничена.

Настройка уведомлений об уязвимостях сети Wi-Fi

Во время работы в сети Wi-Fi ваши конфиденциальные данные могут быть похищены, если сеть Wi-Fi недостаточно защищена. Kaspersky Small Office Security проверяет сеть Wi-Fi при каждом вашем подключении к сети Wi-Fi. Если сеть Wi-Fi небезопасна (например, используется уязвимый протокол шифрования или имя сети Wi-Fi (SSID) является популярным), Kaspersky Small Office Security показывает уведомление о том, что вы подключаетесь к небезопасной сети Wi-Fi. По ссылке в окне уведомления вы можете узнать, как обезопасить себя при работе в сети Wi-Fi.

Чтобы настроить уведомления об уязвимостях сети Wi-Fi:

1. Откройте главное окно приложения.

2. Нажмите на кнопку ⚙ в нижней части главного окна.

   Откроется окно **Настройка**.

3. Выберите раздел **Настройки безопасности**.

4. Выберите компонент **Сетевой экран**.

   В окне отобразятся настройки компонента Сетевой экран.

5. Установите флажок **Уведомлять об уязвимостях при подключении к сети Wi-Fi**, если вы хотите получать уведомления при подключении к уязвимым сетям Wi-Fi. Если вы не хотите получать уведомления, снимите этот флажок. Флажок доступен для изменения, если на компьютере не установлено приложение Kaspersky Secure Connection.

6. По ссылке **Выбрать категории** укажите типы уязвимостей сетей Wi-Fi. При подключении к сети Wi-Fi с указанной уязвимостью приложение Kaspersky Small Office Security предупредит вас об этом.

7. Если флажок **Уведомлять об уязвимостях при подключении к сети Wi-Fi** установлен, вы можете настроить дополнительные настройки отображения уведомлений:

   - Установите флажок **Запрещать передачу пароля в интернете в незащищенном виде и показывать уведомление**, чтобы блокировать передачу пароля в незащищенном текстовом виде при заполнении поля **Пароль** в интернете.

   - По ссылке **Включить** восстановите значения настроек отображения уведомлений о передаче пароля в незащищенном виде. Если ранее вы заблокировали отображение уведомлений о передаче пароля в незащищенном виде, эти уведомления снова будут отображаться.

При подключении к защищенным сетям Wi-Fi, приложение показывает уведомление, в котором спрашивает вас, доверять или нет новой сети. Можно выбрать один из следующих вариантов:

- **Нет, запретить доступ к компьютеру извне**. Будут блокироваться все внешние соединения этой сети, кроме соединений, инициированных с вашего устройства. Вы сможете пользоваться интернетом и заходить на любые сайты. Другие пользователи данной сети не смогут подключаться к ресурсам вашего компьютера (например не получат доступ к содержимому дисков, включая общие папки).

- **Ограничить, разрешив общий доступ**. Вы сможете пользоваться интернетом и заходить на любые сайты. Другим пользователям этой сети будет заблокирован доступ к ресурсам вашего компьютера, кроме ресурсов, отмеченных как общие (например, общие папки).

- **Да, разрешить любую сетевую активность**. Любые соединения этой сети будут разрешены. Вы сможете пользоваться интернетом и заходить на любые сайты. Другие пользователи сети смогут подключаться к вашему компьютеру без ограничений (например, получать доступ к содержимому дисков).

Эта функциональность недоступна, если приложение Kaspersky Small Office Security установлено на файловом сервере.

Как удалить несовместимые приложения

Приложение Kaspersky Small Office Security регулярно проверяет ваш компьютер на наличие несовместимых приложений. Такие приложения добавляются в список несовместимых приложений. Вы можете просмотреть этот список и принять решение, как поступить с несовместимыми приложениями.

Рекомендуется удалять с компьютера несовместимые приложения, иначе приложение Kaspersky Small Office Security не сможет защитить ваш компьютер в полной мере.

Причины несовместимости стороннего приложения с приложением Kaspersky Small Office Security могут быть следующие:

- Приложение конфликтует с Файловым Антивирусом.
- Приложение конфликтует с Сетевым экраном.
- Приложение препятствует защите сетевого трафика.
- Приложение конфликтует с Секретной папкой.
- Приложение конфликтует с Kaspersky Password Manager.

Как удалить несовместимые приложения

Чтобы удалить несовместимые приложения:

1. Откройте главное окно приложения.
2. Нажмите на кнопку **Подробнее** в верхней части окна.

   Откроется окно **Центр уведомлений**.
3. В разделе **Советы** в строке с сообщением о найденных несовместимых приложениях нажмите на кнопку **Показать**.

   Откроется окно **Обнаружено несовместимое программное обеспечение** со списком найденных несовместимых приложений.
4. Оставьте флажки напротив названий несовместимых приложений, которые нужно удалить, и нажмите **Удалить**. Удаление выполняется с помощью средств удаления, предоставляемых этими приложениями. В процессе удаления от вас может потребоваться согласие на удаление или изменение настроек, связанных с удалением приложений.
5. Если на компьютере остались несовместимые приложения, которые невозможно удалить автоматически, откроется окно со списком таких приложений. Чтобы удалить несовместимые приложения вручную, нажмите **Удалить вручную**. Откроется стандартное окно операционной системы со списком установленных приложений. Удалите несовместимые приложения в соответствии с инструкциями для вашей операционной системы.
6. После удаления несовместимых приложений перезагрузите компьютер.

Работа с приложением из командной строки

Вы можете работать с приложением Kaspersky Small Office Security с помощью командной строки.

Синтаксис командной строки:

```
avp.com <команда> [параметры]
```

Для просмотра справочной информации о синтаксисе командной строки предусмотрена команда:

```
avp.com [ /? | HELP ]
```

Эта команда позволяет получить полный список команд, доступных для работы с приложением Kaspersky Small Office Security через командную строку.

Для получения справочной информации о синтаксисе конкретной команды вы можете воспользоваться одной из следующих команд:

```
avp.com <команда> /?
avp.com HELP <команда>
```

Обращаться к приложению через командную строку следует из папки установки приложения либо с указанием полного пути к avp.com.

Вы можете включать и выключать запись событий приложения (создание файлов трассировки) через командную строку, если ранее вы установили пароль на защиту доступа к управлению приложением Kaspersky Small Office Security в окне настройки приложения.

Если вы не установили пароль в окне настройки приложения, вы не сможете создать пароль и включить запись событий из командной строки.

Некоторые команды можно выполнить только под учетной записью администратора.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или в других источниках информации о приложении, рекомендуется обратиться в Службу технической поддержки. Посетите сайт Службы технической поддержки, чтобы связаться с нашими экспертами, которые ответят на ваши вопросы об установке и использовании приложения.

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

Сбор информации для Службы технической поддержки

После того как вы проинформируете специалистов Службы технической поддержки о возникшей проблеме, они могут попросить вас сформировать отчет с информацией об операционной системе и отправить его в Службу технической поддержки. Также специалисты Службы технической поддержки могут попросить вас создать файл трассировки. Файл трассировки позволяет отследить процесс пошагового выполнения команд приложения и обнаружить, на каком этапе работы приложения возникает ошибка.

Для более эффективного оказания поддержки в случае возникновения вопросов по работе приложения специалисты Службы технической поддержки могут попросить вас в отладочных целях на время проведения работ по диагностике изменить настройки приложения. Для этого может потребоваться выполнение следующих действий:

- Собрать расширенную диагностическую информацию.
- Выполнить более тонкую настройку работы отдельных компонентов приложения, недоступную через стандартные средства пользовательского интерфейса.
- Изменить настройки хранения и отправки собираемой диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

Вся необходимая для выполнения перечисленных действий информация (описание последовательности шагов, изменяемые настройки, 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. Собранная расширенная диагностическая информация сохраняется на компьютере пользователя. Приложение Kaspersky Small Office Security использует сжатие NTFS для уменьшения размера файлов трассировки. 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 настроек работы приложения способами, не описанными в справке 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.

О составе и хранении служебных файлов данных

Файлы трассировки и дампов хранятся на вашем компьютере в открытом виде в течение семи дней с момента выключения записи данных. По истечении семи дней файлы трассировки и дампов безвозвратно удаляются.

Файлы трассировки хранятся в папке ProgramData\Kaspersky Lab.

Файлы трассировки имеют следующие названия: `KAV<номер версии_датаXX.XX_времяXX.XX_pidXXX.><тип файла трассировки>.log`.

Файлы трассировки могут содержать конфиденциальные данные. Ознакомиться с содержимым файла трассировки вы можете, открыв его в текстовом редакторе (например, "Блокнот").

Файлы трассировок производительности можно просмотреть с помощью утилиты Windows Performance Analyzer. Утилиту вы можете скачать с сайта Microsoft.

Как включить или отключить трассировку

Включайте и настраивайте трассировки только под руководством специалиста Службы технической поддержки "Лаборатории Касперского".

Чтобы включить или отключить трассировку приложения и трассировку производительности:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части окна.

   Откроется окно **Поддержка**.
3. По ссылке **Мониторинг проблем** перейдите в окно **Мониторинг проблем**.

4. Используйте переключатель, чтобы включить или отключить трассировку приложения и трассировку производительности в соответствии с инструкциями специалиста Службы технической поддержки.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Автоматическая пересылка собранных данных в "Лабораторию Касперского" не выполняется. Вам необходимо нажать на кнопку **Создать отчет**, чтобы настроить и отправить отчет в Службу технической поддержки.

Если необходимо удалить все системные данные, отчеты и события трассировок, то нажмите **Удалить все служебные данные и отчеты**.

Как сделать запись экрана, если у вас возникла проблема с приложением

Если вы используете Microsoft Windows 7, убедитесь, что установлены все последние обновления для корректной работы этой функции.

Вы можете сделать запись экрана и трассировки, если у вас возникла какая-либо проблема с приложением и отправить файл с записью и трассировкой в Службу технической поддержки для анализа.

При включенной записи экрана не отображаются всплывающие уведомления.

Чтобы сделать запись экрана и трассировки:

1. Откройте главное окно приложения.

2. Нажмите на кнопку в нижней части окна.

   Откроется окно **Поддержка**.

3. По ссылке **Запись проблемы** перейдите в окно **Запись проблемы**.

   Чтобы открыть окно **Запись проблемы**, вам потребуется учетная запись системного администратора.

4. Выберите категорию ошибки:

   - **Ошибка во время работы приложения**. Выберите этот вариант, если приложение неожиданно прекращает работу, не отвечает, или сообщает о сбое.
   - **Ошибка при загрузке данных из интернета**. Выберите этот вариант, если приложение блокирует доступ к сайту или сайт отображается неправильно.
   - **Ошибка активации**. Выберите этот вариант, если в приложении не получается активировать лицензию.
   - **Другое**. Выберите этот вариант, если нет категории с вашей проблемой.

5. Установите флажок **Записывать видео с экрана**. Если флажок **Записывать видео с экрана** не установлен, то при нажатии на кнопку **Начать запись** будет создан только файл трассировки (служебный файл о работе приложения).

   Вариант **Использовать DirectX для записи видео с экрана** выбран по умолчанию. Если в записанном видео не отображаются некоторые окна (например, окно приложения) или если у вас возникли какие-либо другие проблемы с видео, попробуйте отключить эту опцию.

6. Установите флажок **Запустить утилиту Kaspersky Get System Information после записи проблемы** и/или флажок **Записывать трассировку детального уровня (необязательно)**, если вас об этом попросил специалист из Службы технической поддержки.

7. Нажмите на кнопку **Создать отчет**, если у вас уже есть необходимые данные и вы хотите отправить их в Службу технической поддержки. Откроется окно **Создание и отправка отчета**.

8. Если вам нужно сделать запись экрана, нажмите кнопку **Начать запись**.

   Индикатор записи появится вверху экрана.

   Если запись экрана не работает, проверьте, установлен ли в вашей системе Windows Server Essentials Media Pack.

9. Выполните действия, которые демонстрируют возникшую у вас проблему.

10. Нажмите на кнопку **Остановить и создать отчет**. Запись будет остановлена и сохранена в архиве.

    Откроется окно **Создание и отправка отчета**.

11. Чтобы включить запись в отчет, необходимо установить флажок **Включить записанные данные**.

12. Чтобы просмотреть файлы в архиве, нажмите на ссылку рядом с **Включить записанные данные**. В открывшемся окне вы можете добавить или удалить файлы из архива, установив или сняв соответствующие флажки. Архив может содержать запись экрана и файлы трассировки.

13. Чтобы сохранить архив с записанными данными на ваш компьютер, нажмите **Сохранить записанные данные**.

    Для доступа к архиву вам понадобится учетная запись администратора. В Windows 11 вам может потребоваться добавить дополнительные права пользователя для открытия архива.

14. Введите номер запроса, назначенный Службой технической поддержки.

15. Нажмите на кнопку **Отправить отчет**, чтобы отправить отчет в Службу технической поддержки.

Если ваше приложение Kaspersky Small Office Security не запускается, вы можете запустить утилиту **troubleshoot.exe** из папки установки приложения, чтобы записать проблему. Утилита предоставляет те же возможности, что и окно записи проблем в приложении Kaspersky Small Office Security.

Доступ к собранным данным можно получить только с правами администратора. Если у вас нет доступа, обратитесь к системному администратору.

Ограничения и предупреждения

Kaspersky Small Office Security имеет ряд некритичных для работы приложения ограничений.

Региональные ограничения доступности приложений "Лаборатории Касперского"

Приложения Kaspersky Secure Connection и Kaspersky Password Manager могут быть недоступны для скачивания в App Store в Польше и Украине. Подробную информацию смотрите в статьях о доступности Kaspersky Secure Connection и Kaspersky Password Manager в различных регионах.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в ПО на территории США.

Ограничения работы некоторых компонентов и обработки файлов в автоматическом режиме

Обработка зараженных файлов и вредоносных ссылок выполняется в автоматическом режиме по правилам, сформированным специалистами "Лаборатории Касперского". Вы не можете вручную изменять эти правила. Правила могут обновиться в результате обновления баз и модулей приложения. Также в автоматическом режиме обновляются правила Сетевого экрана, Защиты веб-камеры, Менеджера приложений, Предотвращения вторжений.

Если проверка устройства запускается из Центра управления Kaspersky Small Office Security, файлы будут обработаны в автоматическом режиме по правилам, заданным в приложении. Обнаруженные на устройстве файлы могут быть обработаны в автоматическом режиме по запросу из Центра управления Kaspersky Small Office Security без вашего подтверждения.

Особенности обработки файлов в интерактивном режиме защиты

Если зараженный файл является частью приложения из Магазина Windows, в интерактивном режиме защиты приложение показывает уведомление с предложением удалить такой файл. Действие Лечить недоступно.

Ограничения подключения к Kaspersky Security Network

Во время работы приложение может обращаться за информацией в Kaspersky Security Network. Если данные из Kaspersky Security Network получить не удалось, приложение принимает решения на основании локальных антивирусных баз.

Ограничения функциональности Мониторинга активности

Функциональность противодействия приложениям-шифровальщикам (шифрование файлов пользователя вредоносным приложением) имеет следующие ограничения:

- Для обеспечения функциональности используется системная папка Temp. Если на системном диске, на котором расположена папка Temp, недостаточно свободного места для создания временных файлов, защита от приложений-шифровальщиков не предоставляется. При этом уведомление о невыполнении копирования (непредоставлении защиты) не выводится.
- Временные файлы удаляются автоматически при завершении работы Kaspersky Small Office Security или отключении компонента Мониторинг активности.
- В случае нештатного завершения работы Kaspersky Small Office Security временные файлы автоматически не удаляются. Чтобы удалить временные файлы, необходимо вручную очистить папку Temp. Для этого откройте окно **Выполнить** и в поле **Открыть** введите `%TEMP%`. Нажмите на кнопку **OK**.
- Защита от приложений-шифровальщиков выполняется только для файлов, расположенных на носителях информации, отформатированных в файловой системе NTFS.
- Количество подлежащих восстановлению файлов не должно превышать 50 на один процесс шифрования.
- Суммарный объем изменений в файлах не должен превышать 100 МБ. Файлы, изменения в которых превышают этот лимит, не подлежат восстановлению.
- Не контролируются изменения файлов, инициированные через сетевой интерфейс.
- Не поддерживаются файлы, зашифрованные системой EFS.
- Для включения защиты от приложений-шифровальщиков после установки Kaspersky Small Office Security требуется перезагрузить компьютер.

Ограничения функциональности проверки защищенных соединений

В связи с техническими ограничениями реализации алгоритмов проверки проверка защищенных соединений не поддерживает некоторые расширения протокола TLS 1.0 и выше (в частности NPN и ALPN). Подключение по этим протоколам может быть ограничено. Браузеры с поддержкой протокола SPDY используют вместо SPDY протокол HTTP поверх TLS, даже если сервер, к которому выполняется подключение, поддерживает SPDY. При этом уровень защиты соединения не снижается. Если сервер поддерживает только протокол SPDY и возможность установить соединение с помощью протокола HTTPS отсутствует, приложение не будет контролировать установленное соединение.

Также приложение не обрабатывает трафик, передаваемый через расширения протокола HTTP/2.

Приложение Kaspersky Small Office Security препятствует обмену данными по протоколу QUIC. Браузеры используют стандартный транспортный протокол (TLS или SSL) независимо от того, включена в браузере поддержка протокола QUIC или нет.

Приложение Kaspersky Small Office Security контролирует только те защищенные соединения, которые оно может расшифровать. Приложение не контролирует соединения, добавленные в список исключений (ссылка **Сайты** в окне **Настройки сети**).

Проверка и расшифровка зашифрованного трафика по умолчанию выполняется следующими компонентами:

- Интернет-защита;
- Безопасные платежи;
- Проверка ссылок;
- Веб-Контроль.

Kaspersky Small Office Security расшифровывает зашифрованный трафик при работе пользователя в браузере Google Chrome, если в этом браузере отсутствует или выключено расширение Kaspersky Protection.

Kaspersky Small Office Security не контролирует трафик, если браузер загружает веб-страницу или ее элементы из локального кеша, а не из интернета.

Ограничения проверки защищенных соединений клиента the Bat

Так как почтовый клиент The Bat использует собственное хранилище сертификатов, Kaspersky Small Office Security определяет сертификат, использующийся для установления HTTPS-соединения этого клиента с сервером, как недоверенный. Чтобы этого не происходило, настройте почтовый клиент The Bat на работу с локальным хранилищем сертификатов Windows (Windows Certificate Store).

Ограничения исключений из проверки защищенных соединений

При проверке защищенных соединений с сайтами, добавленными в исключения, некоторые компоненты, в частности Анти-Баннер, Проверка ссылок и Защита от сбора данных в интернете, могут продолжать проверять защищенные соединения. Компоненты Безопасные платежи, Веб-Контроль и Интернет-защита не проверяют сайты, добавленные в исключения.

Ограничения Резервного копирования

Резервное копирование имеет следующие ограничения:

- Онлайн-хранилище резервных копий становится недоступным при смене жесткого диска или при переходе на новый компьютер. Информацию о том, как восстановить подключение к Онлайн-хранилищу при смене оборудования, смотрите на сайте Службы технической поддержки.
- Изменение служебных файлов хранилища резервных копий может привести к тому, что вы потеряете доступ к хранилищу резервных копий и не сможете восстановить свои данные.
- Так как приложение выполняет резервное копирование через системную службу теневого копирования, автономный файл данных Outlook (OST) не попадает в резервную копию, так как он не предназначен для резервного копирования.

Ограничение функциональности Секретная папка

При создании секретной папки в файловой системе FAT32 размер файла секретной папки на диске не должен превышать 4 ГБ.

Особенности проверки памяти ядра на наличие руткитов во время работы в защищенном режиме браузера

В случае обнаружения недоверенного модуля во время работы защищенного режима браузера открывается новая вкладка браузера с уведомлением о том, что была обнаружена вредоносное приложение. В этом случае рекомендуется закрыть браузер и выполнить полную проверку компьютера.

Особенности защиты данных буфера обмена

Kaspersky Small Office Security разрешает приложению обращаться к буферу обмена в следующих случаях:

- Приложение с активным окном пытается поместить данные в буфер обмена. Активным считается окно, с которым вы работаете в настоящий момент.
- Защищенный процесс приложения пытается поместить данные в буфер обмена.
- Защищенный процесс приложения или процесс с активным окном пытается получить данные из буфера обмена.
- Данные из буфера обмена пытается получить процесс приложения, который ранее сам поместил эти данные в буфер обмена.

Особенности обработки зараженных файлов компонентами приложения

Приложение по умолчанию может удалять зараженные файлы, если их лечение невозможно. Удаление по умолчанию может выполняться при обработке файлов такими компонентами, как Предотвращение вторжений, Почтовый Антивирус, Файловый Антивирус, при выполнении задач проверки, а также при обнаружении опасной активности приложений компонентом Мониторинг активности.

Ограничения работы некоторых компонентов при совместной установке приложения с Kaspersky Fraud Prevention for Endpoints

Работа следующих компонентов Kaspersky Small Office Security ограничивается в защищенном режиме браузера, если приложение установлено совместно с Kaspersky Fraud Prevention for Endpoints:

- Интернет-защита, кроме Анти-Фишинга;
- Веб-Контроль;
- Проверка ссылок;
- Анти-Баннер.

Особенности работы процесса autorun

Процесс autorun выполняет запись результатов своей работы. Данные сохраняются в текстовые файлы с названием вида "kl-autorun-<date><time>.log". Чтобы просмотреть данные, требуется открыть окно **Выполнить**, в поле **Открыть** ввести %TEMP% и нажать на кнопку **OK**.

В файлы трассировки сохраняются пути к файлам установки, загруженным в ходе использования autorun. Данные хранятся в течение работы процесса autorun и безвозвратно удаляются при завершении этого процесса. Данные никуда не отправляются.

Ограничения работы Kaspersky Small Office Security при включенном режиме Device Guard на Microsoft Windows 10 RS4

Частично ограничена работа следующей функциональности:

- защита буфера обмена;
- защита браузера от приложений эмуляции ввода с клавиатуры и мыши (подмен вводимых данных);
- защита от приложений удаленного управления;
- защита браузера (управление через API, защита от атак при помощи опасных сообщений окнам браузера, защита от управления очередью сообщений);
- эвристический анализ (эмуляция запуска вредоносных приложений).

Если в операционной системе Windows включен режим работы UMCI, Kaspersky Small Office Security не обнаруживает приложения блокировки экрана.

О записи событий, касающихся Лицензионного соглашения и Kaspersky Security Network, в журнал событий Windows

События принятия или отказа от условий Лицензионного соглашения, а также принятия или отказа от участия в Kaspersky Security Network записываются в журнал Windows.

Ограничения проверки репутации локальных адресов в Kaspersky Security Network

Ссылки, ведущие на локальные ресурсы, не проверяются в Kaspersky Security Network.

Предупреждение о приложениях сбора информации

Если у вас на компьютере установлено приложение, выполняющее сбор и отправку информации на обработку, приложение Kaspersky Small Office Security может классифицировать такое приложение как вредоносное. Чтобы избежать этого, вы можете исключить приложение из проверки, настроив приложение Kaspersky Small Office Security способом, описанным в этом документе.

Предупреждение о создании отчета об установке приложения

При установке приложения на компьютер создается файл отчета об установке. Если установка приложения завершилась с ошибкой, файл отчета об установке сохраняется, и вы можете отправить его в Службу поддержки "Лаборатории Касперского". Вы можете ознакомиться с содержимым файла отчета об установке по ссылке из окна приложения. В случае успешной установки приложения, файл отчета об установке сразу же удаляется с вашего компьютера.

Ограничения контроля веб-камеры на операционной системе Microsoft Windows 10 Anniversary Update (RedStone 1)

После установки приложения на операционной системе Microsoft Windows 10 Anniversary Update (RedStone 1) контроль доступа к веб-камере не гарантируется до перезагрузки компьютера.

Ограничение резервного копирования и восстановления данных из резервных копий

Невозможно одновременное выполнение задачи резервного копирования в Kaspersky Small Office Security и задачи восстановления данных в утилите Kaspersky Restore Utility на одном компьютере.

Ограничения работы Сетевого экрана

Сетевой экран не контролирует локальные подключения, которые устанавливают контролируемые приложения.

Ограничения работы компонента Предотвращение вторжений

Если на вашем компьютере установлено приложение VeraCrypt, Kaspersky Small Office Security может завершить работу при работе с компонентом Предотвращение вторжений. Для решения этой проблемы требуется обновить приложение VeraCrypt до версии 1.19 или выше.

Ограничение первого запуска приложения после обновления операционной системы Microsoft Windows 7 до Microsoft Windows 10

Если вы обновили операционную систему Microsoft Windows 7 до Microsoft Windows 8 / 8.1 или Microsoft Windows 10 / RS1 / RS2 / RS3, при первом запуске Kaspersky Small Office Security работает со следующими ограничениями:

- Работает только Файловый Антивирус (постоянная защита). Остальные компоненты приложения не работают.
- Работает самозащита файлов и системного реестра. Самозащита процессов не работает.
- Интерфейс приложения недоступен до перезагрузки компьютера. Приложение показывает уведомление о том, что некоторые компоненты приложения не работают, и о том, что требуется перезагрузка компьютера после завершения адаптации к новой операционной системе.
- В контекстном меню значка в области уведомлений доступен только пункт **Выход**.
- Приложение не показывает уведомления и автоматически выбирает рекомендованное действие.

Предупреждение об ошибке адаптации драйверов приложения при обновлении операционной системы с Windows 7 до Windows 10

При обновлении Windows с версии 7 до версии 10 может произойти ошибка адаптации драйверов Kaspersky Small Office Security. Адаптация драйверов происходит в фоновом режиме, вы не получаете оповещений о ее процессе.

В случае возникновения ошибки адаптации драйверов вы не сможете воспользоваться следующими функциями приложения:

- сетевым экраном;
- функцией обнаружения угроз во время загрузки операционной системы;
- функцией защиты процессов приложения с помощью технологии Protected Process Light (PPL) от Microsoft.

Вы можете воспользоваться следующими способами исправления ошибки:

- перезагрузить компьютер и повторить адаптацию приложения из оповещения в Центре уведомлений;
- удалить и заново установить приложение.

Ограничения проверки трафика, передаваемого по протоколу HTTPS, в браузере Mozilla Firefox

В версиях Mozilla Firefox 58.x и выше приложение не проверяет трафик, передаваемый по протоколу HTTPS, если изменение настроек браузера защищено Основным паролем. При обнаружении Основного пароля в браузере, приложение показывает уведомление, в котором содержится ссылка на статью в Базе знаний. Статья содержит инструкцию для решения этой проблемы.

Если трафик, передаваемый по протоколу HTTPS, не контролируется, ограничена работа следующих компонентов:

- Интернет-защита;
- Анти-Фишинг;
- Веб-Контроль;
- Защита приватности;
- Анти-Баннер;
- Защита ввода данных;
- Безопасные платежи.

Ограничения работы расширения Kaspersky Protection в браузерах Google Chrome и Mozilla Firefox

Расширение Kaspersky Protection не работает в браузерах Google Chrome и Mozilla Firefox, если на вашем компьютере установлено приложение Malwarebytes for Windows.

Особенности установки приложения на операционной системе Microsoft Windows 7 Service Pack 0 и Service Pack 1

При установке приложения на операционные системы, которые не поддерживают сертификаты с цифровой подписью SHA256, приложение устанавливает свой доверенный сертификат.

Об автоматическом тестировании функциональности приложений "Лаборатории Касперского"

В приложениях "Лаборатории Касперского", включая Kaspersky Small Office Security, предусмотрен специальный API (application programming interface – интерфейс прикладного программирования) для автоматического тестирования функциональности приложения. Этот API предназначен исключительно для использования разработчиками "Лаборатории Касперского".

Ограничения копирования данных в буфер обмена при совместном подключении нескольких пользователей к терминальному серверу

Если один из пользователей, подключенных к терминальному серверу, открыл какой-либо сайт в защищенном режиме браузера, у других пользователей, подключенных к этому терминальному серверу, перестает работать функция копирования данных в буфер обмена.

Ограничения защиты ввода данных с аппаратной клавиатуры при запуске нескольких терминальных сессий

Защита ввода данных с аппаратной клавиатуры не осуществляется, если запущено несколько параллельных терминальных сессий.

Ограничения расширения для Microsoft Outlook

Расширение для Microsoft Outlook не поддерживается в Microsoft Outlook 2023. Это означает, что компонент Почтовый Антивирус не будет работать для этого почтового клиента.

Особенности использования шрифта большого размера в вашей операционной системе

Рекомендуется увеличить окно приложения, если вы используете большой размер шрифта в вашей операционной системе, иначе некоторые элементы интерфейса приложения могут не отображаться.

Снижение производительности приложения при отключении UDP Receive Segment Coalescing Offload (URO)

Операционные системы Windows, начиная с версии 11 24H2, поддерживают технологию UDP Receive Segment Coalescing Offload (URO). Технология включена по умолчанию, если на компьютере установлены совместимая сетевая карта и драйверы. Отключение URO на компьютере пользователя может значительно снизить производительность приложения.

Ограничения проверки веб-почтовых клиентов

Функция **Проверять веб-почтовые клиенты** не поддерживает веб-почтовый клиент Gmail.

Ограничения при установке приложения вместе с КриптоПро CSP

Установка приложения Kaspersky Small Office Security на Windows 11 поддерживается только при использовании КриптоПро CSP версии 5.0 или выше.

Другие источники информации о приложении

Страница приложения Kaspersky Small Office Security в Базе знаний

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

На странице приложения Kaspersky Small Office Security в Базе знаний вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании приложения.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к приложению Kaspersky Small Office Security, но и к другим приложениям "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Поддержка приложений "Лаборатории Касперского" на нашем Форуме

Вы можете получить поддержку от пользователей и экспертов "Лаборатории Касперского" на нашем Форуме.

На Форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения и получения помощи.

Сетевые параметры для взаимодействия с внешними службами

Приложение Kaspersky Small Office Security использует следующие сетевые параметры для взаимодействия с внешними службами.

Сетевые параметры

Адрес	Описание
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Протокол: `HTTPS` Порт: `443`	Активация приложения.

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`s08.upd.kaspersky.com`
`s09.upd.kaspersky.com`
`s10.upd.kaspersky.com`
`s11.upd.kaspersky.com`
`s12.upd.kaspersky.com`
`s13.upd.kaspersky.com`
`s14.upd.kaspersky.com`
`s15.upd.kaspersky.com`
`s16.upd.kaspersky.com`
`s17.upd.kaspersky.com`
`s18.upd.kaspersky.com`
`s19.upd.kaspersky.com`
`cm.k.kaspersky-labs.com`
Протокол: `HTTPS`
Порт: `443`
	Обновление баз и модулей приложения.

Адрес	Описание
`downloads.upd.kaspersky.com` Протокол: `HTTPS` Порт: `443`	• Обновление баз и модулей приложения. • Проверка доступа к серверам "Лаборатории Касперского". При сбоях доступа к серверам через системный DNS приложение будет использовать публичный DNS. Это нужно для обновления антивирусных баз и поддержки уровня безопасности компьютера. Приложение Kaspersky Small Office Security будет использовать следующие публичные DNS в порядке их обхода: 1. Google Public DNS (8.8.8.8). 2. Cloudflare DNS (1.1.1.1). 3. Alibaba Cloud DNS (223.6.6.6). 4. Quad9 DNS (9.9.9.9). 5. CleanBrowsing (185.228.168.168). Запросы приложения могут содержать адреса доменов и внешний IP-адрес пользователя, так как приложение устанавливает с DNS-сервером TCP/UDP-соединение. Эти данные нужны, например, для проверки сертификата веб-ресурса при обращении по HTTPS. Если приложение Kaspersky Small Office Security использует публичный DNS-сервер, правила обработки данных регламентируются Политикой конфиденциальности этого сервиса. Если требуется запретить приложению Kaspersky Small Office Security использовать публичный DNS-сервер, обратитесь в Службу технической поддержки за приватным патчем.
`touch.kaspersky.com` Протокол: `HTTP`	• Получение доверенного времени для проверки срока действия сертификата (TLS-соединение). • Предупреждение о запрете доступа к веб-ресурсу в браузере при работе Интернет-защиты.

Адрес	Описание
p00.upd.kaspersky.com p01.upd.kaspersky.com p02.upd.kaspersky.com p03.upd.kaspersky.com p04.upd.kaspersky.com p05.upd.kaspersky.com p06.upd.kaspersky.com p07.upd.kaspersky.com p08.upd.kaspersky.com p09.upd.kaspersky.com p10.upd.kaspersky.com p11.upd.kaspersky.com p12.upd.kaspersky.com p13.upd.kaspersky.com p14.upd.kaspersky.com p15.upd.kaspersky.com p16.upd.kaspersky.com p17.upd.kaspersky.com p18.upd.kaspersky.com p19.upd.kaspersky.com downloads.kaspersky-labs.com cm.k.kaspersky-labs.com Протокол: `HTTP` Порт: `80`	Обновление баз и модулей приложения.
ds.kaspersky.com Протокол: `HTTPS` Порт: `443`	Использование Kaspersky Security Network.
ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com Протокол: `Любой` Порт: `443`, `1443`	Использование Kaspersky Security Network.
click.kaspersky.com redirect.kaspersky.com Протокол: `HTTPS`	Переход по ссылкам из интерфейса.

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки приложения.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Adobe, Acrobat, Reader являются либо зарегистрированными товарными знаками, либо товарными знаками компании Adobe в США и/или других странах.

Apple, App Store, Mac, macOS, MacBook, MacBook Air, Mac Pro, iMac, iPad, iPod, iPhone, QuickTime, Safari, Sand – товарные знаки Apple Inc.

Arm – зарегистрированный товарный знак Arm Limited (или дочерних компаний) в США и/или других странах.

Cloudflare, логотип Cloudflare и Cloudflare Workers являются товарными знаками и/или зарегистрированными товарными знаками компании Cloudflare, Inc. в США и других юрисдикциях.

Dropbox – товарный знак Dropbox, Inc.

Google, Google+, Google Chrome, Google Public DNS, Chromium, SPDY, YouTube, Android, Gmail – товарные знаки Google LLC.

Intel, Celeron, и Atom товарные знаки Intel Corporation или ее дочерних компаний.

IOS является зарегистрированным товарным знаком или товарным знаком Cisco Systems, Inc. и/или ее аффилированных компаний в США и в определенных других странах.

Java и JavaScript – зарегистрированные товарные знаки компании Oracle и/или аффилированных компаний.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

LogMeIn Pro и Remotely Anywhere – товарные знаки компании LogMeIn, Inc.

Mail.ru – зарегистрированный товарный знак, правообладателем которого является ООО "Мэйл.Ру".

OpenSSL является товарным знаком правообладателя OpenSSL Software Foundation.

ActiveX, Active Directory, Direct3D, DirectX, Microsoft, Microsoft Edge, Windows, Windows Media, Windows XP, Windows Server, Windows Store, Internet Explorer, Outlook, PowerPoint, PowerShell, Bing являются товарными знаками группы компаний Microsoft.

Mozilla, Thunderbird и Firefox являются товарными знаками Mozilla Foundation в США и других странах.

VMware – зарегистрированный товарный знак и/или товарный знак VMware, Inc. в США или других странах.

Как настроить безопасное VPN-соединение для категорий сайтов

Функциональность Безопасное VPN-соединение доступна не во всех регионах.

По умолчанию приложение Kaspersky Secure Connection не устанавливает безопасное VPN-соединение, когда вы открываете сайты в браузере. Вы можете настроить включение безопасного VPN-соединения для разных категорий сайтов, если на вашем компьютере установлено и активировано приложение Kaspersky Plus, Kaspersky Premium или Kaspersky Small Office Security. Например, вы можете указать, что безопасное VPN-соединение должно включаться, когда вы посещаете сайты платежных систем или социальных сетей.

Чтобы настроить безопасное VPN-соединение для категорий сайтов:

1. Откройте главное окно приложения.
2. В главном окне приложения нажмите на кнопку ☰.
3. Выберите пункт **Настройка** → блок **Сайты**.
4. Нажмите на кнопку **Настроить**.

   Откроется окно **Правила подключения к сайтам**.
5. Выберите категорию сайтов:
   - Банковские сайты. К этой категории относятся сайты банков.
   - Платежные системы. К этой категории относятся сайты платежных систем.
   - Интернет-магазины с онлайн-оплатой. К этой категории относятся сайты интернет-магазинов, содержащих встроенные платежные системы.
   - социальные сети. К этой категории относятся сайты социальных сетей.
6. Выберите вариант действия при посещении выбранной категории сайтов:
   - **Включать безопасное VPN-соединение**. Приложение будет включать безопасное VPN-соединение при посещении сайтов выбранной категории.
   - **Спрашивать**. При посещении какого-либо сайта из выбранной категории приложение будет спрашивать вас, нужно ли включать безопасное VPN-соединение для этого сайта. В окне браузера выберите нужное действие и установите флажок **Запомнить выбор для этого сайта**. Приложение будет выполнять выбранное вами действие каждый раз при посещении этого сайта. Если флажок не установлен, приложение запоминает ваш выбор на один час.
   - **Не реагировать**. Приложение не будет включать безопасное VPN-соединение при посещении сайтов выбранной категории.

7. Если выбран вариант **Включать безопасное VPN-соединение**, в раскрывающемся списке **Выбирать** укажите локацию VPN-сервера, через который вы хотите устанавливать безопасное VPN-соединение для этой категории сайтов.

8. Установите флажок **Уведомлять о включении**, если вы хотите получать уведомления о включении безопасного VPN-соединения, когда вы посещаете сайт этой категории.

По умолчанию Kaspersky Secure Connection не предлагает включать безопасное VPN-соединение, если подключение к сайту выполняется по протоколу HTTPS.

Перейти в справку Kaspersky Secure Connection.

О дополнительных возможностях безопасного VPN-соединения

Функциональность Безопасное VPN-соединение доступна не во всех регионах.

Дополнительные возможности безопасного VPN-соединения доступны, если на вашем устройстве установлено приложение Kaspersky Plus, Kaspersky Premium или Kaspersky Small Office Security.

Дополнительные возможности безопасного VPN-соединения включают в себя следующее:

- Настройка включения безопасного VPN-соединения при посещении следующих категорий сайтов:
  - банковские сайты;
  - платежные системы;
  - интернет-магазины и сайты электронной коммерции;
  - социальные сети.
- Настройка автоматической смены локации VPN-сервера. Если вы указали в настройках безопасного VPN-соединения разные локации при подключении к сайтам разных категорий, вы можете указать, надо ли менять локацию VPN-сервера, когда вы перемещаетесь между сайтами разных категорий.
- Настройка безопасного VPN-соединения для отдельных сайтов, например, для сайтов, которые вы часто посещаете.

Перейти в справку Kaspersky Secure Connection.

Как настроить безопасное VPN-соединение для выбранного сайта

Вы можете настроить включение безопасного VPN-соединения для разных категорий сайтов, если на вашем компьютере установлено и активировано приложение Kaspersky Plus, Kaspersky Premium или Kaspersky Small Office Security.

Функциональность Безопасное VPN-соединение доступна не во всех регионах.

Чтобы настроить безопасное VPN-соединение для выбранного сайта:

1. Откройте главное окно приложения.
2. В главном окне приложения нажмите на кнопку ☰.
3. Выберите пункт **Настройка** → блок **Сайты**.
4. Нажмите на кнопку **Настроить**.

   Откроется окно **Правила подключения к сайтам**.
5. В блоке **Исключения для сайтов** нажмите на кнопку **Настроить**.

   Откроется окно **Исключения для сайтов**.
6. Нажмите на кнопку **Добавить**, чтобы добавить сайт в список исключений из настроек, которые заданы для категорий сайтов.

   Откроется окно **Добавление сайта**.
7. В поле **Веб-адрес (URL)** введите адрес сайта.

8. В блоке **Действие при открытии сайта** укажите, какое действие должно выполнить приложение, когда вы заходите на этот сайт:

   - **Включать безопасное VPN-соединение**. Приложение включает безопасное VPN-соединение, когда вы посещаете указанный сайт. Например, вы можете указать, что приложение должно включать безопасное VPN-соединение, когда вы посещаете сайт вашего банка. Настройка действует, даже если в окне **Правила подключения к сайтам** в блоке **При посещении незащищенных банковских сайтов** выбран вариант **Не реагировать**.

     a. В раскрывающемся списке **Выбирать** выберите локацию VPN-сервера, через который вы хотите устанавливать безопасное VPN-соединение, когда посещаете этот сайт. Если для сайта и категории, в которую входит этот сайт, заданы разные локации для включения безопасного VPN-соединения, подключение к сайту происходит через локацию, которая указана для этого сайта, а не всей категории.

     b. Установите флажок **Уведомлять о включении**, если вы хотите получать уведомления о включении безопасного VPN-соединения, когда вы посещаете этот сайт.

   - **Не реагировать**. Приложение не включает безопасное VPN-соединение, когда вы посещаете указанный сайт.

9. Нажмите на кнопку **Добавить**.

Приложение не включает безопасное VPN-соединение, если подключение к сайту выполняется по протоколу HTTPS.

Перейти в справку Kaspersky Secure Connection.

Окно Ввод кода активации

Поля для ввода кода активации

Вы могли получить код активации по электронной почте или в оффлайн-магазине. Код активации состоит из четырех групп символов (например, **ABA9C-CDEFG-ABCBC-ABC2D**).

Получить лицензию из аккаунта

По ссылке открывается окно с формой подключения устройства к аккаунту Центра управления Kaspersky Small Office Security для активации приложения по лицензии, которая хранится в аккаунте.

Где найти код активации?

По ссылке **Где найти код активации?** открывается окно браузера с подробной информацией об активации приложения с помощью кода активации.

Купить лицензию

По ссылке открывается окно браузера на странице интернет-магазина, в котором вы можете приобрести лицензию.

Активировать

По кнопке запускается активация приложения с помощью введенного кода активации.

Код активации соответствует другому приложению

Это окно отображается, если введенный код активации соответствует другому приложению. Вы можете перейти к использованию этого приложения сейчас или после истечения срока действия лицензии на Kaspersky Small Office Security.

Отмена

По ссылке вы можете отменить активацию приложения.

Продолжить

При нажатии на кнопку запускается установка и активация приложения, которому соответствует введенный вами код активации.

Информация о категориях сайтов

По ссылке вы можете ознакомиться с описанием категорий веб-сайтов.

Используйте эти параметры в следующих задачах

Проверка безопасности сайта

Как настроить защиту DNS по HTTPS

Когда вы вводите название сайта в адресной строке браузера, браузер отправляет ваш запрос на DNS-сервер. DNS-сервер определяет IP-адрес запрашиваемого вами сайта. Передача данных с вашего компьютера на DNS-сервер при этом происходит с использованием обычного текстового протокола, не защищенного шифрованием. Злоумышленники могут перехватить информацию о том, на какие сайты вы заходите, и использовать их в своих целях. Чтобы этого не случилось, эту информацию лучше передавать по защищенному протоколу HTTPS. Сервер, который отвечает за прием и анализ таких запросов, называется DNS поверх HTTPS или DoH-сервер.

Приложение Kaspersky Small Office Security автоматически получает данные о том, какой DoH-сервер используется в браузере Mozilla Firefox. Если вы добавили DoH-сервер в приложении Kaspersky Small Office Security вручную и хотите, чтобы данные DNS передавались через этот DoH-сервер, вам нужно добавить этот сервер в настройках браузера Mozilla Firefox. Информацию о настройке DoH-сервера смотрите в справке Mozilla Firefox.

Добавление DoH-сервера

Чтобы добавить DoH-сервер:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.
3. В разделе **Дополнительно** выберите подраздел **Сеть**.

   Откроется окно **Настройки сети**.
4. В блоке **Обработка трафика** по ссылке **Управлять DoH-серверами** перейдите в окно **DoH-серверы**.
5. Нажмите на кнопку **Добавить**.
6. В открывшемся окне введите имя или IP-адрес DoH-сервера и нажмите на кнопку **Добавить**.

DoH-сервер будет добавлен в список.

Окно Найдена информация о действующей лицензии

Да, использовать <приложение>

При выборе этого варианта работа мастера активации завершается. Приложение будет работать по обнаруженной действующей лицензии. Если обнаружена лицензия на Kaspersky Small Office Security, будет запущен мастер миграции.

Нет, продолжить работу мастера и ввести новый код активации

При выборе этого варианта мастер активации продолжает работу и активирует приложение. Вам потребуется ввести новый код активации, соответствующий этому приложению.

Окно Регистрация

В этом окне нужно указать регистрационные данные, которые понадобятся в случае обращения в Службу технической поддержки.

Отсутствует соединение с интернетом

Это окно отображается, если попытка активировать приложение не удалась из-за проблем с подключением к интернету.

Повторить попытку

По ссылке мастер активации пытается активировать приложение повторно. Если проблемы с интернетом краткосрочные, то повторная попытка может оказаться успешной.

Раздел Выбор папки для восстановленных файлов

Исходная папка

При выборе этого варианта приложение помещает восстановленные файлы в папку, в которой находились исходные файлы в момент создания резервной копии.

Указанная папка

При выборе этого варианта приложение помещает восстановленные файлы в папку, указанную в поле ниже.

Выбрать

При нажатии на кнопку открывается окно **Выберите папку**. В этом окне можно выбрать папку, в которую нужно поместить восстановленные файлы.

Кнопка доступна, если выбран вариант **Указанная папка**.

При совпадении имен файлов

В раскрывающемся списке можно выбрать действие, которое должно выполнять приложение, если в папке, куда требуется поместить восстановленный файл, уже находится файл с таким же именем:

- **спрашивать** – приложение при совпадении имен файлов предлагает выбрать один из вариантов: заменить файл резервной копией, сохранить оба файла или не восстанавливать этот файл.
- **заменить файл резервной копией** – Приложение Kaspersky Small Office Security удаляет существующий файл и помещает на его место файл, восстановленный из резервной копии.
- **сохранить оба файла** – Приложение Kaspersky Small Office Security оставляет существующий файл без изменений и сохраняет файл, восстановленный из резервной копии, под новым именем в этой же папке.
- **не восстанавливать этот файл** – Приложение Kaspersky Small Office Security оставляет существующий файл без изменений, не восстанавливая одноименный файл из резервной копии.

Восстановить файлы

При нажатии на кнопку запускается восстановление файлов из резервных копий.

Ошибка активации

Не удалось активировать приложение. По ссылке **Причины и возможные решения** вы можете просмотреть информацию о проблеме в базе знаний.

Причины и возможные решения

По ссылке вы можете перейти к статье базы знаний с информацией о причинах ошибки и возможных решениях.

Для некоторых ошибок ссылка на статью в базе знаний может отсутствовать.

Отмена

По ссылке вы можете отменить активацию приложения.

Переход к использованию другого приложения

После нажатия на кнопку **Продолжить** будет запущен мастер миграции. В результате работы мастера миграции будет установлено приложение, соответствующее введенному коду активации.

Если срок действия лицензии на приложение Kaspersky Small Office Security еще не истек, вы можете использовать приложение Kaspersky Small Office Security на другом компьютере.

По ссылке **Отмена** вы можете отменить переход на другое приложение.

Отмена

По ссылке можно отменить запуск мастера миграции и вернуться к предыдущему шагу.

Окно Последовательность запуска

Последовательность запуска приложений

В списке содержится информация о приложениях, запущенных выбранным приложением (дочерних приложениях). По умолчанию дочерние приложения отсортированы по времени запуска, начиная с самого раннего.

Запуск

В графе отображается время запуска дочернего приложения.

ID процесса

В графе отображается идентификатор процесса дочернего приложения.

Приложение

В графе отображается название дочернего приложения.

Группа доверия

В графе отображается группа доверия, в которую входит приложение:

- **Доверенные**. Приложение работает без ограничений, но контролируется компонентом Файловый Антивирус.
- **Слабые ограничения**. Приложению запрещено обращаться к конфиденциальным данным и настройкам пользователя, изменять публичные данные. При попытке изменения системных данных и выполнения привилегированных операций запрашивается разрешение пользователя. Сетевая активность такого приложения ограничена.
- **Сильные ограничения**. Приложению запрещено обращаться к конфиденциальным данным и настройкам пользователя, публичным и системным данным. При попытке выполнения привилегированных операций запрашивается разрешение пользователя. Сетевая активность такого приложения заблокирована.
- **Недоверенные**. Работа такого приложения полностью блокируется.

Закладка Работающие

Список работающих приложений

В списке отображаются приложения и процессы, выполняемые на вашем компьютере в настоящее время.

По правой клавише мыши можно открыть контекстное меню заголовка любой графы. С помощью контекстного меню можно настроить отображение граф с дополнительной информацией о приложениях и процессах:

- название исполняемого файла приложения или процесса;
- сведения о производителе приложениях;
- идентификатор процесса;
- расположение исполняемого файла приложения;
- имя пользователя, запустившего приложение или процесс;
- время создания и запуска приложения или процесса;
- настройки автозапуска приложения.

С помощью пункта **Упорядочить столбцы по умолчанию** можно восстановить исходный вид таблицы.

По правой клавише мыши на строке приложения или процесса открывается контекстное меню. Из контекстного меню можно выполнить следующие действия:

- открыть окно **Правила приложения**, в котором можно настроить правила для контроля действий приложения;
- отобразить последовательность запуска процессов в окне **Последовательность запуска**;
- переместить приложение в другую группу доверия;
- установить для приложения настройки контроля активности, предусмотренные по умолчанию;
- завершить процесс;
- открыть папку, содержащую исполняемый файл приложения.

Вид

В раскрывающемся списке можно включить отображение системных процессов и процессов Kaspersky Small Office Security:

- **Показывать системные процессы**. При выборе этого элемента в общем списке приложений и процессов отображаются процессы, необходимые для работы операционной системы.
- **Показывать процессы Kaspersky Small Office Security**. При выборе этого элемента в общем списке приложений и процессов отображаются процессы, запущенные Kaspersky Small Office Security.

В раскрывающемся списке можно выбрать способ отображения приложений и процессов:

- **Показывать как список**. При выборе этого варианта приложения / процессы отображаются в виде списка.
- **Показывать как дерево**. При выборе этого варианта приложения / процессы отображаются в виде иерархической структуры в соответствии с последовательностью вызова процессов.

Приложение

В графе отображается название приложения или процесса.

Цифровая подпись

В графе отображается информация о наличии цифровой подписи у приложения и владельце цифровой подписи.

Группа доверия

В графе отображается группа доверия, в которую помещено приложение. В зависимости от группы доверия приложения в графе отображаются следующие значки:

- Красный значок означает, что приложение находится в группе "Недоверенные".
- Розовый значок означает, что приложение находится в группе "Сильные ограничения".
- Желтый значок означает, что приложение находится в группе "Слабые ограничения".
- Зеленый значок означает, что приложение находится в группе "Доверенные".
- Некоторые специализированные системные процессы (например, System или MemCompression) не распределяются по группам доверия и не контролируются приложением Kaspersky Small Office Security. Такие процессы отображаются в виде серого значка с отметкой "Неизвестные".

Популярность

В графе отображается уровень популярности приложения среди участников Kaspersky Security Network (KSN). Уровень популярности соответствует числу участников KSN, использующих приложение.

Процессор

В графе отображается текущее потребление ресурсов центрального процессора приложением / процессом.

Память

В графе отображается текущее потребление оперативной памяти приложением / процессом.

Диск

В графе отображается суммарная скорость чтения и записи данных на диск приложением или процессом.

Сеть

В графе отображается суммарная скорость приема и передачи данных приложением через сетевой интерфейс.

Завершить процесс

При нажатии на кнопку завершается работа приложения, выбранного в списке.

Закладка Запускаемые при старте

Список приложений, запускаемых при старте

Список содержит приложения, которые запускаются при старте операционной системы.

По правой клавише мыши можно открыть контекстное меню заголовка любой графы. С помощью контекстного меню можно настроить отображение граф в таблице. С помощью пункта **Упорядочить столбцы по умолчанию** можно восстановить исходный вид таблицы.

По правой клавише мыши на строке приложения или процесса открывается контекстное меню. Из контекстного меню можно выполнить следующие действия:

- открыть окно **Правила приложения**, в котором можно настроить правила для контроля действий приложения;
- переместить приложение в другую группу доверия;
- установить для приложения настройки контроля активности, предусмотренные по умолчанию;
- открыть папку, содержащую исполняемый файл приложения.

Приложение

В графе отображается название приложения, запускаемого при старте операционной системы.

Статус

В графе отображается состояние приложения: *Выполняется* или *Остановлено*.

Цифровая подпись

В графе отображается информация о наличии цифровой подписи у приложения и владельце цифровой подписи.

Группа доверия

В графе отображается группа доверия, в которую помещено приложение. В зависимости от группы доверия приложения в графе отображаются следующие значки:

- Красный значок означает, что приложение находится в группе "Недоверенные".
- Розовый значок означает, что приложение находится в группе "Сильные ограничения".
- Желтый значок означает, что приложение находится в группе "Слабые ограничения".
- Зеленый значок означает, что приложение находится в группе "Доверенные".
- Некоторые специализированные системные процессы (например, System или MemCompression) не распределяются по группам доверия и не контролируются приложением Kaspersky Small Office Security. Такие процессы отображаются в виде серого значка с отметкой "Неизвестные".

Популярность

В графе отображается уровень популярности приложения среди участников Kaspersky Security Network (KSN). Уровень популярности соответствует числу участников KSN, использующих приложение.

Последний запуск

В графе отображается время последнего запуска приложения.

Закладка Все приложения

Список приложений

В списке содержатся приложения, установленные на вашем компьютере. Для каждого приложения в списке отображается информация о статусе, цифровой подписи, группе доверия, популярности приложения среди пользователей KSN и времени последнего запуска.

По двойному щелчку мышью на строке приложения или процесса открывается окно **Правила приложения**. В окне можно настроить правила для контроля действий приложения.

По правой клавише мыши на строке приложения открывается контекстное меню. Из контекстного меню можно выполнить следующие действия:

- открыть окно **Правила приложения**, в котором можно настроить разрешения для действий приложения;
- разрешить или запретить запуск приложения;
- переместить приложение в другую группу доверия;
- установить для приложения настройки контроля активности, предусмотренные по умолчанию (сбросить настройки приложения);
- удалить приложение из списка;
- открыть папку, содержащую исполняемый файл приложения.

Приложения в списке объединены в группы и подгруппы. По правой клавише мыши на строке группы открывается контекстное меню. Из контекстного меню можно выполнить следующие действия:

- открыть окно **Правила группы**, в котором можно настроить разрешения для действий приложения из этой группы, используемые по умолчанию;
- создать подгруппу внутри группы; по умолчанию к подгруппе применяются правила, указанные для группы, в которую она входит;
- добавить приложение в группу; по умолчанию к приложению применяются правила, указанные для группы, в которую она входит;
- установить для группы и всех входящих в нее подгрупп и приложений настройки контроля активности, предусмотренные по умолчанию (сбросить настройки группы);
- установить для подгрупп и приложений, входящих в группу, настройки контроля активности, предусмотренные по умолчанию, оставив настройки группы без изменений (сбросить настройки подгрупп и приложений);
- удалить входящие в группу подгруппы и приложения.

Приложение

В графе отображается название приложения.

Статус

В графе отображается состояние приложения: *Выполняется* или *Остановлено*.

Цифровая подпись

В графе отображается информация о наличии цифровой подписи у приложения и владельце цифровой подписи.

Группа доверия

В графе отображается группа доверия, в которую помещено приложение. Группа доверия определяет правила использования приложения на компьютере: запрет или разрешение запуска, доступ приложения к файлам и системному реестру, ограничения сетевой активности приложения.

Популярность

В графе отображается уровень популярности приложения среди участников Kaspersky Security Network (KSN). Уровень популярности соответствует числу участников KSN, использующих приложение.

Последний запуск

В графе отображается время последнего запуска приложения.

Окно Отправить отзыв

Проблема

Раскрывающийся список, где вы можете выбрать категорию, к которой относится ваш отзыв. Категория отзыва может затрагивать проблему с сайтом, открытым в защищенном режиме браузера:

- **Не использую**. Выберите этот элемент, если вы не используете или решили отказаться от использования Безопасных платежей.
- **Медленно открывается сайт**. Выберите этот элемент, если сайт работает медленнее, чем в браузере, запущенном в обычном режиме.
- **Защищенный режим браузера включается не тогда, когда нужно**. Выберите этот элемент, если в защищенном режиме браузера открываются сайты, не требующие использования Безопасных платежей.
- **Не получается авторизоваться на сайте**. Выберите этот элемент, если при попытках авторизоваться на сайте, открытом в защищенном режиме браузера, возникают ошибки.
- **Не открывается или неправильно отображается сайт**. Выберите этот элемент, если сайты не открываются в защищенном режиме браузера или отображаются с ошибками / искажениями.
- **Сертификаты сайта проверяются с ошибками**. Выберите этот элемент, если при проверке сертификатов сайта появляются сообщения об ошибках.
- **Невозможно сделать снимок экрана, если включен защищенный режим браузера**. Выберите этот элемент, если в защищенном режиме браузера не создаются скриншоты.
- **Ошибки во время ввода данных с клавиатуры или из буфера обмена**. Выберите этот элемент, если во время ввода данных в защищенном режиме браузера возникают ошибки.
- **Не печатается страница, открытая в защищенном режиме браузера**. Выберите этот элемент, если вы не можете распечатать открытую страницу сайта.
- **Появляется предупреждение о том, что не установлены важные обновления операционной системы**. Выберите этот элемент, если при запуске защищенного режима браузера появляется сообщение "Не установлены важные обновления операционной системы".
- **Защищенный режим браузера включается в другом браузере**. Выберите этот элемент, если защищенный режим браузера открывается не в том браузере, в котором вы его запустили.
- **Работает с ошибками**. Выберите этот элемент, если при работе защищенного режима браузера возникают ошибки.
- **Другая причина**. Выберите этот элемент, если ваша проблема не относится к указанным в других пунктах.

  Указывать категорию отзыва не обязательно.

Подробнее

В поле вы можете указать информацию, которая поможет сотрудникам "Лаборатории Касперского" решить вашу проблему. Заполнять поле необязательно.

Отправить

Отправка отзыва в "Лабораторию Касперского".

Вы можете отправить до 10 отзывов о работе с Безопасными платежами в сутки. Если приложению не удается отправить отзыв (например, отсутствует соединение с интернетом), приложение сохраняет отзыв на вашем компьютере. Отзывы хранятся в открытом виде в течение 30 дней.

Разрешения

Пароль защищает от изменения пользователем или группой пользователей следующие настройки приложений. Если флажок установлен напротив какого-либо действия, это означает, что выбранное действие разрешено пользователю или группе пользователей.

Настройка приложения	Изменение настроек приложения в главном окне, окне **Настройка**, в Центре уведомлений и в самих уведомлениях. Включение и выключение трассировки приложения.
Управление резервным копированием	Создание, изменение, удаление задач резервного копирования, а также задач восстановления данных из резервных копий.
Вход в Веб-Контроль	Вход и изменение настроек компонента Веб-Контроль
Завершение работы приложения	Выход из приложения.
Удаление / изменение / восстановление приложения	Удаление, изменение или восстановление приложения.
Удаление ключа	Удаление или изменение кода активации.
Просмотр отчетов	Переход в окно **Отчеты**.
Выключение компонентов защиты	Выключение и включение компонентов защиты, представленных в окне **Настройка**.

Устранение повреждений / Отмена изменений

В этом окне отображается процесс устранения повреждений операционной системы, обнаруженных в ходе анализа. Устранение повреждений может занять некоторое время.

Если на первом шаге был выбран вариант **Отменить изменения**, мастер восстановления после заражения выполняет откат действий, выбранных на предыдущем шаге.

Окно Информация о лицензии

В окне содержится информация о лицензии на приложение:

- Лицензионный ключ.
- Статус лицензии.
- Количество компьютеров, на которые распространяется лицензия.
- Дата активации.
- Дата окончания срока действия лицензии.
- Количество дней, оставшихся до окончания срока действия лицензии.

Предотвращение вторжений

В блоке **Приложения** отображается информация о количестве приложений, которые контролирует приложение Kaspersky Small Office Security.

Управлять приложениями

По ссылке открывается окно **Управление приложениями**. В этом окне можно указать группы доверия приложений, разрешить или запретить запуск приложений, а также перейти к настройке разрешений для отдельного приложения.

В блоке **Текущая активность** отображается информация о количестве приложений и процессов, запущенных в данный момент. В графическом виде представлена информация о загрузке центрального процессора, объеме оперативной памяти и дискового пространства, а также о сетевой активности.

Посмотреть всю активность

По ссылке открывается окно **Активность приложений** на закладке **Работающие**. В этом окне можно просмотреть информацию о потреблении ресурсов компьютера каждым приложением, запущенным в текущий момент, а также перейти к настройке разрешений для отдельного приложения.

Предотвращение вторжений. Исключения

Исключения

Содержит ресурсы с персональными данными, исключаемые из области защиты Предотвращения вторжений. Ресурсом может быть файл, папка или ключ реестра.

Ресурс

Графа, в которой указывается название ресурса.

Путь

Графа, в которой указывается расположение ресурса. Путь может содержать маску.

Статус

В графе отображается раскрывающийся список со статусом ресурса:

- **Включить контроль**. Если выбран этот вариант, приложение контролирует действия с этим ресурсом.
- **Выключить контроль**. Если выбран этот вариант, приложение не контролирует действия с этим ресурсом.

Нажав левой клавишей мыши на значок статуса, в раскрывающемся списке вы можете включить или выключить контроль ресурса.

Добавить

При нажатии на кнопку открывается окно, в котором можно указать ресурс с персональными данными, добавляемыми в список.

Изменить

Кнопка, при нажатии на которую открывается окно **Изменение файла или папки** / **Изменение ключа реестра**. В окне можно изменить настройки выбранного ресурса.

Ресурсы, добавленные в список по умолчанию, не подлежат изменению.

Удалить

Кнопка, при нажатии на которую выбранный ресурс удаляется из списка.

Ресурсы, добавленные в список по умолчанию, не подлежат удалению.

Закладка Общие

Закладка Общие

Описание выбранной группы приложений.

Закладка Ресурсы

На этой закладке можно выбрать системные ресурсы или ресурсы пользователя и изменить права доступа приложений к этим ресурсам.

Кнопка 

С помощью кнопки-переключателя можно открывать или скрывать панель настройки правил.

Вид

В раскрывающемся списке можно выбрать два варианта фильтрации ресурсов:

- **Скрывать системные приложения**. Если выбран этот вариант, в списке ресурсов не отображаются ресурсы системных приложений.
- **Скрывать Kaspersky Small Office Security**. Если выбран этот вариант, в списке не отображаются ресурсы приложения Kaspersky Small Office Security.

Операционная система

Содержит настройки и ресурсы операционной системы выбранной категории. Ресурсом может быть файл или папка, ключ реестра, сетевой сервис или IP-адрес. Предотвращение вторжений контролирует доступ других приложений к ресурсам из списка.

По умолчанию в список **Операционная система** входят следующие объекты:

- ключи реестра, содержащие настройки автозапуска;
- ключи реестра, содержащие настройки работы в интернете;
- ключи реестра, влияющие на безопасность операционной системы;
- ключи реестра, содержащие настройки системных служб;
- системные файлы и папки;
- папки автозапуска.

Персональные данные

Содержит персональные данные пользователя, распределенные по ресурсам и категориям. Ресурсом может быть файл или папка. Предотвращение вторжений анализирует действия других приложений над ресурсами из списка.

По умолчанию в список персональных данных входят следующие объекты:

- файлы пользователя (папка "Мои документы", файлы cookies, данные об активности пользователя);
- файлы, папки и ключи реестра, содержащие настройки работы и важные данные наиболее часто используемых приложений: браузеров, файловых менеджеров, почтовых клиентов, IM-клиентов и электронных кошельков.

Ресурс

Графа, в которой содержится название ресурса операционной системы, защищаемого Предотвращением вторжений.

Путь

Графа, в которой указывается расположение ресурса. Путь может содержать маску.

Статус

В графе отображается раскрывающийся список со статусом ресурса:

- **Включить контроль**. Если выбран этот вариант, приложение контролирует действия с этим ресурсом.
- **Выключить контроль**. Если выбран этот вариант, приложение не контролирует действия с этим ресурсом.

Нажав левой клавишей мыши на значок статуса, в раскрывающемся списке вы можете включить или выключить контроль ресурса.

Добавить

В раскрывающемся списке можно добавить категорию ресурсов, файл или папку с ресурсами или ключ системного реестра.

Изменить

По ссылке открывается окно, в котором можно изменить название выбранного ресурса и путь к нему.

Удалить

По ссылке можно удалить из списка выбранную категорию ресурсов, файл или папку с ресурсами или ключ системного реестра. Предотвращение вторжений не будет контролировать доступ других приложений к этому ресурсу.

Восстановить

В раскрывающемся списке можно выбрать варианты действия:

- **настройки категории**. Если выбран этот вариант, настройки выбранной категории получат значения по умолчанию.
- **настройки подгрупп и ресурсов**. Если выбран этот вариант, настройки входящих в категорию подгрупп и ресурсов получат значения по умолчанию.

Список приложений

В списке отображаются группы доверия и приложения, входящие в эти группы доверия. В графах **Чтение**, **Запись**, **Создание**, **Удаление** указаны права доступа приложения или группы приложений к выбранному ресурсу.

В таблице ниже приведено описание действий Kaspersky Small Office Security, если приложение или группа приложений пытается получить доступ к ресурсу.

Операции производимые приложением Kaspersky Small Office Security

Действие	Описание
Наследовать	Приложение или группа приложений наследует реакцию из вышестоящей группы.
Разрешить	Приложение Kaspersky Small Office Security разрешает приложением, входящим в выбранную группу, доступ к ресурсу.
Запретить	Приложение Kaspersky Small Office Security запрещает приложениям, входящим в выбранную группу, доступ к ресурсу.
Спрашивать пользователя	Если в разделе **Настройка → Настройки безопасности → Исключения и действия с найденными объектами** установлен флажок **Автоматически выполнять рекомендуемые действия**, приложение Kaspersky Small Office Security автоматически выбирает действие с этим ресурсом по правилам, созданным специалистами "Лаборатории Касперского". По сноске вы можете прочитать, какое именно действие будет выбрано. Если флажок снят, приложение Kaspersky Small Office Security спрашивает пользователя, разрешать этому приложению доступ к ресурсу или нет.
Записывать в отчет	Помимо заданной реакции приложение Kaspersky Small Office Security записывает в отчет информацию о попытке доступа приложения к ресурсу.

Окно Лицензионное соглашение

Окно содержит текст Лицензионного соглашения. Для просмотра Лицензионного соглашения вы можете воспользоваться полосой прокрутки.

Окно Лицензирование

В блоке, расположенном в верхней части окна, представлена информация о лицензии:

- Лицензионный ключ

  Использование программы по действующей лицензии можно прекратить, нажав на кнопку .

- Статус ключа.
- Количество компьютеров, на которое распространяется лицензия.
- дату активации;
- Дата окончания срока действия лицензии.
- Количество дней, оставшихся до окончания срока действия лицензии.

  Для подписки возможно отображение дополнительной информации о статусе подписки.

О лицензии / О подписке

По ссылке открывается окно со сведениями о действующей лицензии или подписке.

Лицензионное соглашение

При нажатии на кнопку открывается окно с текстом Лицензионного соглашения.

В зависимости от наличия лицензии, подписки и от особенностей вашей версии приложения в окне могут отображаться различные кнопки для запуска действий, связанных с лицензией или подпиской. Ниже приведены описания кнопок, предусмотренных по умолчанию.

Активировать приложение / Ввести код активации

Кнопка, при нажатии на которую запускается мастер активации приложения.

Кнопка отображается, если приложение не активировано, или если подписка, по которой вы используете приложение, истекла или истекает.

Купить лицензию

При нажатии на кнопку открывается окно браузера на странице интернет-магазина, в котором вы можете приобрести лицензию.

Восстановить мои коды активации

По ссылке вы можете перейти на сайт Центр управления Kaspersky Small Office Security и посмотреть информацию о ваших кодах активации.

Обновить базы

Кнопка, при нажатии на которую запускается обновление баз приложения.

Кнопка отображается, если возникшие проблемы с лицензией можно решить обновлением баз (например, дата выпуска баз не соответствует сроку действия лицензии).

Причины и возможные решения

Кнопка, при нажатии на которую открывается окно браузера на сайте Службы технической поддержки с информацией о возникшей проблеме.

Кнопка отображается, если возникли проблемы с действующей лицензией.

Обновить статус

Кнопка, при нажатии на которую с сервера поставщика услуг скачивается актуальная информация о статусе подписки.

Кнопка отображается, если приложение используется по подписке.

Посетить сайт поставщика услуг

Кнопка, при нажатии на которую открывается окно браузера на сайте поставщика услуг.

Кнопка отображается, если приложение используется по подписке.

Найдены другие несовместимые приложения

Список несовместимых приложений

В списке перечислены приложения, несовместимые с устанавливаемым приложением. Для корректной работы устанавливаемого приложения нужно удалить несовместимые с ним приложения.

Удалить вручную

Кнопка, при нажатии на которую открывается окно со списком приложений, установленных на компьютере. В этом списке можно выбрать приложения, несовместимые с устанавливаемым приложением, чтобы удалить их с компьютера.

Продолжить

Кнопка, при нажатии на которую несовместимые приложения, представленные в списке, остаются на компьютере, а мастер продолжает работу.

Одновременное использование приложений, несовместимых с устанавливаемым приложением, может привести к некорректной работе устанавливаемого приложения и существенному ослаблению защиты вашего компьютера.

Найдены несовместимые приложения

Список несовместимых приложений

В списке перечислены приложения, несовместимые с устанавливаемым приложением. Для корректной работы устанавливаемого приложения нужно удалить несовместимые с ним приложения.

Удалить

Кнопка, при нажатии на которую несовместимые приложения, представленные в списке, удаляются с компьютера, а мастер продолжает работу.

Оставить

Кнопка, при нажатии на которую несовместимые приложения, представленные в списке, остаются на компьютере, а мастер продолжает работу.

Одновременное использование приложений, несовместимых с устанавливаемым приложением, может привести к некорректной работе устанавливаемого приложения и существенному ослаблению защиты вашего компьютера.

Необходимо перезагрузить компьютер

Перезагрузить компьютер

Флажок включает / выключает перезагрузку компьютера, необходимую для продолжения работы мастера миграции.

Если флажок установлен, то при нажатии на кнопку **Готово** компьютер перезагружается, после чего мастер миграции продолжает работу.

Если флажок снят, то компьютер не перезагружается. Мастер миграции автоматически продолжит работу после того, как вы перезагрузите или выключите и снова включите компьютер.

Начало работы

Показать информацию о сертификате

По ссылке открывается окно с информацией о сертификате "Лаборатории Касперского".

Далее

Кнопка, при нажатии на которую мастер установки сертификата начинает работу.

Установка сертификата

В этом окне отображается процесс автоматической установки сертификата. Выполнение задачи может занять некоторое время.

Приложение Kaspersky Small Office Security выполняет поиск браузеров, установленных на компьютере пользователя, и автоматически устанавливает сертификаты в хранилище сертификатов Microsoft Windows.

В процессе установки сертификата на экране может появиться предупреждение системы безопасности Microsoft Windows, в котором потребуется подтвердить намерение установить сертификат.

Завершение работы мастера

Готово

Кнопка, при нажатии на которую приложение Kaspersky Small Office Security завершает работу мастера установки сертификата.

Раздел Заблокированные компьютеры

Заблокированные компьютеры

Содержит данные о компьютерах, сетевую активность которых по отношению к вашему компьютеру заблокировал компонент Защита от сетевых атак.

Адрес компьютера

Графа, в которой отображается IP-адрес заблокированного компьютера.

Время начала блокирования

Графа, в которой отображается время с момента блокирования.

По умолчанию компонент Защита от сетевых атак блокирует входящий трафик от атакующего компьютера в течение часа.

Вы можете разблокировать выбранный в списке компьютер с помощью его контекстного меню.

Разблокировать

При нажатии на кнопку компонент Защита от сетевых атак разблокирует выбранный компьютер.

Разблокировать все компьютеры

По ссылке компонент Защита от сетевых атак разблокирует все заблокированные компьютеры.

Раздел Открытые порты

Вид

При нажатии на кнопку открывается меню, которое содержит следующие пункты:

- **Показывать все порты** – в списке отображаются все открытые порты вашего компьютера.
- **Скрывать порты loopback** – в списке отображаются все порты, кроме тех, которые используются сетевым программным обеспечением операционной системы.

Открытые порты

Содержит информацию обо всех открытых в данный момент портах для каждого процесса.

Для каждого порта указана следующая информация:

- номер порта;
- имя процесса (приложения, службы, сервера), который использует порт;
- идентификатор процесса;
- локальный IP-адрес процесса;
- протокол, по которому выполняется соединение через порт.

По двойному щелчку на строке списка открывается окно **Правила приложения** на закладке **Сетевые правила**. В этом окне вы можете настроить сетевые правила для приложения, которое использует выбранный порт.

По правой клавише мыши на элементе списка открывается контекстное меню, из которого можно перейти к настройке сетевых правил.

Меню содержит следующие пункты:

- **Сетевые правила приложений**. При выборе этого пункта меню открывается окно **Правила приложения** на закладке **Сетевые правила**. В окне вы можете настроить сетевое правило для приложения, которое использует порт, выбранный в списке.
- **Все сетевые правила**. При выборе этого пункта меню открывается окно **Пакетные правила**. В окне вы можете настроить пакетные правила для приложения, которое использует порт, выбранный в списке.

Раздел Сетевая активность

Вид

Кнопка, при нажатии на которую открывается меню. Меню содержит следующие пункты:

- **Показывать локальные соединения** – в списке отображается информация о соединениях вашего компьютера с другими компьютерами в локальной сети.
- **Показывать соединения Kaspersky Small Office Security** – в списке отображается информация о соединениях, установленных приложением Kaspersky Small Office Security.

Сетевая активность

Содержит активные сетевые соединения, установленные на вашем компьютере в данный момент.

Для каждого соединения указана следующая информация:

- название процесса (приложения, службы, сервера), который инициировал соединение;
- направление соединения (входящее / исходящее);
- протокол, по которому выполняется соединение;
- настройки соединения (удаленный порт и IP-адрес);
- объем переданной / принятой информации в килобайтах.

По правой клавише мыши на элементе списка открывается контекстное меню, из которого можно перейти к настройке сетевых правил.

Меню содержит следующие пункты:

- **Сетевые правила приложений**. При выборе этого пункта меню открывается окно **Правила приложения** на закладке **Сетевые правила**. В этом окне вы можете настроить сетевое правило для приложения, выбранного в списке.
- **Все сетевые правила**. При выборе этого пункта меню открывается окно **Пакетные правила**. В этом окне вы можете настроить пакетные правила для приложения, выбранного в списке.

Блокировать любую сетевую активность

По ссылке Сетевой экран запрещает сетевую активность всем процессам.

В нижней части окна отображается график объема входящего и исходящего трафика для процесса, выбранного в списке. График показывает объем трафика в режиме реального времени. Объем трафика указывается в килобайтах.

Особенности добавления правила для сетевого адаптера

Когда вы создаете разрешающее правило для сетевого адаптера и / или правило с указанием TTL, это правило может конфликтовать с запрещающим правилом для приложений. Например, если приложение находится в группе "Сильные ограничения", ей будет запрещен сетевой доступ, даже если вы создали разрешающее пакетное правило для сетевого адаптера (а также для TTL).

Чтобы разрешающее правило работало для всех приложений, которые будут пытаться подключаться к сети через этот сетевой адаптер, необходимо создать следующие правила в порядке приоритета от наиболее приоритетного к наименее приоритетному (в общем списке пакетных правил приоритет считается сверху вниз от самого приоритетного к наименее приоритетному).

1. Разрешающее правило для выбранного сетевого адаптера.

2. Запрещающие правила для всех остальных сетевых адаптеров.

3. Разрешающее правило без указания сетевого адаптера.

Чтобы работало разрешающее правило для сетевого адаптера с использованием TTL, необходимо создать следующие правила в порядке приоритета от наиболее приоритетного к наименее приоритетному:

1. Разрешающее правило для конкретного значения TTL.

2. Запрещающее правило для TTL со значением равным 255.

3. Разрешающее правило без указания конкретного значения TTL.

Раздел Сетевой трафик

Период

Список содержит интервалы времени для просмотра распределения сетевого трафика.

Возможные значения:

- **За день**. В списке отображается распределение сетевого трафика за текущие сутки.
- **За вчера**. В списке отображается распределение сетевого трафика за вчерашние сутки.
- **За месяц**. В списке отображается распределение сетевого трафика за текущий месяц.
- **За год**. В списке отображается распределение сетевого трафика за текущий год.

Сетевой трафик

Содержит информацию обо всех входящих и исходящих соединениях между вашим компьютером и другими компьютерами.

Для каждого приложения (компьютера, службы, сервера, процесса) указан объем входящего и исходящего трафика.

По двойному щелчку на приложении в списке открывается окно **Правила приложения** на закладке **Сетевые правила**. В этом окне вы можете настроить сетевые правила для выбранного приложения.

По правой клавише мыши на элементе списка открывается контекстное меню, из которого можно перейти к настройке сетевых правил.

Меню содержит следующие пункты:

- **Сетевые правила приложений**. При выборе этого пункта открывается окно **Правила приложения** на закладке **Сетевые правила**, на которой вы можете настроить сетевое правило для выбранного приложения.
- **Все сетевые правила**. При выборе этого пункта открывается окно **Пакетные правила**, в котором вы можете настроить пакетные правила для выбранного приложения.

В нижней части окна отображается диаграмма распределения трафика выбранного приложения по времени за выбранный период.

Разрыв сетевых соединений

Если в момент завершения работы на компьютере или приостановки защиты были установлены сетевые соединения, контролируемые приложением, на экран будет выведено уведомление о разрыве этих соединений. Это необходимо для корректного завершения работы приложения. Разрыв происходит автоматически по истечении 10 секунд либо при нажатии на кнопку **Да**. Большинство прерванных соединений восстанавливается через некоторое время.

Если во время разрыва соединения вы скачиваете файл без использования менеджера загрузки, передача данных будет прервана. Для получения файла вам потребуется повторно инициировать его загрузку.

Вы можете отменить разрыв соединений. Для этого в окне уведомления нажмите на кнопку **Нет**. При этом приложение продолжит свою работу.

Обнаруженные объекты

Устранить

При нажатии на кнопку приложение Kaspersky Small Office Security запускает обработку обнаруженного объекта.

Кнопка отображается при наличии обнаруженного объекта.

При нажатии на кнопку раскрывается меню, в котором можно выбрать дополнительное действие:

- **Добавить в исключения** – создать исключение, в соответствии с которым объект не должен считаться вредоносным.
- **Игнорировать** – перенести уведомление в раздел **Игнорируемые уведомления**.
- **Открыть папку с файлом** – открыть папку исходного размещения файла.
- **Узнать больше** – открыть веб-страницу с описанием обнаруженного объекта.

Окна уведомлений Kaspersky Small Office Security

Уведомления приложения, появляющиеся в области уведомлений панели задач, информируют о событиях, происходящих в процессе работы приложения и требующих вашего внимания.

При появлении на экране уведомления следует выбрать один из предложенных в уведомлении вариантов действия. Оптимальный вариант – тот, который рекомендован специалистами "Лаборатории Касперского" по умолчанию.

Окно Веб-Контроль

Список учетных записей

Содержит учетные записи пользователей компьютера.

В списке отображается следующая информация о пользователе:

- изображение пользователя, установленное в настройках Веб-Контроля;
- псевдоним пользователя;
- статус контроля пользователя с помощью Веб-Контроля (**Включен** или **Выключен**).

Изображение пользователя

По нажатию на изображение пользователя открывается окно, содержащее статистику использования интернета и приложений. Из этого окна можно перейти к просмотру отчета Веб-Контроля, а также к настройке Веб-Контроля.

Настроить ограничения

По ссылке открывается окно, в котором вы можете настроить контроль действий пользователя с помощью Веб-Контроля.

Посмотреть отчет

По ссылке открывается окно, содержащее статистику использования интернета и приложений выбранным пользователем. Из этого окна можно перейти к просмотру отчета Веб-Контроля, а также к настройке Веб-Контроля.

Переключатель  / 

Переключатель включает / выключает контроль действий пользователя:

 – контроль действий пользователя включен.

 – контроль действий пользователя выключен.

Окно Создайте пароль

Защита паролем

Отображается при переходе к настройкам Веб-Контроля, если не задан пароль для ограничения доступа к управлению Kaspersky Small Office Security. Включает в себя следующие элементы управления:

- **Пароль**. В этом поле вводится пароль.
- **Подтверждение**. В этом поле пароль вводится повторно.
- **Продолжить**. При нажатии на эту кнопку отображается окно **Веб-Контроль**, из которого можно перейти к просмотру профилей пользователей и настройке Веб-Контроля.
- **Пропустить**. По ссылке отображается окно **Веб-Контроль**, доступ к управлению Веб-Контролем не ограничивается.

Введите пароль

Отображается при переходе к настройкам Веб-Контроля, если доступ к нему защищен паролем. Включает в себя следующие элементы управления:

- Поле ввода пароля.
- **Войти**. При нажатии на эту кнопку открывается окно **Веб-Контроль**.
- **Запомнить пароль на эту сессию**. При установке этого флажка Kaspersky Small Office Security запоминает введенный пароль и в течение текущей сессии больше его не запрашивает.

Об облачной защите

В этом окне вы можете ознакомиться с информацией о Kaspersky Security Network.

Окно Активация

В этом окне отображается процесс активации приложения.

Отмена

При нажатии на кнопку можно отменить активацию приложения.

Регистрация и авторизация

Адрес электронной почты

Поле для ввода адреса электронной почты для подключения к существующему аккаунту Центр управления Kaspersky Small Office Security или создания нового аккаунта.

Войти с помощью Google

При нажатии на кнопку выполняется переход к форме входа в аккаунт Google в браузере по умолчанию (доступно не во всех регионах).

Войти с помощью Facebook*

При нажатии на кнопку выполняется переход к форме входа в аккаунт Facebook* в браузере по умолчанию (доступно не во всех регионах).

Войти с помощью Apple

При нажатии на кнопку выполняется переход к форме входа в аккаунт Apple в браузере по умолчанию.

Войти с помощью Яндекс ID

При нажатии на кнопку выполняется переход к форме входа в аккаунт Яндекс в браузере по умолчанию.

Войти с помощью VK ID

При нажатии на кнопку выполняется переход к форме входа в аккаунт VK в браузере по умолчанию.

Доступность функции быстрого входа зависит от вашего региона. Более подробную информацию об ограничениях в России можно найти в этой статье (доступна только на английском и русском языках).

У меня есть код активации

При нажатии на ссылку открывается форма ввода кода активации.

Продолжить

При нажатии на кнопку выполняется переход в форму ввода пароля от существующего аккаунта Центр управления Kaspersky Small Office Security или начинается процесс создания нового аккаунта.

При входе в существующий аккаунт Центр управления Kaspersky Small Office Security в окне отображается следующее:

Пароль

Поле для ввода пароля от аккаунта Центр управления Kaspersky Small Office Security.

Забыли пароль?

Переход к окну восстановления пароля от аккаунта Центра управления Kaspersky Small Office Security, если вы его забыли.

Ввести другой email

При нажатии на кнопку происходит возврат в форму ввода адреса электронной почты.

Войти

При нажатии на кнопку происходит подключение устройства к аккаунту Центр управления Kaspersky Small Office Security.

В процессе создания аккаунта Центр управления Kaspersky Small Office Security в окне отображается следующее:

Я разрешаю уведомлять меня о персонализированных специальных предложениях, обзорах, опросах, незавершенных заказах и актуальных новостях и событиях. Я понимаю, что могу отозвать согласие в любое время в настройках аккаунта или по ссылке в письмах

Если флажок установлен, вы будете получать от "Лаборатории Касперского" специальные предложения, обзоры, опросы, напоминания о завершении заказа, актуальную информацию о новостях и событиях на указанный адрес электронной почты. Вы можете в любой момент отказаться от получения маркетинговых материалов через My Kaspersky. Более подробную информацию смотрите в этой статье.

Регион

По ссылке открывается окно выбора региона. От выбранного региона зависит, какие приложения и какие способы оплаты вы сможете использовать.

Ввести другой email

При нажатии на кнопку происходит возврат в форму ввода адреса электронной почты.

Создать

При нажатии на кнопку выполняется регистрация аккаунта Центра управления Kaspersky Small Office Security. На указанный вами адрес электронной почты придет письмо, содержащее ссылку для создания пароля от аккаунта Центр управления Kaspersky Small Office Security.

Подробнее об аккаунте Центр управления Kaspersky Small Office Security

*Facebook принадлежит компании META Inc, признанной экстремистской организацией на территории Российской Федерации.

Окно Выбор ключа в реестре

Выбрать

При нажатии на кнопку поля в окне **Добавление ключа реестра** заполняются значениями выбранного ключа.

Окно Выбор папки хранения секретной папки

В этом окне можно выбрать место хранения создаваемой секретной папки.

Выбрать

При нажатии на кнопку можно подтвердить, что указанный путь верный.

Окно Выбор файла или папки

Выбрать

При нажатии на кнопку путь к файлу или папке отображается в окне **Добавление файла или папки** в поле **Путь**.

Окно Группа доверия для неизвестных приложений

В этом окне отображаются приложения, которые не удалось распределить по другим группам. Вы можете выбрать группу доверия из списка и нажать на кнопку **Сохранить**. Приложения, которые не удалось распределить по другим группам, будут попадать в указанную вами группу доверия.

По умолчанию такие приложения помещаются в группу **Слабые ограничения**.

Окно Группа доверия для приложений, запущенных до начала работы Kaspersky Small Office Security

В этом окне можно выбрать группу доверия для неизвестных приложений, запущенных до начала работы приложения Kaspersky Small Office Security.

Список групп доверия

В списке можно указать группу доверия, в которую нужно помещать приложения, запущенные до начала работы приложения Kaspersky Small Office Security. Сетевая активность таких приложений будет ограничиваться в соответствии с правилами выбранной группы доверия. По умолчанию сетевая активность приложений, запущенных до начала работы приложения Kaspersky Small Office Security, ограничивается в соответствии с правилами, заданными специалистами "Лаборатории Касперского".

Выбрать группу доверия автоматически

Если выбран этот вариант, компонент Предотвращение вторжений помещает приложения, запущенные до начала работы приложения Kaspersky Small Office Security, в одну из групп доверия на основании правил, заданных специалистами "Лаборатории Касперского".

Выбрать группу доверия вручную

Если выбран этот вариант, вы можете самостоятельно выбрать группу доверия, в которую необходимо помещать приложения, запущенные до начала работы приложения Kaspersky Small Office Security.

Окно Добавление / изменение исключения Защиты от сбора данных в интернете

Маска веб-адреса

В поле вы можете указать IP-адрес или веб-адрес (URL) сайта, на котором вы хотите разрешить сбор данных о ваших действиях.

Настройки Обнаружения удаленного доступа

Доверенные приложения удаленного администрирования (такие как TeamViewer, LogMeIn Pro и Remotely Anywhere) могут изменять настройки Kaspersky Small Office Security.

Недоверенным приложениям удаленного администрирования изменение настроек приложения Kaspersky Small Office Security будет запрещено.

Настройки Самозащиты

Настройка	Описание
Включить самозащиту	Если флажок установлен, то Kaspersky Small Office Security предотвращает изменение и удаление файлов приложения на жестком диске, процессов в памяти и записей в системном реестре.
Разрешить управление настройками Kaspersky Small Office Security через приложения удаленного управления	Если флажок установлен, доверенные приложения удаленного администрирования (такие как TeamViewer, LogMeIn Pro и Remotely Anywhere) могут изменять настройки приложения Kaspersky Small Office Security. Недоверенным приложениям удаленного администрирования изменение настроек приложения Kaspersky Small Office Security будет запрещено, даже если флажок установлен.
Блокировать внешнее управление службами приложения	Если флажок установлен, то приложение Kaspersky Small Office Security запрещает управление службами приложения с помощью сторонних приложений (например, CMD). При попытке управления службами приложениями с удаленного компьютера, над значком приложения в области уведомлений панели задач Microsoft Windows отображается уведомление (если служба уведомлений не выключена пользователем). Вы можете предоставить возможность внешнего управления службами приложения только на компьютерах без поддержки технологии AM-PPL или с выключенной технологией. Технология AM-PPL доступна для операционных систем Windows 10 версии 1703 (RS2) и выше, а также для Windows Server 2019.

Окно Добавление / Изменение категории

Название категории

В этом поле можно указать название категории ресурсов, доступ к которым со стороны приложений должен анализировать и контролировать компонент Предотвращение вторжений.

Окно Добавление / Изменение ключа реестра

Выбрать

При нажатии на кнопку открывается окно **Выбор ключа в реестре**, где вы можете выбрать ключ реестра, доступ к которому должен контролировать компонент Предотвращение вторжений.

Название

В поле можно указать название ресурса с ключом реестра.

Путь к ключу

В поле можно указать путь к ключу реестра.

Защитить значение ключа

Если флажок установлен, от изменения защищается только значение ключа, указанное в поле **Значение ключа**.

Если флажок снят, то защищаются все значения этого ключа реестра.

Если в поле **Значение ключа** не указано никакого значения, то защищается значение ключа реестра по умолчанию.

Флажок автоматически устанавливается при выборе ключа реестра.

Значение ключа

В поле можно указать значение ключа реестра, которое компонент Предотвращение вторжений должен защищать от изменения.

Поле доступно, если установлен флажок **Защитить значение ключа**.

Добавить

При нажатии на кнопку ключ реестра добавляется в список ресурсов.

Окно Добавление / Изменение файла или папки

Название

В поле можно указать название ресурса с файлом или папкой, доступ к которым должно контролировать Предотвращение вторжений.

Путь

В поле вы можете вручную указать путь к файлу или папке.

При вводе пути вручную вы можете использовать маску.

Маска `\*` позволяет указать, что нужно контролировать доступ ко всем файлам в выбранной папке.

Маска `\*<расширение>` позволяет указать, что нужно контролировать доступ ко всем файлам с определенным расширением в выбранной папке.

Также вы можете контролировать доступ приложений к файловым ресурсам, расположенным на удаленном компьютере. Для этого укажите путь к сетевому ресурсу в UNC-формате согласно правилу `\\<Server>\<Share>\<Относительный путь>`, в котором:

- <Server> – доменное имя компьютера или IP-адрес в формате IPv4 или IPv6 (обязательно для ввода).
- <Share> – сетевое имя общей папки (обязательно для ввода).
- <Относительный путь> – путь к папке или файлу из общей папки (необязательно для ввода).

  Примеры путей:

- `\\Server1\ShareFolder1\test\example.exe`
- `\\Server1\ShareFolder1\test\*.docx`
- `\\Server1\ShareFolder1\*`

  Приложение не контролирует доступ к файловому ресурсу, если заданный в правиле путь отличается от пути, по которому выполняется обращение.

Выбрать

При нажатии на кнопку открывается окно, где вы можете выбрать файл или папку.

Добавить

При нажатии на кнопку папка или файл добавляется в список ресурсов.

Окно завершения активации

Это окно открывается, если приложение активировано успешно.

Готово

При нажатии на кнопку завершается процедура активации приложения. Выполняется переход в окно лицензирования.

Окно Запрещенные и разрешенные приложения

В этом окне отображается список приложений, которым разрешено или запрещено изменять настройки операционной системы. Пустой список означает, что вы еще не разрешали и не запрещали приложениям изменять настройки операционной системы.

Список приложений

Список приложений содержит следующую информацию:

- **Приложение**. В графе отображается название приложения.
- **Имя файла**. В графе отображается название исполняемого файла приложения.
- **Путь**. В графе отображается путь к исполняемому файлу приложения на жестком диске вашего компьютера.
- **Издатель**. В графе отображается цифровая подпись издателя приложения.
- **Изменения**. В графе отображается, запрещено или разрешено приложению изменять настройки операционной системы, браузеров, а также настройки сети.

Окно Защита приватности

В этом окне вы можете включать и выключать следующие компоненты:

Контроль камеры и микрофона

Защита от сбора данных в интернете

Обновление приложений. Исключения

Исключения

В список **Исключения** попадают пропущенные вами обновления установленных приложений. Вы можете пропустить как отдельное обновление, так и все обновления для приложения, установленного на компьютере.

Список **Исключения** состоит из следующих граф:

- **Приложение** – в графе отображается название приложения.
- **Пропускать** – графа может содержать следующие значения:
  - **Версия обновления** – отображается, если вы пропустили отдельное обновление для установленного приложения.
  - **Все обновления** – отображается, если вы решили не обновлять приложение.

Удалить

При нажатии на кнопку выбранные приложения удаляются из списка исключений. Кнопка доступна, если приложение выбрано в списке.

Приложение Kaspersky Small Office Security будет сообщать о наличии обновлений для приложений, удаленных из списка.

Окно Исключения Защиты от сбора данных в интернете

Список исключений

Список включает в себя адреса сайтов, на которых разрешен сбор данных о ваших действиях. На указанных сайтах компонент Защита от сбора данных в интернете обнаруживает попытки сбора данных, но не блокирует их, даже если в настройках компонента указано блокировать сбор данных этими категориями сервисов отслеживания.

Вы можете добавить в список веб-адрес или маску веб-адреса.

Изменить

Открывает окно, в котором можно изменить выбранный веб-адрес / маску веб-адреса.

Удалить

Удаляет из списка выбранный веб-адрес / маску веб-адреса.

Добавить

Открывает окно, в котором можно добавить веб-адрес / маску веб-адреса.

Окно Использование приложений

Приложение

В графе отображаются приложения и группы приложений, использование которых вы можете ограничить.

Использование

В графе указано, разрешено или запрещено пользователю работать с приложением или группой приложений:

- **Разрешено** – пользователь может работать с этим приложением или группой приложений.
- **Заблокировано** – пользователю запрещено работать с этим приложением или группой приложений.
- **Ограничено** – пользователь может работать с этим приложением или группой приложений ограниченное количество времени.

Вы можете разрешить, запретить или ограничить использование приложения или группы приложений для выбранного пользователя, выбрав нужный пункт раскрывающегося списка.

Путь

В графе отображается путь к исполняемому файлу приложения.

Правила

По кнопке открывается окно, где вы можете ограничить использование выбранного приложения по времени.

Удалить

Нажатие на кнопку удаляет выбранное приложение из списка. После удаления приложения из списка приложение Kaspersky Small Office Security перестает контролировать использование приложения, пользователь может работать с этим приложением без ограничений.

Добавить приложение

По кнопке открывается окно, в котором вы можете выбрать исполняемый файл приложения для добавления в список. Веб-Контроль помещает приложение в подходящую категорию в списке.

Окно Карантин

Список объектов на карантине

Содержит перечень файлов, помещенных на карантин. Карантин предназначен для хранения резервных копий файлов, которые были удалены или изменены в процессе лечения.

Файл

Графа, в которой отображается имя файла, помещенного на карантин.

По правой клавише мыши открывается контекстное меню, из которого можно перейти к действиям с файлом, помещенным на карантин: восстановлению, удалению, открытию файла в его исходной папке.

Путь

Графа, в которой отображается путь к файлу.

Обнаружено

Графа, в которой отображается тип обнаруженного объекта, например, *Сетевая атака*.

Дата и время

Графа, в которой отображается дата и время помещения файла на карантин.

Восстановить

При нажатии на кнопку приложение Kaspersky Small Office Security возвращает файл, выбранный в списке, в папку, в которой он находился до помещения на карантин.

Удалить

Кнопка, при нажатии на которую приложение Kaspersky Small Office Security удаляет резервную копию файла, выбранную в списке.

Удалить все

При нажатии на кнопку приложение Kaspersky Small Office Security удаляет все резервные копии файлов, помещенные на карантин.

Приложение Kaspersky Small Office Security не выполняет лечение приложений из Магазина Windows. Если в результате проверки такое приложение признано опасным, оно будет удалено с вашего компьютера. При удалении приложений из Магазина Windows приложение Kaspersky Small Office Security не создает резервные копии. Для восстановления таких объектов необходимо использовать средства восстановления операционной системы (подробную информацию можно получить из документации к операционной системе, установленной на вашем компьютере) либо обновить приложения через Магазин Windows.

Окно Новости

Список новостей

Новости в окне представлены в виде списка. Для каждой новости указывается ее заголовок, анонс, время появления.

По нажатию на заголовок новости открывается окно с текстом новости.

Окно Новости

Кнопки 

Кнопки, с помощью которых можно переходить к предыдущей или следующей новости.

Окно Настройки Менеджера приложений

Включить / выключить Менеджер приложений

Включение Менеджера приложений. Если переключатель включен, приложение Kaspersky Small Office Security контролирует установку и удаление дополнительных приложений, а также показ шагов установки, содержащих рекламу.

Во время установки приложений автоматически снимать флажки установки дополнительных приложений. Предупреждать при попытке установить дополнительные приложения

Если флажок установлен, при установке приложений на ваш компьютер приложение Kaspersky Small Office Security блокирует установку дополнительных приложений.

Если флажок снят после того, как вы уже запустили установку какого-либо приложения, Блокировщик скрытых установок продолжит свою работу в рамках текущей установки. Флажки напротив приложений, предлагаемых к дополнительной установке, будут сняты, а сами дополнительные приложения не будут устанавливаться. При последующей установке приложений эта функциональность работать не будет. Дополнительные приложения будут устанавливаться совместно с основным.

Функциональность помощника по установке ограничена в Microsoft Windows XP (x64). Функциональность помощника по установке может быть недоступна для некоторых приложений по установке.

Не отображать шаги установки, которые могут содержать рекламу или предложения об установке дополнительных приложений

Если флажок установлен, при установке приложений на ваш компьютер приложение Kaspersky Small Office Security блокирует показ рекламы или предложений об установке дополнительных приложений.

Окно Настройки обновления приложений

Включить поиск обновлений для приложений

Если флажок установлен, приложение Kaspersky Small Office Security ищет обновления для установленных приложений и предлагает скачать и установить их.

Задать расписание

По ссылке открывается окно, в котором вы можете задать режим поиска обновлений для приложений, установленных на вашем компьютере.

Если приложение Kaspersky Small Office Security установлено на файловом сервере, по умолчанию поиск уведомлений выполняется каждую пятницу в 19:30.

Автоматически скачивать и устанавливать обновления, если не требуется принимать новое лицензионное соглашение

Если флажок установлен, Kaspersky Small Office Security автоматически ищет обновления для установленных программ, а также скачивает и устанавливает найденные обновления, если для этого от вас не требуется принять новое лицензионное соглашение.

Это флажок недоступен, если приложение Kaspersky Small Office Security установлено на файловом сервере.

Искать обновления для приложений

В настройке требуется выбрать, какие обновления приложений будут устанавливаться:

- **Важные обновления, которые повышают безопасность компьютера** – будет установлены только важные обновления, которые устраняют уязвимости и повышают безопасность вашего компьютера.
- **Все обновления для известных приложений** – будут установлены все обновления.

Исключения

По ссылке открывается окно **Исключения** со списком исключений. В список исключений попадают пропущенные вами обновления установленных приложений. Вы можете пропустить как отдельное обновление, так и все обновления для приложения, установленного на компьютере.

Режим поиска обновлений / Расписание

В таблице описаны настройки, применимые к расписанию работы следующих компонентов: Обновление приложений, Менеджер приложений.

Настройка	Описание
Режим поиска обновлений (Обновление приложений) **Выполнять анализ** (Менеджер приложений)	**Автоматически**. Приложение Kaspersky Small Office Security выполняет задачу один раз в сутки согласно внутренним настройкам. **По минутам** / **По часам** / **По дням** / **Еженедельно** / **Ежемесячно** / **В указанное время**. Приложение Kaspersky Small Office Security выполняет задачу по сформированному вами расписанию, которое можно уточнить до минут. При выборе одного из этих вариантов доступен список **Отложить запуск после старта приложения на N минут**. **После запуска приложения**. Приложение Kaspersky Small Office Security выполняет задачу после своего запуска, спустя столько минут, сколько указано в поле **Запускать через N минут**. **После каждого обновления**. Приложение Kaspersky Small Office Security выполняет задачу после загрузки и установки нового пакета обновлений.
Запускать поиск обновлений на следующий день, если компьютер был выключен (Обновление приложений) **Выполнять анализ объектов на следующий день, если компьютер был выключен** (Менеджер приложений)	Если запланированный по расписанию поиск обновлений для приложений или анализ объектов пропущен из-за того, что компьютер был выключен, приложение Kaspersky Small Office Security выполняет задачу после включения компьютера. Флажок отображается, если выбран один из следующих режимов запуска: **По дням** / **Еженедельно** / **Ежемесячно** / **В указанное время**.
Искать обновления для приложений только в случае, когда компьютер заблокирован или включена экранная заставка (Обновление приложений) **Выполнять анализ объектов только в случае, когда компьютер заблокирован или включена экранная заставка** (Менеджер приложений)	Приложение Kaspersky Small Office Security запускает задачу тогда, когда вы закончили работу на компьютере. Таким образом, задача не будет занимать ресурсы компьютера во время работы. Флажок отображается, если выбран режим запуска **После каждого обновления**.

Настройки обновления

Настройка	Описание
Расписание обновления баз	По ссылке открывается окно **Расписание обновления баз**, в котором можно выбрать один из режимов запуска обновлений баз: **Автоматически**. Режим запуска задачи обновления, при котором приложение Kaspersky Small Office Security проверяет наличие пакета обновлений в источнике обновлений с определенной периодичностью. Частота проверки наличия пакета обновлений увеличивается во время вирусных эпидемий и сокращается при их отсутствии. Обнаружив свежий пакет обновлений, приложение Kaspersky Small Office Security скачивает его и устанавливает обновления на компьютер. **Вручную**. Этот режим запуска задачи обновления позволяет вам запускать задачу обновления вручную. **По минутам** / **По часам** / **По дням** / **Еженедельно** / **Ежемесячно** / **В указанное время** / **После запуска приложения**. Режим запуска задачи обновления, при котором приложение Kaspersky Small Office Security выполняет задачу обновления по сформированному вами расписанию. Если выбран этот режим запуска задачи обновления, вы также можете запускать задачу обновления приложения Kaspersky Small Office Security вручную.
Настроить источники обновлений	По ссылке открывается окно со списком источников обновлений. *Источник обновлений* – это HTTP- или FTP-сервер или папка общего доступа (локальная или сетевая), откуда приложение может загрузить обновления баз и модулей. По умолчанию список источников обновлений содержит серверы обновлений "Лаборатории Касперского". Вы можете добавлять в список другие источники обновлений. Если в списке выбрано несколько источников обновлений, приложение Kaspersky Small Office Security обращается к ним по очереди, пока не скачает пакет обновлений с первого доступного источника обновлений.
Запускать обновление баз с правами	По ссылке открывается окно, в котором вы можете выбрать, от имени какого пользователя запускать обновление баз. По умолчанию задача обновления приложения Kaspersky Small Office Security запускается от имени пользователя, с правами которого вы зарегистрированы в операционной системе. Однако обновление приложения Kaspersky Small Office Security может производиться из источника обновления, к которому у пользователя нет прав доступа (например, из папки общего доступа, содержащей пакет обновлений) или для которого не настроено использование аутентификации на прокси-сервере. Вы можете указать пользователя, обладающего этими правами, в параметрах приложения и запускать задачу обновления приложения Kaspersky Small Office Security от имени этого пользователя.

Окно Поиск уязвимостей в приложениях

Запустить

Кнопка, при нажатии на которую запускается поиск уязвимостей в приложениях.

Стоп

Кнопка, при нажатии на которую поиск уязвимостей в приложениях останавливается.

Кнопка отображается, если запущен поиск уязвимостей в приложениях.

N уязвимых приложений

По ссылке открывается окно **Уязвимые приложения** со списком уязвимых приложений, обнаруженных при проверке. Ссылка отображается, если был запущен поиск уязвимостей в приложениях.

Окно Приостановка защиты

Приостановить на

Режим возобновления работы компонентов защиты, при котором защита автоматически включается через указанный вами промежуток времени.

Промежуток времени вы можете указать в раскрывающемся списке ниже.

Приостановить до перезапуска приложения

Режим возобновления работы компонентов защиты, при котором защита включается после перезапуска приложения или перезагрузки операционной системы (при условии, что включен автоматический запуск приложения).

Приостановить

Режим возобновления работы компонентов защиты, при котором защита включится только тогда, когда вы сами решите возобновить ее.

Окно Проверка пароля

Пароль

Пароль, ограничивающий доступ к управлению приложением Kaspersky Small Office Security.

Запомнить пароль на эту сессию

Если флажок установлен, приложение Kaspersky Small Office Security запоминает введенный пароль и больше не запрашивает его во время текущего сеанса работы.

Окно Рекомендуемая настройка

Включить защиту от рекламных предложений, чтобы устанавливать только нужные приложения и блокировать дополнительные установки

Если флажок установлен, приложение Kaspersky Small Office Security блокирует показ рекламы во время установки на компьютер какого-либо программного обеспечения. При этом блокируется также установка предлагаемых в рекламе дополнительных приложений.

Готово

При нажатии на кнопку вы переходите в главное окно приложения.

Окно Отчеты

Для удобства работы с отчетами вы можете использовать следующие возможности:

- фильтрация по дате;
- фильтрация по значению в любой из ячеек;
- поиск по тексту записи о событии;
- сортировка списка по каждой графе отчета;
- изменение порядка и набора граф, отображаемых в отчете.

В отчетах применяются следующие уровни важности событий:

ⓘ **Информационные сообщения**. События справочного характера, как правило, не несущие важной информации.

⚠ **Предупреждения**. События, на которые нужно обратить внимание, поскольку они отражают важные ситуации в работе приложения Kaspersky Small Office Security.

⊗ **Критические события**. События критической важности, указывающие на проблемы в работе приложения Kaspersky Small Office Security или на уязвимости в защите компьютера пользователя.

По кнопке **Сохранить отчет** можно сохранить отчет в файл формата TXT или CSV.

Окно Выбор файла или папки для проверки

Объект

Поле содержит путь к файлу или папке, которые нужно добавить в список объектов, включенных в область проверки / защиты. Файл или папку можно выбрать в дереве, расположенном выше поля ввода, или указать вручную.

Окно Настройки учетной записи

Запускать обновление баз с правами

Выбор учетной записи, с правами которой приложение Kaspersky Small Office Security будет запускать задачи обновления. Функция доступна для запуска задачи обновления приложения Kaspersky Small Office Security как вручную, так и по сформированному расписанию.

Возможны следующие варианты:

- **Текущего пользователя**. Задачи обновления будут запускаться с правами текущей учетной записи, под которой вы зарегистрированы в операционной системе.
- **Другого пользователя**. Задачи обновления будут запускаться от имени указанного пользователя. При выборе этого варианта вам нужно указать имя и пароль учетной записи в полях **Учетная запись** и **Пароль**.

Область полной проверки / быстрой проверки

Список объектов

Содержит список дисков, папок и других объектов, которые приложение Kaspersky Small Office Security проверяет при выполнении выбранной задачи: полной проверки, быстрой проверки или поиска уязвимостей.

Если флажок в строке объекта установлен, то приложение Kaspersky Small Office Security проверяет объект при выполнении задачи.

Если флажок в строке объекта снят, то приложение Kaspersky Small Office Security исключает этот объект из проверки.

Добавить

При нажатии на кнопку открывается окно для выбора файла или папки, которую нужно добавить в список объектов для проверки. Выбранный объект для проверки добавляется в конец списка.

Создание и отправка отчета

Информация об операционной системе

Флажок позволяет добавить в отчет, отсылаемый на сервер Службы технической поддержки, информацию о состоянии операционной системы.

Полученные для анализа данные

Флажок позволяет добавить файлы трассировок и дампов в отчет, отсылаемый на сервер Службы технической поддержки. В этих файлах сохранена история выполнения приложением всех команд, а также информация о состоянии приложения.

По ссылке **<количество файлов>**, **<объем данных>** рядом с флажком открывается окно **Полученные для анализа данные**. В окне отображаются список файлов и суммарный объем информации, которая будет передана на сервер Службы технической поддержки.

Сохранить отчет

По ссылке открывается окно для сохранения файла отчета.

Введите номер запроса

Номер, присвоенный вашему запросу при обращении в Службу технической поддержки через сайт Центр управления Kaspersky Small Office Security.

Отправить отчет

Кнопка, при нажатии на которую выбранные файлы загружаются на FTP-сервер Службы технической поддержки.

Окно Полученные для анализа данные

Список файлов данных

Список файлов, которые приложение Kaspersky Small Office Security включает в отчет, отсылаемый на сервер Службы технической поддержки. В состав списка входят файлы трассировок и дампов. В этих файлах сохранена история выполнения приложением всех команд, а также информация о состоянии приложения.

Если флажок в строке файла установлен, то файл будет загружен на сервер Службы технической поддержки. Перед загрузкой подготовленные файлы данных будут упакованы в архив.

Если флажок в строке файла снят, то файл не будет загружен на сервер Службы технической поддержки.

Файл

Графа, в которой указывается название файла, готового для отправки на сервер Службы технической поддержки.

Размер

Объем информации, который будет передан на сервер Службы технической поддержки, если указанный файл включен в состав отчета. Приложение помещает файл в отчет, если установлен флажок в строке этого файла.

Запуск скрипта

Текст скрипта для выполнения

Текст скрипта, полученный от Службы технической поддержки.

Специалисты "Лаборатории Касперского" не рекомендуют самостоятельно вносить изменения в скрипт.

Выполнить

Кнопка, при нажатии на которую скрипт выполняется.

Выполнение скрипта AVZ

В этом окне отображается процесс выполнения скрипта AVZ. Выполнение скрипта может занять некоторое время.

Результат выполнения скрипта

Ошибка

Сообщение об ошибке. Выводится, если в скрипте AVZ были найдены ошибки. При этом работа мастера выполнения скрипта AVZ останавливается.

Готово

Кнопка, при нажатии на которую мастер выполнения скрипта AVZ завершает работу.

Результат выполнения скрипта

Закрыть

Кнопка, при нажатии на которую мастер выполнения скрипта AVZ завершает работу.

Изменить

По кнопке можно заново ввести скрипт и повторить попытку выполнения скрипта.

Окно Уязвимые приложения

Уязвимые приложения

Приложение Kaspersky Small Office Security не обнаруживает уязвимости в OpenSSL приложениях.

Содержит найденные в приложениях уязвимости.

Из-за особенностей работы службы обновлений уязвимости некоторых приложений могут быть обнаружены повторно.

Для каждой найденной уязвимости доступны следующие кнопки:

- **Подробнее**

Кнопка, при нажатии на которую открывается сайт Службы технической поддержки с описанием угрозы. На сайте вы можете скачать нужное обновление для вашей версии приложения и установить его.

- **Добавить в исключения**

Кнопка, при нажатии на которую приложение будет добавлено в доверенную зону.

Выберите zip-файл или папку

Применение альтернативных тем оформления доступно не во всех регионах.

При выборе темы оформления учитывайте следующие ограничения:

- Приложение Kaspersky Small Office Security не сможет использовать выбранную тему оформления в следующих случаях:
  - Если внутри архива файлы отличаются наименованием или имеют иное расположение в структуре папок, чем в стандартной теме.
  - Если внутри архива повреждены файлы, отвечающие за тексты на окнах приложения.
- Темы оформления предназначены для определенной версии приложения Kaspersky Small Office Security и не применимы к другим версиям и другим приложениям. При обновлении приложения до новой версии или установки поверх нее другого приложения тема оформления меняется на стандартную.

Если в результате выбора альтернативной темы оформления вы столкнулись с проблемами и не можете установить стандартную тему оформления предусмотренным для этого способом (например, не можете снять флажок **Использовать альтернативную тему оформления** в окне **Настройки интерфейса** из-за того, что шрифт сливается с фоном и нужные элементы управления неразличимы), рекомендуется переустановить приложение Kaspersky Small Office Security.

Окно Добавление / изменение исключения для аппаратной клавиатуры

Маска веб-адреса

Веб-адрес сайта, который нужно добавить в список. Вы можете указать веб-адрес или маску веб-адреса.

В блоке **Область применения** вы можете указать область, на которую распространяется действие исключения для защиты ввода данных с аппаратной клавиатуры.

Применить ко всему сайту

Защита ввода данных с аппаратной клавиатуры включена для любой страницы сайта, указанного в поле **Маска веб-адреса**.

Применить к указанной странице

Защита ввода данных с аппаратной клавиатуры включена только на веб-странице, указанной в поле **Маска веб-адреса**.

В блоке **Защита ввода с аппаратной клавиатуры** вы можете указать, будет ли приложение Kaspersky Small Office Security защищать ввод данных с аппаратной клавиатуры для выбранного сайта или веб-страницы.

Защищать

Приложение Kaspersky Small Office Security защищает ввод данных с аппаратной клавиатуры для выбранного сайта или веб-страницы.

Не защищать

Приложение Kaspersky Small Office Security не защищает ввод данных с аппаратной клавиатуры для выбранного сайта или веб-страницы.

Окно Добавление / изменение исключения для Экранной клавиатуры

Маска веб-адреса

Веб-адрес сайта, который нужно добавить в список. Вы можете указать веб-адрес или маску веб-адреса.

В блоке **Область применения** вы можете указать, к чему применяются настройки отображения значка Экранной клавиатуры: к сайту целиком или к указанной странице.

Применить ко всему сайту

Значок быстрого вызова Экранной клавиатуры отображается в полях ввода на любой странице сайта, указанного в поле **Маска веб-адреса**.

Применить к указанной странице

Значок быстрого вызова Экранной клавиатуры отображается в полях ввода только на веб-странице, указанной в поле **Маска веб-адреса**.

В блоке **Значок Экранной клавиатуры** вы можете указать, должно ли приложение показывать значок Экранной клавиатуры на страницах, соответствующих заданной маске веб-адреса.

Показывать значок в окне браузера

Приложение Kaspersky Small Office Security отображает значок быстрого вызова Экранной клавиатуры в полях ввода.

Не показывать значок в окне браузера

Приложение Kaspersky Small Office Security не отображает значок быстрого вызова Экранной клавиатуры в полях ввода.

Настройки отчетов и карантина

В блоке **Отчеты** вы можете изменить настройки формирования и хранения отчетов.

Хранить отчеты не более

Если флажок установлен, то максимальный срок хранения отчетов ограничен заданным интервалом времени. Отчеты могут храниться от одного до 10000 дней.

При достижении указанного значения приложение удаляет все записи в отчете старше, чем указанное количество дней, минус 10 %. Если вы указали значение в тридцать дней, при появлении в отчете события старше тридцати дней, из отчета удаляются все события, которые хранятся дольше 27 дней.

Если флажок снят, срок хранения отчетов не ограничен.

Ограничить размер файла отчетов до

Если флажок установлен, то максимальный размер файла отчетов ограничен заданным значением. Максимальный размер файла указывается в мегабайтах.

По умолчанию максимальный размер файла отчета составляет 4000 МБ. Удаление происходит при достижении половины от указанного размера. При этом удаляется 10 % от фактического размера файла отчета. Если указанное значение составляет 4000 МБ, то удаление более старых записей в файле отчета начнется при достижении размера файла отчета 2000 МБ, при этом размер файла отчета будет сокращен на 10 % от фактического размера за счет удаления наиболее старых записей.

Если флажок снят, то размер файла отчета не ограничен.

Очистить

При нажатии на кнопку приложение Kaspersky Small Office Security удаляет данные из папки отчетов.

По умолчанию приложение Kaspersky Small Office Security удаляет отчеты задач проверки, отчеты задачи обновления, отчеты обработки правил Сетевого экрана, отчеты Веб-Контроля.

В блоке **Карантин** вы можете изменить настройки карантина.

Хранить объекты не более

Если флажок установлен, объекты хранятся в течение срока, выбранного в раскрывающемся списке рядом с флажком. Объекты могут храниться от одного до 10000 дней.

Если флажок снят, срок хранения объектов не ограничен.

Ограничить размер карантина до

Если флажок установлен, то максимальный размер резервного хранилища ограничен заданным значением. По умолчанию максимальный размер составляет 4000 МБ. После достижения максимального размера резервного хранилища приложение Kaspersky Small Office Security автоматически удаляет наиболее старые файлы таким образом, чтобы размер резервного хранилища не превышал максимального значения.

Если флажок снят, размер хранилища не ограничен.

Настройки самозащиты

Включить самозащиту

Флажок включает / выключает механизм защиты приложения Kaspersky Small Office Security от изменения или удаления собственных файлов на диске, процессов в памяти, записей в системном реестре.

Если флажок установлен, также отключается возможность внешнего управления системной службой. Если отключено внешнее управление системной службой, приложение Kaspersky Small Office Security блокирует любую попытку удаленного управления сервисами приложений. При попытке удаленного управления появляется уведомление над значком Kaspersky Small Office Security в области уведомлений панели задач Microsoft® Windows® (если уведомления не отключены).

Разрешить управление настройками Kaspersky Small Office Security через приложения удаленного управления

Если флажок установлен, доверенные приложения удаленного администрирования (такие как TeamViewer, LogMeIn Pro и Remotely Anywhere) могут изменять настройки приложения Kaspersky Small Office Security.

Недоверенным приложениям удаленного администрирования изменение настроек приложения Kaspersky Small Office Security будет запрещено, даже если флажок установлен.

Настройки прокси-сервера

Не использовать прокси-сервер

Переключатель включает / выключает использование прокси-сервера для выхода в интернет. Приложение Kaspersky Small Office Security использует подключение к интернету в работе некоторых компонентов защиты, а также для обновления баз и модулей приложения.

Использовать настройки прокси-сервера ОС

Приложение Kaspersky Small Office Security определяет настройки прокси-сервера автоматически с помощью протокола WPAD (Web Proxy Auto-Discovery Protocol).

В случае, если по этому протоколу определить адрес не удается, Kaspersky Small Office Security использует настройки прокси-сервера, указанные в браузере Microsoft Edge на базе Chromium. Kaspersky Small Office Security не учитывает настройки прокси-серверов, указанные для других браузеров, установленных на компьютере пользователя.

Использовать указанные настройки прокси-сервера

Приложение Kaspersky Small Office Security использует прокси-сервер, отличный от заданного в настройках соединения браузера.

Адрес

Содержит IP-адрес или символьное имя (URL) прокси-сервера.

Поле доступно, если выбрана настройка **Использовать указанные настройки прокси-сервера** (например, IP-адрес 192.168.0.1).

Порт

Порт прокси-сервера.

Поле доступно, если выбрана настройка **Использовать указанные настройки прокси-сервера**.

Использовать аутентификацию на прокси-сервере

Аутентификация – это проверка регистрационных данных пользователя.

Флажок включает / выключает использование аутентификации на прокси-сервере.

Если флажок установлен, то приложение Kaspersky Small Office Security попытается выполнить NTLM-, а затем BASIC-аутентификацию.

Если флажок не установлен или настройки прокси-сервера не указаны, то приложение Kaspersky Small Office Security попытается выполнить NTLM-аутентификацию с использованием учетной записи, от имени которой запущена задача (например, задача обновления).

Если аутентификация на прокси-сервере необходима, а вы не указали имя пользователя и пароль, или указанные данные по каким-либо причинам не были приняты прокси-сервером, откроется окно запроса имени пользователя и пароля. Если аутентификация пройдет успешно, приложение Kaspersky Small Office Security будет использовать в дальнейшем указанные имя пользователя и пароль. В противном случае приложение Kaspersky Small Office Security повторно запросит настройки аутентификации.

Имя пользователя

Имя пользователя, которое используется при аутентификации на прокси-сервере.

Пароль

Пароль для введенного имени пользователя.

Не использовать прокси-сервер для локальных адресов

Если флажок установлен, приложение Kaspersky Small Office Security не использует прокси-сервер при обновлении баз и модулей приложения из локальной или сетевой папки.

Если флажок снят, приложение Kaspersky Small Office Security использует прокси-сервер при обновлении баз и модулей приложения из локальной или сетевой папки.

Раздел Защита

Список компонентов защиты

Содержит компоненты защиты, предназначенные для защиты компьютера от различных видов информационных угроз.

Каждый тип угроз обрабатывается отдельным компонентом защиты. Вы можете включать и выключать компоненты защиты независимо друг от друга, а также настраивать их работу.

Контроль камеры и микрофона

Включить / выключить Контроль камеры и микрофона

Переключатель включает / выключает компонент Контроль камеры и микрофона.

В блоке **Настройки камеры** доступны следующие параметры:

Запретить всем приложениям подключаться к камере

Если выбран этот вариант, то запрет на доступ к камере распространяется на все установленные на вашем компьютере приложения.

Запрашивать подтверждение подключаться к камере

Если выбран этот вариант, приложение Kaspersky Small Office Security выводит на экран уведомление при доступе к камере приложения, которому доступ разрешен. С помощью уведомления вы можете изменить настройки доступа приложения к камере, а также отказаться от дальнейшего отображения уведомлений.

Эта настройка недоступна, если выбран вариант действия **Запретить всем приложениям подключаться к камере**.

Разрешенные приложения

По этой ссылке открывается список приложений, имеющих доступ к камере без каких-либо уведомлений.

Запрещенные приложения

По этой ссылке открывается список приложений, для которых доступ к камере заблокирован.

В блоке **Настройки микрофона** доступны следующие параметры:

Запретить всем приложениям подключаться к микрофону

Если выбран этот вариант, то запрет на доступ к микрофону распространяется на все установленные на вашем компьютере приложения.

Запрашивать подтверждение подключаться к микрофону

Если выбран этот вариант, приложение Kaspersky Small Office Security выводит на экран уведомление при доступе к микрофону приложения, которому доступ разрешен. С помощью уведомления вы можете изменить настройки доступа приложения к микрофону, а также отказаться от дальнейшего отображения уведомлений.

Эта настройка недоступна, если выбран вариант действия **Запретить всем приложениям подключаться к микрофону**.

Разрешенные приложения

По этой ссылке открывается список приложений, имеющих доступ к микрофону без каких-либо уведомлений.

Запрещенные приложения

По этой ссылке открывается список приложений, для которых доступ к микрофону заблокирован.

Подробнее о доступе к камере и микрофону

Обнаружено подозрительное перенаправление

Удалить записи

Приложение Kaspersky Small Office Security удаляет все подозрительные записи из файла hosts.

Пропустить

Приложение Kaspersky Small Office Security не удаляет из файла hosts подозрительные записи, представленные в списке.

Список подозрительных записей

Список содержит адреса вредоносных или неизвестных веб-серверов, на которые производится перенаправление при обращении приложения к серверам "Лаборатории Касперского".

Рекомендуется удалять подозрительные записи из файла hosts.

Окно Ввод пароля

Текущий пароль

Текущий пароль, который используется для доступа к управлению приложением Kaspersky Small Office Security.

Запомнить пароль на эту сессию

Если флажок установлен, приложение Kaspersky Small Office Security запоминает введенный пароль и больше не запрашивает его во время текущего сеанса работы.

Окно Защита паролем

Ссылка **Изменить или удалить пароль** отображается, если пароль для защиты доступа к функциям приложения Kaspersky Small Office Security ранее был задан.

Изменить или удалить пароль

По ссылке отображаются поля ввода, в которых можно указать новый пароль и подтвердить его.

Новый пароль

Пароль, ограничивающий доступ к управлению приложением Kaspersky Small Office Security.

Подтверждение пароля

Повторный ввод пароля, введенного в поле **Новый пароль**.

В блоке **Область действия пароля** вы можете указать, какие функции управления приложением нужно защитить паролем.

Настройка приложения

Флажок включает / выключает запрос пароля при попытке пользователя сохранить изменения настроек приложения.

Управление Веб-Контролем

Флажок включает / выключает запрос пароля при попытке пользователя открыть окно Веб-Контроля.

Управление Резервным копированием

Флажок включает / выключает запрос пароля при попытке пользователя открыть окно **Резервное копирование**.

Завершение работы приложения

Флажок включает / выключает запрос пароля при попытке пользователя завершить работу приложения.

Удаление приложения

Флажок включает / выключает запрос пароля при попытке пользователя удалить приложение.

Настройки проверки

В таблице описаны настройки, применимые к следующим видам проверки: полная проверка, быстрая проверка, выборочная проверка, проверка из контекстного меню.

Настройка	Описание
Уровень безопасности	Для проверки приложение Kaspersky Small Office Security применяет разные наборы настроек. Наборы настроек, сохраненные в приложении, называются *уровнями безопасности*. • **Предельный**. Приложение Kaspersky Small Office Security проверяет файлы всех типов. При проверке составных файлов приложение анализирует архивы, дистрибутивы, файлы Microsoft Office и файлы в формате электронной почты, но не сканирует архивы, защищенные паролем. При установке данного уровня безопасности приложение выполняет эвристический анализ с уровнем детализации **Глубокий**. • **Оптимальный**. Приложение Kaspersky Small Office Security проверяет файлы всех типов. При проверке составных файлов приложение анализирует архивы, дистрибутивы, файлы Microsoft Office и файлы в формате электронной почты, но не сканирует архивы, защищенные паролем. При установке данного уровня безопасности приложение выполняет эвристический анализ с уровнем детализации **Средний**. • **Низкий**. Приложение Kaspersky Small Office Security проверяет файлы по формату. При проверке составных файлов приложение анализирует архивы, дистрибутивы и файлы Microsoft Office, но не сканирует защищенные паролем архивы и файлы в формате электронной почты. При установке данного уровня безопасности приложение выполняет эвристический анализ с уровнем детализации **Поверхностный**.

Действие при обнаружении угрозы	• **Спрашивать пользователя**. Если во время проверки приложение Kaspersky Small Office Security обнаруживает зараженный или возможно зараженный объект, оно сразу уведомляет вас об этом и запрашивает действие над обнаруженным объектом.
	Этот вариант доступен, если в разделе **Настройка** → **Настройки безопасности** → **Исключения и действия с найденными объектами** снят флажок **Автоматически выполнять рекомендуемые действия**.
	• **Выбирать действие автоматически**. При обнаружении зараженных или возможно зараженных объектов приложение Kaspersky Small Office Security выполняет действие, рекомендуемое специалистами "Лаборатории Касперского":
	  • Зараженный объект приложение Kaspersky сначала пытается вылечить и, если это не удается - удаляет.
	  • Возможно зараженный объект приложение Kaspersky Small Office Security удаляет, если установлен флажок **Удалять вредоносные утилиты, рекламные приложения, приложения автодозвона и подозрительные упаковщики**. Если флажок снят, приложение не удаляет возможно зараженный объект; уведомление об обнаружении такого объекта отображается в центре уведомлений (открывается по кнопке **Подробнее** в главном окне приложения).
	Этот вариант доступен, если в разделе **Настройка** → **Настройки безопасности** → **Исключения и действия с найденными объектами** установлен флажок **Автоматически выполнять рекомендуемые действия**.
	• **Лечить. Удалять, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то приложение их удаляет.
	• **Лечить. Блокировать, если лечение невозможно**. Если выбран этот вариант действия, то приложение Kaspersky Small Office Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то приложение добавляет информацию об обнаруженных зараженных файлах в список обнаруженных объектов.
	• **Информировать**. Если выбран этот вариант действия, то при обнаружении зараженных файлов приложение Kaspersky Small Office Security добавляет информацию об этих файлах в список обнаруженных объектов.
	Перед лечением или удалением зараженного файла приложение формирует его резервную копию на тот случай, если впоследствии понадобится восстановить файл или появится возможность его вылечить.

Спящий режим Windows	**Откладывать переход в спящий режим Windows до завершения проверки**. Если вы выберете эту функцию, приложение Kaspersky Small Office Security обеспечит бесперебойную работу Windows до завершения сканирования.

Настройка	Описание
Изменить область проверки (нет в настройках проверки из контекстного меню)	По ссылке открывается окно со списком объектов, которые проверяет приложение Kaspersky Small Office Security. В зависимости от типа проверки (полная проверка, быстрая проверка или выборочная проверка) в список по умолчанию включены разные объекты. Сканирование электронной почты выполняется постоянно компонентом Почтовый Антивирус. Вы можете добавить в список объекты или удалить добавленные вами объекты. Чтобы исключить объект из проверки, не обязательно удалять объект из списка, достаточно снять флажок напротив названия объекта. Вы также можете ввести путь вручную, нажав на кнопку **Добавить**. Kaspersky Small Office Security поддерживает переменные среды и символы `*` и `?` для ввода маски. • Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках. • Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает. • Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов. Вы можете использовать маски в начале, в середине или в конце пути к файлу. Например, если вы хотите добавить папку для всех пользователей в исключения, введите маску `?:\Users\*\Folder\`. Вы можете исключить сетевые папки. Для этого введите путь к сетевой папке вручную (например, `\\Network Share\*`).
Расписание проверки (нет в настройках проверки из контекстного меню)	**Вручную**. Режим запуска, при котором вы запускаете проверку вручную в удобное для вас время. **По расписанию**. Режим запуска задачи проверки, при котором приложение выполняет задачу проверки по сформированному вами расписанию. Если выбран этот режим запуска задачи проверки, вы также можете запускать задачу проверки вручную.
Запускать проверку с правами	По ссылке открывается окно, в котором вы можете выбрать, от имени какого пользователя запускать проверку. По умолчанию задача проверки запускается от имени пользователя, с правами которого вы зарегистрированы в операционной системе. Область защиты может включать сетевые диски или другие объекты, для доступа к которым нужны специальные права. Вы можете указать пользователя, обладающего этими правами, в параметрах приложения, и запускать задачу проверки от имени этого пользователя.
Типы файлов	Файлы без расширения приложение Kaspersky Small Office Security считает исполняемыми. Приложение проверяет исполняемые файлы всегда, независимо от того, файлы какого типа вы выбрали для проверки. **Все файлы**. Если выбран этот параметр, Kaspersky Small Office Security проверяет все файлы без исключения (любых форматов и расширений). **Файлы, проверяемые по формату**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы. Перед началом поиска вредоносного кода в файле выполняется анализ его внутреннего заголовка на предмет формата файла (например, TXT, DOC, EXE). В процессе проверки учитывается также расширение файла. **Файлы, проверяемые по расширению**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы. Формат файла определяется на основании его расширения.
Проверять только новые и измененные файлы	Проверка только новых файлов и тех файлов, которые изменились после предыдущей проверки. Это позволит сократить время выполнения проверки. Такой режим проверки распространяется как на простые, так и на составные файлы.
Пропускать файл, если его проверка длится более N секунд	Ограничение длительности проверки одного объекта. По истечении заданного времени приложение прекращает проверку файла. Это позволит сократить время выполнения проверки.
Проверять архивы	Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива).
Проверять дистрибутивы	Проверка сторонних дистрибутивов.

Настройка	Описание
Проверять файлы офисных форматов	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты. Приложение проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка.
Проверять файлы почтовых форматов	Флажок включает / выключает функцию, с помощью которой приложение Kaspersky Small Office Security проверяет файлы почтовых форматов, а также почтовые базы данных. Приложение полностью проверяет только файлы почтовых форматов Microsoft Outlook, Windows Mail / Microsoft Outlook Express и формата EML, и только при наличии на компьютере почтового клиента Microsoft Outlook x86. Если флажок установлен, приложение Kaspersky Small Office Security разбирает файл почтового формата и анализирует на наличие вирусов каждый его компонент (тело письма, вложения). Если флажок снят, приложение Kaspersky Small Office Security проверяет файл почтового формата как единый объект.
Проверять архивы, защищенные паролем	Если флажок установлен, приложение проверяет архивы, защищенные паролем. Перед проверкой файлов, содержащихся в архиве, на экран выводится запрос пароля. Если флажок не установлен, приложение пропускает проверку защищенных паролем архивов.
Не распаковывать составные файлы большого размера **Максимальный размер файла**	Если флажок установлен, то приложение не проверяет составные файлы, размеры которых больше заданного значения. Если флажок снят, приложение проверяет составные файлы любого размера. Приложение проверяет файлы больших размеров, извлеченные из архивов, независимо от состояния флажка.
Эвристический анализ	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.
Технология iSwift	Технология, представляющая собой развитие технологии iChecker для компьютеров с файловой системой NTFS. Технология iSwift имеет ограничение: она привязана к конкретному местоположению файла в файловой системе и применима только к объектам, расположенным в файловой системе NTFS. При обновлении версии приложения Kaspersky Small Office Security, технология iSwift включается для всех типов проверки, даже если ранее она была выключена.
Технология iChecker	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз приложения Kaspersky Small Office Security, дату предыдущей проверки файла, а также изменение настроек проверки. Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной приложению структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

Настройки проверки внешних дисков

Настройка	Описание
Действие при подключении внешнего диска	• **Быстрая проверка**. Если выбран этот вариант, то после подключения внешнего устройства Kaspersky Small Office Security проверяет только файлы определенных форматов, наиболее подверженные заражению, находящиеся в корневой папке подключенного устройства. Также при быстрой проверке приложение не распаковывает и не проверяет архивы. • **Подробная проверка**. Если выбран этот вариант, то после подключения внешнего устройства приложение Kaspersky Small Office Security проверяет все файлы, расположенные во всех папках внешнего устройства, а также распаковывает и проверяет архивы, кроме защищенных паролем.
Максимальный размер внешнего диска	Если флажок установлен, то Kaspersky Small Office Security проверяет внешние устройства, размер которых не превышает указанный максимальный размер. Если флажок снят, то Kaspersky Small Office Security проверяет внешние устройства любого размера.
Отображать ход проверки	Если флажок установлен, то Kaspersky Small Office Security отображает ход проверки внешних устройств в отдельном окне, а также в окне запуска проверки.
Запретить остановку задачи проверки	Если флажок установлен, то для задачи проверки внешних устройств недоступна кнопка **Стоп** в окне запуска проверки.

Настройки фоновой проверки

Если фоновая проверка включена, приложение Kaspersky Small Office Security выполняет фоновую проверку. Фоновая проверка – это автоматический режим проверки без показа уведомлений. Такая проверка требует меньше ресурсов компьютера, чем другие виды проверок (например, полная проверка). В этом режиме приложение Kaspersky Small Office Security проверяет системную память, системные разделы, загрузочные секторы и объекты автозапуска, а также выполняет поиск руткитов.

Если компьютер работает от аккумулятора, приложение Kaspersky Small Office Security не выполняет фоновую проверку компьютера.

Настройки поиска уязвимостей в приложениях

Настройка	Описание
Изменить область поиска	По ссылке открывается окно **Область поиска уязвимостей** со списком объектов, которые проверяются при поиске уязвимостей в приложениях. Вы можете добавить в список объекты или удалить добавленные вами объекты. Чтобы исключить объект из проверки, не обязательно удалять объект из списка, достаточно снять флажок напротив названия объекта.
Расписание поиска	**Вручную**. Режим запуска, при котором вы запускаете поиск уязвимостей в приложениях вручную в удобное для вас время. **По расписанию**. Режим запуска задачи проверки, при котором приложение выполняет задачу проверки по сформированному вами расписанию. Если выбран этот режим запуска задачи проверки, вы также можете запускать задачу проверки вручную.

Настройки учетной записи

Запускать проверку с правами

Выбор учетной записи, с правами которой приложение Kaspersky Small Office Security будет запускать задачи проверки. Функция доступна для запуска проверки как вручную, так и по расписанию.

Возможны следующие варианты:

- **Текущего пользователя**. Задачи проверки будут запускаться с правами текущей учетной записи.
- **Другого пользователя**. Задачи проверки будут запускаться от имени указанного пользователя. При выборе этого варианта нужно указать имя и пароль учетной записи в полях **Учетная запись** и **Пароль**.

Настройки Анти-Баннера

Включить / выключить Анти-Баннер

Переключатель включает / выключает использование Анти-Баннера.

Если переключатель включен, Анти-Баннер блокирует отображение баннеров на просматриваемых вами сайтах и в интерфейсе некоторых приложений. По умолчанию Анти-Баннер блокирует на сайтах баннеры из списка известных баннеров. Список входит в состав баз приложения Kaspersky Small Office Security.

Список фильтров

По ссылке открывается окно **Список фильтров**, в котором вы можете с помощью специальных фильтров детально указать, какие именно баннеры нужно блокировать.

Сайты с разрешенными баннерами

По ссылке открывается окно со списком сайтов, на которых вы разрешили отображение баннеров.

Запрещенные баннеры

По ссылке открывается окно **Запрещенные баннеры**. В этом окне вы можете сформировать список баннеров, запрещенных для отображения.

Разрешенные баннеры

По ссылке открывается окно **Разрешенные баннеры**. В этом окне вы можете сформировать список баннеров, разрешенных для отображения.

Разрешить баннеры на сайтах "Лаборатории Касперского"

Если флажок установлен, Анти-Баннер не блокирует баннеры на сайтах "Лаборатории Касперского" и сайтах партнеров компании, на которых размещена реклама "Лаборатории Касперского". Список этих сайтов доступен по ссылке **Сайты "Лаборатории Касперского"**.

Сайты "Лаборатории Касперского"

По ссылке открывается окно со списком сайтов "Лаборатории Касперского".

Ссылка доступна, если установлен флажок **Разрешить баннеры на сайтах "Лаборатории Касперского"**.

Окно Добавление / изменение баннера

Маска веб-адреса (URL)

IP-адрес, веб-адрес (URL) или маска веб-адреса.

При вводе маски веб-адреса можно использовать символы `*` и `?`, где `*` – любая последовательность символов, а `?` – любой один символ.

Статус

В блоке **Статус** вы можете указать, должен ли Анти-Баннер использовать этот адрес при проверке баннеров.

Возможны следующие варианты:

- **Активно**. Анти-Баннер использует этот адрес при проверке баннеров.
- **Неактивно**. Анти-Баннер не использует этот адрес при проверке баннеров.

Окно Добавление / изменение сайта

Сайт

Веб-адрес (URL) сайта.

Статус

В блоке **Статус** вы можете указать, должен ли Анти-Баннер разрешать отображение баннеров на указанном сайте.

Возможны следующие варианты:

- **Активно**. Анти-Баннер разрешает отображение баннеров на указанном сайте.
- **Неактивно**. Анти-Баннер не разрешает отображение баннеров на указанном сайте.

Окно Запрещенные баннеры

Кнопка

При нажатии на кнопку открывается меню со следующими пунктами:

- **Импортировать и добавить к существующим**. При выборе этого пункта открывается окно, позволяющее загрузить список запрещенных адресов из файла формата CSV. Текущие адреса не удаляются.
- **Импортировать и заменить существующие**. При выборе этого пункта открывается окно, позволяющее загрузить список запрещенных адресов из файла формата CSV. Текущие адреса удаляются.
- **Экспортировать**. При выборе этого пункта открывается окно, позволяющее сохранить список запрещенных адресов в файле формата CSV.

Список запрещенных баннеров

Содержит адреса или маски адресов запрещенных баннеров. Анти-Баннер блокирует баннер, если его адрес есть в списке запрещенных баннеров.

Вы можете добавить в список адрес или маску адреса.

Если в графе **Статус** в строке адреса установлено значение *Активно*, Анти-Баннер использует этот адрес при проверке баннеров.

Если в графе **Статус** в строке адреса установлено значение *Неактивно*, Анти-Баннер не использует этот адрес при проверке баннеров.

Маска веб-адреса (URL)

Графа, в которой указан адрес или маска адреса запрещенного баннера.

Статус

Графа, в которой указано, использует ли Анти-Баннер этот адрес при проверке баннеров.

Если в строке адреса установлено значение *Активно*, Анти-Баннер использует этот адрес при проверке баннеров.

Если в строке адреса установлено значение *Неактивно*, Анти-Баннер не использует этот адрес при проверке баннеров.

Изменить

Кнопка, при нажатии на которую открывается окно для изменения адреса или маски адреса баннера в списке запрещенных баннеров.

Удалить

Кнопка, при нажатии на которую Анти-Баннер удаляет выбранный адрес баннера или маску адреса из списка.

Добавить

Кнопка, при нажатии на которую открывается окно для добавления адреса или маски адреса баннера в список запрещенных баннеров.

Окно Разрешенные баннеры

Кнопка

При нажатии на кнопку открывается меню со следующими пунктами:

- **Импортировать и добавить к существующим**. При выборе этого пункта можно загрузить список разрешенных адресов из файла формата CSV. Текущие адреса не удаляются.
- **Импортировать и заменить существующие**. При выборе этого пункта можно загрузить список разрешенных адресов из файла формата CSV. Текущие адреса удаляются.
- **Экспортировать**. При выборе этого пункта можно сохранить список адресов в файле формата CSV. Вы можете экспортировать как весь список адресов, так и адреса, выбранные из списка.

Список разрешенных баннеров

Содержит адреса или маски адресов разрешенных баннеров. Анти-Баннер не блокирует баннер, если его адрес есть в списке разрешенных баннеров.

Вы можете добавить в список адрес или маску адреса.

Если в графе **Статус** в строке адреса установлено значение *Активно*, Анти-Баннер использует этот адрес при проверке баннеров.

Если в графе **Статус** в строке адреса установлено значение *Неактивно*, Анти-Баннер не использует этот адрес при проверке баннеров.

Маска веб-адреса (URL)

Графа, в которой указана адрес или маска адреса разрешенного баннера.

Статус

Графа, в которой указано, использует ли Анти-Баннер этот адрес при проверке баннеров.

Если в строке адреса установлено значение *Активно*, Анти-Баннер использует этот адрес при проверке баннеров.

Если в строке адреса установлено значение *Неактивно*, Анти-Баннер не использует этот адрес при проверке баннеров.

Изменить

Кнопка, при нажатии на которую открывается окно для изменения адреса или маски адреса баннера в списке разрешенных баннеров.

Удалить

Кнопка, при нажатии на которую Анти-Баннер удаляет выбранный адрес или маску адреса баннера из списка разрешенных баннеров.

Добавить

Кнопка, при нажатии на которую открывается окно для добавления адреса или маски адреса баннера в список разрешенных баннеров.

Окно Сайты с разрешенными баннерами

Кнопка

При нажатии на кнопку открывается меню со следующими пунктами:

- **Импортировать и добавить к существующим**. При выборе этого пункта можно загрузить список разрешенных адресов из файла формата CSV. Текущие адреса не удаляются.
- **Импортировать и заменить существующие**. При выборе этого пункта можно загрузить список разрешенных адресов из файла формата CSV. Текущие адреса удаляются.
- **Экспортировать**. При выборе этого пункта можно сохранить список адресов в файле формата CSV. Вы можете экспортировать как весь список адресов, так и адреса, выбранные из списка.

Список сайтов с разрешенными баннерами

Содержит адреса сайтов, на которых вы разрешили отображение баннеров. Анти-Баннер не блокирует баннеры на сайте, если его адрес есть в списке.

Если в графе **Статус** в строке адреса установлено значение *Активно*, Анти-Баннер разрешает отображение баннеров на этом сайте.

Если в графе **Статус** в строке адреса установлено значение *Неактивно*, Анти-Баннер блокирует баннеры на этом сайте.

Изменить

Кнопка, при нажатии на которую открывается окно для изменения адреса, выбранного в списке.

Удалить

Кнопка, при нажатии на которую Анти-Баннер удаляет выбранный адрес сайта из списка.

Добавить

Кнопка, при нажатии на которую открывается окно для добавления адреса сайта в список.

Окно Сайты "Лаборатории Касперского"

В окне представлен список сайтов "Лаборатории Касперского" и сайты партнеров компании, на которых размещена реклама "Лаборатории Касперского".

Список составляют и обновляют специалисты "Лаборатории Касперского". Список обновляется автоматически при обновлении баз и модулей приложения.

Настройки Безопасных платежей

Включить / выключить Безопасные платежи

Переключатель включает / выключает Безопасные платежи.

Если переключатель включен, приложение отслеживает все обращения к веб-сайтам банков или платежных систем и выполняет действие, заданное по умолчанию или настроенное пользователем. По умолчанию в режиме Безопасных платежей приложение запрашивает подтверждение пользователя на запуск защищенного режима браузера.

Если переключатель выключен, приложение разрешает обращение к веб-сайтам банков или платежных систем с использованием обычного браузера.

Узнать больше

По ссылке открывается окно браузера на странице с более подробной информацией о компоненте.

В блоке **При первом обращении к сайтам банков или платежных систем** вы можете выбрать действие, которое приложение выполняет при первом обращении к сайтам банков и платежных систем.

Открывать в защищенном режиме браузера

Если приложение обнаруживает попытку доступа к указанному сайту, то открывает этот сайт в защищенном режиме браузера. В обычном браузере, использованном для обращения к сайту, отображается сообщение о запуске защищенного режима браузера.

Спрашивать пользователя

Если приложение обнаруживает попытку доступа к указанному сайту, то предлагает запустить защищенный режим браузера либо открыть сайт при помощи обычного браузера.

Не открывать в защищенном режиме браузера

Когда вы обращаетесь к указанному сайту, приложение не использует защищенный режим браузера. Сайт открывается в обычном браузере.

Блок **Дополнительно** позволяет настроить дополнительные настройки работы Безопасных платежей.

Для перехода к сайтам из окна Безопасных платежей использовать

В раскрывающемся списке можно выбрать браузер, в котором приложение будет открывать сайты банков или платежных систем, выбранные из окна Безопасные платежи.

Безопасные платежи доступны при работе со следующими браузерами: Microsoft Internet Explorer, Microsoft Edge на базе Chromium, Mozilla Firefox, Google Chrome, Яндекс.Браузер и Opera на базе Chromium.

По умолчанию Безопасные платежи используют браузер, установленный в операционной системе в качестве браузера по умолчанию.

Уведомлять об уязвимостях в операционной системе

Флажок включает / выключает отображение уведомлений об опасности обращения к сайту банка или платежной системы из-за наличия уязвимости в операционной системе.

Если флажок установлен и автоматическое обновление операционной системы включено, приложение Kaspersky Small Office Security предлагает скачать соответствующее обновление с сайта производителя операционной системы. Если автоматическое обновление операционной системы отключено, приложение Kaspersky Small Office Security предлагает включить его.

Создать ярлык для Безопасных платежей

По ссылке на рабочем столе создается ярлык для запуска Безопасных платежей. Ярлык позволяет открыть окно со списком сайтов банков или платежных систем, при обращении к которым используется защищенный режим браузера.

В 64-разрядной версии Windows 8, Windows 8.1 и Windows 10 для защиты браузера используется аппаратная виртуализация.

Настройки Интернет-защиты

Настройка	Описание
Уровень безопасности	Для работы Интернет-защиты приложение применяет разные наборы настроек. Наборы настроек, сохраненные в приложении, называются *уровнями безопасности*. • **Предельный**. Уровень безопасности веб-трафика, при котором компонент Интернет-защита максимально проверяет веб-трафик, поступающий на компьютер по HTTP- и FTP-протоколам. Интернет-защита детально проверяет все объекты веб-трафика, используя полный набор баз приложения, а также выполняет максимально глубокий эвристический анализ. • **Оптимальный**. Уровень безопасности веб-трафика, обеспечивающий оптимальный баланс между производительностью приложения и безопасностью веб-трафика. Компонент Интернет-защита выполняет эвристический анализ на среднем уровне. Этот уровень безопасности веб-трафика рекомендован для использования специалистами "Лаборатории Касперского". • **Низкий**. Уровень безопасности веб-трафика, параметры которого обеспечивают максимальную скорость проверки веб-трафика. Компонент Интернет-защита выполняет эвристический анализ на поверхностном уровне.
Действие при обнаружении угрозы	• **Выполнять действие автоматически**. Интернет-защита выбирает действие автоматически на основе установленных настроек. Если веб-ресурс находится в списке исключений или не содержит зараженных или возможно зараженных объектов, то Интернет-защита разрешает доступ к нему. Если в результате проверки Интернет-защита обнаруживает, что веб-ресурс содержит зараженный или возможно зараженный объект, он блокирует доступ к веб-ресурсу. Этот вариант доступен, если в разделе **Настройка → Настройки безопасности → Исключения и действия с найденными объектами** установлен флажок **Автоматически выполнять рекомендуемые действия**. • **Блокировать**. Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта компонент Интернет-защита блокирует доступ к объекту и показывает сообщение в браузере. • **Информировать**. Интернет-защита информирует вас об обнаружении зараженного или возможно зараженного объекта и запрашивает дальнейшее действие над ним. Этот вариант доступен, если в разделе **Настройка → Настройки безопасности → Исключения и действия с найденными объектами** снят флажок **Автоматически выполнять рекомендуемые действия**.
Методы проверки **Проверять веб-адрес по базе вредоносных веб-адресов**	Проверка ссылок на принадлежность к базе вредоносных веб-адресов позволяет отследить веб-сайты, которые находятся в списке запрещенных веб-адресов. База вредоносных веб-адресов формируется специалистами "Лаборатории Касперского", входит в комплект поставки приложения и пополняется при обновлении баз приложения Kaspersky Small Office Security.
Проверять веб-адрес по базе веб-адресов, на которых находятся рекламные приложения	Например, приложение, которое в процессе вашей работы с интернетом перенаправляет поисковый запрос на рекламный сайт. Таким образом, вы попадаете не на тот интернет-ресурс, который наилучшим образом соответствует вашему запросу, а на рекламный сайт.
Проверять веб-адрес по базе веб-адресов, на которых находятся легальные приложения, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или вашим данным	Например, приложение удаленного администрирования, которое легально используют системные администраторы для диагностики и устранения неполадок. Злоумышленник может без вашего ведома установить такое приложение на ваш компьютер, получить к нему доступ и использовать в своих целях. Приложение Kaspersky Small Office Security разрешает скачивание таких приложений по ссылкам на веб-страницах. Исключение составляют одноразовые ссылки. По ним невозможно скачать легальные приложения, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или вашим данным.
Использовать эвристический анализ	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса. Во время проверки веб-трафика на наличие вирусов и других приложений, представляющих угрозу эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.

Настройка	Описание
Анти-Фишинг **Проверять веб-адрес по базе фишинговых веб-адресов и поддельных криптовалютных бирж** (или **Проверять веб-адрес по базе фишинговых веб-адресов**)	В состав базы фишинговых веб-адресов и поддельных криптовалютных бирж включены веб-адреса известных на настоящее время веб-сайтов, которые используются для фишинг-атак. Специалисты "Лаборатории Касперского" пополняют базу веб-адресами, предоставленными международной организацией по борьбе с фишингом The Anti-Phishing Working Group. База фишинговых веб-адресов и поддельных криптовалютных бирж входит в комплект поставки приложения и пополняется при обновлении баз приложения Kaspersky Small Office Security.
Использовать эвристический анализ	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет обнаружить фишинг, даже если веб-адрес отсутствует в базе фишинговых веб-адресов.
Проверка сайтов на мошенничество	Если установлен флажок **Проверять сайты по базе подозрительных веб-ресурсов**, приложение Kaspersky Small Office Security будет проверять веб-сайты по базам данных подозрительных веб-ресурсов, которые могут использоваться мошенниками для обмана пользователей. В их числе сайты финансовых пирамид, ломбардов и онлайн-магазинов, которые продают подделки или контрафакт. Более подробную информацию смотрите в этой статье.
Проверять ссылки	Компонент Проверка ссылок проверяет ссылки на веб-странице открытой в любом из поддерживаемых браузеров. Рядом с проверенной ссылкой приложение Kaspersky Small Office Security отображает один из следующих значков:  – если веб-страница, которая открывается по ссылке, безопасна по данным "Лаборатории Касперского";  – если нет информации о безопасности веб-страницы, которая открывается по ссылке;  – если веб-страница, которая открывается по ссылке, по данным "Лаборатории Касперского" может быть использована злоумышленниками для нанесения вреда компьютеру или вашим данным;  – если веб-страница, которая открывается по ссылке, по данным "Лаборатории Касперского" может быть заражена или взломана;  – если веб-страница, которая открывается по ссылке, опасна по данным "Лаборатории Касперского". При наведении курсора мыши на значок отображается всплывающее окно с более подробным описанием ссылки.
На всех сайтах, кроме указанных **Настроить исключения**	При выборе этого варианта приложение проверяет ссылки на всех сайтах, кроме указанных в окне **Исключения**. Окно **Исключения** открывается по ссылке **Настроить исключения**.
Только на указанных сайтах **Настроить проверяемые сайты**	При выборе этого варианта Kaspersky Small Office Security проверяет ссылки только на тех сайтах, которые указаны в окне **Проверяемые сайты**. Окно **Проверяемые сайты** открывается по ссылке **Настроить проверяемые сайты**.
Настроить проверку ссылок	• **Любые ссылки**. Приложение проверяет ссылки на всех типах веб-страниц. • **Только ссылки в результатах поиска**. Приложение проверяет ссылки на веб-страницах с результатами поиска при использовании поисковых систем.
Категории сайтов	Если установлен флажок **Отображать информацию о категориях содержимого сайтов**, приложение добавляет в комментарий к ссылке сведения о том, не принадлежит ли сайт к одной из указанных категорий (например, **Насилие, разжигание вражды** или **Для взрослых**). Вы можете снять флажки напротив категорий, о которых предупреждать не нужно.
Не проверять веб-трафик с доверенных веб-адресов	Если флажок установлен, компонент Интернет-защита не проверяет содержимое веб-страниц / веб-сайтов, адреса которых включены в список доверенных веб-адресов. Вы можете добавить в список доверенных веб-адресов как конкретный адрес веб-страницы / веб-сайта, так и маску адреса веб-страницы / веб-сайта. Список доверенных веб-адресов доступен в окне **Доверенные веб-адреса**, открывающемся по ссылке **доверенных веб-адресов**.

Окно Сайты "Лаборатории Касперского" и ее партнеров

В окне представлен список сайтов "Лаборатории Касперского" и ее партнеров.

Список составляют и обновляют специалисты "Лаборатории Касперского". Список обновляется автоматически при обновлении баз и модулей приложения.

Настройки Защиты от сетевых атак

Компонент Защита от сетевых атак (также Intrusion Detection System (IDS) - система обнаружения вторжений) отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на компьютер пользователя, приложение Kaspersky Small Office Security блокирует сетевое соединение с атакующим компьютером. Описания известных в настоящее время видов сетевых атак и методов борьбы с ними содержатся в базах приложения Kaspersky Small Office Security. Список сетевых атак, которые обнаруживает компонент Защита от сетевых атак, пополняется в процессе обновления баз и модулей приложения.

Настройки компонента Защита от сетевых атак

Настройка	Описание
Считать атаками сканирование портов и интенсивные сетевые запросы	*Атака типа Интенсивные сетевые запросы (англ. Network Flooding)* – атака на сетевые ресурсы организации (например, веб-серверы). Атака заключается в отправке большого количества запросов для превышения пропускной способности сетевых ресурсов. Таким образом пользователи не могут получить доступ к сетевым ресурсам организации. *Атака типа Сканирование портов* заключается в сканировании UDP- и TCP-портов, а также сетевых служб на компьютере. Атака позволяет определить степень уязвимости компьютера перед более опасными видами сетевых атак. Сканирование портов также позволяет злоумышленнику определить операционную систему на компьютере и выбрать подходящие для нее сетевые атаки. Если переключатель включен, компонент Защита от сетевых атак блокирует сканирование портов и интенсивные сетевые запросы.
Блокировать атакующие компьютеры на N мин	Если функция включена, компонент Защита от сетевых атак добавляет атакующий компьютер в список блокирования. Это означает, что компонент Защита от сетевых атак блокирует сетевое соединение с атакующим компьютером после первой попытки сетевой атаки в течение заданного времени, чтобы автоматически защитить компьютер пользователя от возможных будущих сетевых атак с этого адреса. Минимальное время, на которое атакующий компьютер можно добавить в список блокирования, составляет одну минуту. Максимальное – 999 минут.
Настроить исключения	Список содержит IP-адреса, сетевые атаки с которых компонент Защита от сетевых атак не блокирует. Вы можете добавить IP-адрес с указанием используемого порта и протокола. Приложение не заносит в отчет информацию о сетевых атаках с IP-адресов, входящих в список исключений.

Настройки Предотвращения вторжений

Включить / выключить Предотвращение вторжений

Переключатель включает / выключает Предотвращение вторжений.

Узнать больше

По ссылке открывается окно браузера на странице с более подробной информацией о компоненте.

Управление приложениями

По ссылке открывается окно **Управление приложениями**. В нем вы можете отредактировать список правил для приложений.

Управление ресурсами

По ссылке открывается окно **Управление ресурсами**. В нем вы можете сформировать список персональных данных, а также список настроек и ресурсов операционной системы, доступ к которым контролирует Предотвращение вторжений.

Группа доверия для приложений, не включенных в другие группы

По ссылке открывается окно **Группа доверия для приложений, не включенных в другие группы**. В окне можно выбрать группу доверия, в которую будут помещаться неизвестные приложения.

Можно выбрать один из следующих вариантов:

- Доверенные;
- Слабые ограничения;
- Сильные ограничения;
- Недоверенные.

Группа доверия для приложений, запущенных до Kaspersky Small Office Security

По ссылке открывается окно **Группа доверия для приложений, запущенных до Kaspersky Small Office Security**. В окне можно изменить группу доверия для приложений, запущенных до начала работы приложения Kaspersky Small Office Security. Сетевая активность приложений, запущенных до начала работы приложения Kaspersky Small Office Security, будет контролироваться в соответствии с правилами выбранной вами группы доверия.

По умолчанию приложений, запущенные до начала работы приложения Kaspersky Small Office Security, помещаются в одну из групп доверия на основании правил, заданных специалистами "Лаборатории Касперского".

Доверять приложениям, имеющим цифровую подпись

Если флажок установлен, Предотвращение вторжений считает доверенными приложения, имеющие цифровую подпись. Предотвращение вторжений помещает такие приложения в группу **Доверенные** и не проверяет их активность.

Если флажок снят, Предотвращение вторжений не считает приложения с обычной цифровой подписью доверенными и проверяет их активность. Приложения доверенных поставщиков программного обеспечения (например, Microsoft) Предотвращение вторжений считает доверенными независимо от того, установлен флажок или снят.

Загружать правила для приложений из Kaspersky Security Network (KSN)

Если флажок установлен, для определения группы доверия приложения Предотвращение вторжений отправляет запрос в базу Kaspersky Security Network.

Если флажок снят, Предотвращение вторжений не ищет информацию в базе Kaspersky Security Network для определения группы доверия, к которой относится приложение.

Окно Веб-маяки

В окне представлен список веб-маяков.

Список составляют и обновляют специалисты "Лаборатории Касперского". Список обновляется автоматически при обновлении баз и модулей приложения.

Защита от сбора данных в интернете. Категории и исключения

Сервисы веб-аналитики

Если флажок установлен, компонент Защита от сбора данных в интернете блокирует сервисы веб-аналитики, использующие сбор данных с целью анализа ваших действий в интернете.

По ссылке **Показать список** открывается окно со списком сервисов веб-аналитики, использующих сбор данных с целью анализа ваших действий в интернете.

Рекламные агентства

Если флажок установлен, компонент Защита от сбора данных в интернете блокирует сбор данных о ваших действиях в интернете, который выполняют рекламные агентства в рекламных целях.

По ссылке **Показать список** открывается окно со списком рекламных агентств, выполняющих сбор данных о ваших действиях в интернете в рекламных целях.

Веб-маяки

Если флажок установлен, компонент Защита от сбора данных в интернете блокирует сбор данных о ваших действиях в интернете, выполняемый веб-маяками. Веб-маяки представляют собой невидимые пользователю объекты, внедренные в веб-страницу.

По ссылке **Показать список** открывается окно со списком веб-маяков.

Социальные сети

Если флажок установлен, компонент Защита от сбора данных в интернете блокирует сбор данных при посещении вами социальных сетей, кроме сбора данных, выполняемого самими социальными сетями. Блокирование сбора данных не мешает вам использовать функции "Мне нравится", "+1" и подобные им.

Флажки с названиями социальных сетей позволяют указать социальные сети, на сайтах которых приложение должно блокировать сбор данных.

Исключения

По ссылке открывается окно, где вы можете указать сайты, на которых разрешаете сбор данных о ваших действиях.

Окно Несовместимые сайты

В окне представлен список сайтов, о которых специалистам "Лаборатории Касперского" известно, что их работоспособность может быть нарушена в результате запрета на сбор данных.

Список составляют и обновляют специалисты "Лаборатории Касперского". Список обновляется автоматически при обновлении баз и модулей приложения.

Окно Настройки Защиты от сбора данных в интернете

Включить / выключить Защиту от сбора данных в интернете

Если переключатель включен, то, когда вы находитесь в интернете, компонент Защита от сбора данных в интернете обнаруживает попытки сбора данных сервисами отслеживания. Сервисы отслеживания используют полученную информацию для анализа ваших действий и могут применять результаты анализа, например, для показа вам соответствующей рекламной информации.

Только собирать статистику

При выборе этого варианта компонент Защита от сбора данных в интернете работает в *режиме обнаружения*, предоставляя вам возможность просмотреть отчеты об обнаруженных попытках сбора данных.

Запретить сбор данных

При выборе этого варианта компонент Защита от сбора данных в интернете работает в *режиме блокировки*, обнаруживая и блокируя попытки сбора данных. Информация о попытках сбора данных записывается в отчет.

Категории и исключения

По ссылке открывается окно, где можно указать категории сервисов отслеживания, которым вы хотите запретить или разрешить сбор данных. Из этого окна можно перейти к формированию списка сайтов, на которых вы хотите разрешить сбор данных.

Отправлять запрет на сбор данных

Если флажок установлен, то в режиме блокировки при обращении к сайту браузер отправляет на сайт HTTP-заголовок Do not track, означающий запрет на сбор данных о ваших действиях.

Разрешить сбор данных на сайтах "Лаборатории Касперского" и ее партнеров

Если флажок установлен, приложение Kaspersky Small Office Security разрешает сбор данных на сайтах "Лаборатории Касперского" и ее партнеров.

Сайты "Лаборатории Касперского" и ее партнеров

По ссылке открывается окно со списком сайтов "Лаборатории Касперского" и ее партнеров.

Разрешить сбор данных на несовместимых сайтах

Если флажок установлен, приложение Kaspersky Small Office Security разрешает сбор данных на сайтах, работоспособность которых может быть нарушена в результате запрета на сбор данных.

Несовместимые сайты

По ссылке открывается окно со списком сайтов, работоспособность которых может быть нарушена в результате запрета на сбор данных.

Окно Рекламные агентства

В окне представлен список рекламных агентств, выполняющих сбор данных о ваших действиях в интернете в рекламных целях.

Список составляют и обновляют специалисты "Лаборатории Касперского". Список обновляется автоматически при обновлении баз и модулей приложения.

Окно Сервисы веб-аналитики

В окне представлен список сервисов веб-аналитики, использующих сбор данных с целью анализа ваших действий в интернете.

Список составляют и обновляют специалисты "Лаборатории Касперского". Список обновляется автоматически при обновлении баз и модулей приложения.

Настройки Почтового Антивируса

Настройка	Описание
Уровень безопасности	Для работы Почтового Антивируса приложение применяет разные наборы настроек. Наборы настроек, сохраненные в приложении, называются *уровнями безопасности*. • **Предельный**. Уровень безопасности почты, при котором компонент Почтовый Антивирус максимально контролирует сообщения. Компонент Почтовый Антивирус проверяет входящие и исходящие сообщения электронной почты, а также выполняет глубокий эвристический анализ. Высокий уровень безопасности почты рекомендуется применять для работы в опасной среде. Примером опасной среды может служить подключение к одному из бесплатных почтовых сервисов из домашней сети, не обеспечивающей централизованной защиты почты. • **Оптимальный**. Уровень безопасности почты, обеспечивающий оптимальный баланс между производительностью приложения и безопасностью почты. Компонент Почтовый Антивирус проверяет входящие и исходящие сообщения электронной почты, а также выполняет эвристический анализ среднего уровня. Этот уровень безопасности почты рекомендован для использования специалистами "Лаборатории Касперского". • **Низкий**. Уровень безопасности почты, при котором компонент Почтовый Антивирус проверяет только входящие сообщения электронной почты, а также выполняет их поверхностный эвристический анализ. Почтовый Антивирус не проверяет архивы, вложенные в сообщения. Если используется этот уровень безопасности почты, компонент Почтовый Антивирус проверяет сообщения электронной почты максимально быстро и затрачивает минимум ресурсов операционной системы. Низкий уровень безопасности почты рекомендуется применять для работы в хорошо защищенной среде. Примером такой среды может служить локальная сеть организации с централизованным обеспечением безопасности почты.
Действие при обнаружении угрозы	• **Спрашивать пользователя**. Почтовый Антивирус сообщает вам об обнаружении зараженного или возможно зараженного объекта и запрашивает дальнейшее действие над ним. Этот вариант доступен, если в разделе **Настройка → Настройки безопасности → Исключения и действия с найденными объектами** снят флажок **Автоматически выполнять рекомендуемые действия**. • **Выбирать действие автоматически**. При обнаружении зараженных или возможно зараженных объектов Почтовый Антивирус автоматически выполняет действие, рекомендуемое специалистами "Лаборатории Касперского". Для зараженных объектов таким действием будет Лечить. Это значение выбрано по умолчанию. Перед лечением или удалением зараженного объекта Почтовый Антивирус создает его резервную копию на тот случай, если впоследствии понадобится восстановить объект или появится возможность его вылечить. Этот вариант доступен, если в разделе **Настройка → Настройки безопасности → Исключения и действия с найденными объектами** установлен флажок **Автоматически выполнять рекомендуемые действия**. • **Лечить. Удалять, если лечение невозможно**. При обнаружении зараженного объекта во входящем или исходящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение удаляет зараженный объект. Приложение добавит информацию о выполненном действии в тему сообщения, например: *[Сообщение было обработано] <тема сообщения>*. • **Лечить. Блокировать, если лечение невозможно**. При обнаружении зараженного объекта во входящем сообщении приложение Kaspersky Small Office Security пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение Kaspersky Small Office Security пытается вылечить обнаруженный объект. Если вылечить объект не удалось, приложение Kaspersky Small Office Security блокирует отправку сообщения, почтовый клиент показывает ошибку. • **Блокировать**. При обнаружении зараженного объекта во входящем сообщении приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение Kaspersky Small Office Security блокирует отправку сообщения, почтовый клиент показывает ошибку.
Область защиты	*Область защиты* – это объекты, которые проверяет компонент во время своей работы: входящие и исходящие сообщения или только входящие сообщения. Для защиты компьютеров достаточно проверять только входящие сообщения. Вы можете включить проверку исходящих сообщений для предотвращения отправки зараженных файлов в архивах. Вы также можете включить проверку исходящих сообщений, если вы хотите запретить обмен файлами определенных форматов, например, аудио или видео.
Проверять трафик POP3, SMTP, NNTP, IMAP	Флажок включает / выключает проверку компонентом Почтовый Антивирус почтового трафика, проходящего по протоколам POP3, SMTP, NNTP и IMAP.

Настройка	Описание
Подключить расширение для Microsoft Outlook (недоступно на файловом сервере)	Если флажок установлен, включена проверка сообщений электронной почты, передающихся по протоколам POP3, SMTP, NNTP, IMAP на стороне расширения, интегрированного в Microsoft Outlook. В случае проверки почты с помощью расширения для Microsoft Outlook рекомендуется использовать режим кеширования Exchange (Cached Exchange Mode). Более подробную информацию о режиме кеширования Exchange и рекомендации по его использованию вы можете найти в базе знаний Microsoft.
Проверять веб-почтовые клиенты	Если флажок установлен, приложение проверяет вложения электронной почты, доступ к которым осуществляется через веб-почтовые клиенты.
Эвристический анализ	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.
Проверять вложенные файлы форматов Microsoft Office	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты. Приложение проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка.
Проверять вложенные архивы	Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива).
Не проверять архивы размером более	Если флажок установлен, компонент Почтовый Антивирус исключает из проверки вложенные в сообщения электронной почты архивы, размер которых больше заданного. Если флажок снят, компонент Почтовый Антивирус проверяет архивы любого размера, вложенные в сообщения электронной почты.
Ограничить время проверки архива до	Если флажок установлен, то время проверки архивов, вложенных в сообщения электронной почты, ограничено указанным периодом.
Фильтр вложений	Фильтр вложений не работает для исходящих сообщений электронной почты. Фильтр вложений работает для вложений электронной почты в почтовых веб-клиентах, если выбран вариант **Проверять веб-почтовые клиенты**. • **Не применять фильтр**. Если выбран этот вариант, компонент Почтовый Антивирус не фильтрует файлы, вложенные в сообщения электронной почты. • **Переименовывать вложения указанных типов**. Если выбран этот вариант, компонент Почтовый Антивирус заменяет последний символ расширения вложенных файлов указанных типов на символ подчеркивания (например, attachment.doc_). Таким образом, чтобы открыть файл, пользователю нужно переименовать файл. • **Удалять вложения указанных типов**. Если выбран этот вариант, компонент Почтовый Антивирус удаляет из сообщений электронной почты вложенные файлы указанных типов. Типы вложенных файлов, которые нужно переименовывать или удалять из сообщений электронной почты, вы можете указать в списке масок файлов.

Окно Свойства сети (адаптер)

Название

Название сетевого адаптера.

Тип подключения

Тип сетевого адаптера, например, проводная или беспроводная сеть, модемное соединение.

Состояние

Текущее состояние сетевого соединения: *Подключено* или *Отключено*.

В блоке **Новые подключения** вы можете выбрать действие, которое Сетевой экран должен выполнить при обнаружении нового соединения с помощью этого адаптера.

Запрашивать группу

Если Сетевой экран обнаружит новое сетевое соединение, он уведомит вас об этом и запросит выбрать статус для новой сети.

Автоматически помещать новые сети в группу

Если Сетевой экран обнаружит новое сетевое соединение, он автоматически присвоит сети статус, выбранный в раскрывающемся списке.

В раскрывающемся списке вы можете назначить сети статус, который Сетевой экран автоматически присвоит новой сети.

Настройки Мониторинга активности

Включить / выключить

Переключатель включает / выключает Мониторинг активности.

Если переключатель включен, Мониторинг активности собирает и сохраняет данные о всех событиях, которые происходят в операционной системе (например, изменение файла, изменение ключей в реестре, запуск драйверов, попытка завершить работу компьютера). Эти данные используются, чтобы отследить вредоносную и другую активность приложения (в том числе приложений-вымогателей) и восстановить состояние операционной системы до установки этого приложения (отменить последствия вредоносной или другой активности приложения). В некоторых случаях отменить последствия действий приложения невозможно, например, если приложение было обнаружено компонентом Предотвращение вторжений.

Мониторинг активности собирает данные из разных источников, в том числе и от других компонентов приложения Kaspersky Small Office Security. Мониторинг активности анализирует активность приложений и предоставляет собранную информацию о событиях другим компонентам приложения Kaspersky Small Office Security.

В блоке **Защита от эксплойтов** вы можете настроить действия при запуске исполняемых файлов из уязвимых приложений.

Контролировать попытки выполнить несанкционированные операции

Флажок включает / выключает функцию защиты от эксплойтов.

Если флажок установлен, приложение Kaspersky Small Office Security отслеживает исполняемые файлы, запускаемые уязвимыми приложениями. Если приложение Kaspersky Small Office Security обнаруживает, что попытка запустить исполняемый файл из уязвимого приложения не была инициирована пользователем, то он выполняет действие, выбранное в раскрывающемся списке **При обнаружении угрозы**.

При обнаружении угрозы

В раскрывающемся списке можно выбрать действие, которое должен выполнять Мониторинг активности в случае запуска исполняемых файлов из контролируемых уязвимых приложений.

Список содержит следующие варианты действий:

- **Спрашивать пользователя**. Мониторинг активности запрашивает действие у пользователя. Этот вариант доступен, если в разделе **Настройка → Настройки безопасности → Исключения и действия с найденными объектами** снят флажок **Автоматически выполнять рекомендуемые действия**.
- **Выбирать действие автоматически**. Мониторинг активности автоматически выполняет действие, указанное в настройках приложения Kaspersky Small Office Security и добавляет информацию о выбранном действии в отчет. Этот вариант доступен, если в разделе **Настройка → Настройки безопасности → Исключения и действия с найденными объектами** установлен флажок **Автоматически выполнять рекомендуемые действия**.
- **Разрешать действие**. Мониторинг активности разрешает запуск исполняемого файла.
- **Запрещать действие**. Мониторинг активности блокирует запуск исполняемого файла.

При обнаружении вредоносной или другой активности приложения

В раскрывающемся списке можно выбрать действие, которое должен выполнять Мониторинг активности, если в результате анализа активности была замечена вредоносная или другая активность приложения.

- **Спрашивать пользователя**. Мониторинг активности запрашивает действие у пользователя. Этот вариант доступен, если в разделе **Настройка → Настройки безопасности → Исключения и действия с найденными объектами** снят флажок **Автоматически выполнять рекомендуемые действия**.
- **Выбирать действие автоматически**. Мониторинг активности автоматически выполняет действие, рекомендуемое специалистами "Лаборатории Касперского". Этот вариант доступен, если в разделе **Настройка → Настройки безопасности → Исключения и действия с найденными объектами** установлен флажок **Автоматически выполнять рекомендуемые действия**.
- **Удалять приложение**. Мониторинг активности удаляет приложение.
- **Завершать работу приложения**. Мониторинг активности завершает все процессы приложения.
- **Пропускать**. Мониторинг активности не предпринимает никаких действий с приложением.

При возможности отменить последствия вредоносной или другой активности приложения

В раскрывающемся списке можно выбрать действие, которое Мониторинг активности должен выполнять при наличии возможности отменить последствия вредоносной или другой активности приложения.

- **Спрашивать пользователя**. Если в результате работы Мониторинга активности, Файлового Антивируса или выполнения задачи проверки подтверждается необходимость отмены последствий, Мониторинг активности запрашивает действие у пользователя. Этот вариант доступен, если в разделе **Настройка → Настройки безопасности → Исключения и действия с найденными объектами** снят флажок **Автоматически выполнять рекомендуемые действия**.

- **Выбирать действие автоматически**. Если по результатам анализа активности приложения Мониторинг активности признает его вредоносным, то он выполняет отмену последствий активности приложения и уведомляет об этом пользователя. Этот вариант доступен, если в разделе **Настройка → Настройки безопасности → Исключения и действия с найденными объектами** установлен флажок **Автоматически выполнять рекомендуемые действия**.

- **Выполнять откат**. Мониторинг активности выполняет отмену последствий вредоносной или другой активности приложения.

- **Не выполнять откат**. Мониторинг активности сохраняет информацию о вредоносной или другой активности приложения, но не выполняет отмену действий приложения.

В блоке **Защита от приложений блокировки экрана** вы можете настроить действия при активизации приложений блокировки экрана. Приложения блокировки экрана – это вредоносные приложения, которые ограничивают возможность работы на компьютере, блокируя экран, клавиатуру, доступ к панели задач и ярлыкам. Приложения блокировки экрана могут требовать выкуп за возврат возможности работы с операционной системой. С помощью функции защита от приложений блокировки экрана можно завершить работу приложения блокировки экрана по нажатию определенной комбинации клавиш.

Распознавать и закрывать приложения блокировки экрана

Флажок включает / выключает использование функции защиты от приложений блокировки экрана.

Если флажок установлен, при обнаружении действий приложения блокировки экрана вы можете остановить ее работу по нажатию комбинации клавиш, указанной в раскрывающемся списке под флажком.

Для закрытия приложения блокировки экрана вручную использовать комбинацию клавиш

В раскрывающемся списке можно выбрать клавишу или комбинацию клавиш, при нажатии которой функция защиты от приложений блокировки экрана обнаруживает и удаляет приложение блокировки экрана.

По умолчанию используется следующая комбинация клавиш: CTRL+ALT+SHIFT+F4.

Настройки Файлового Антивируса

Настройка	Описание
Уровень безопасности	Для работы Файлового Антивируса приложение применяет разные наборы настроек. Наборы настроек, сохраненные в приложении, называются *уровнями безопасности*. • **Предельный**. Уровень безопасности файлов, при котором компонент Файловый Антивирус максимально контролирует все открываемые, сохраняемые и запускаемые файлы. Компонент Файловый Антивирус проверяет все типы файлов на всех жестких, сменных и сетевых дисках компьютера, а также архивы, установочные пакеты и вложенные OLE-объекты. • **Оптимальный**. Уровень безопасности файлов, который рекомендован для использования специалистами "Лаборатории Касперского". Компонент Файловый Антивирус проверяет только файлы определенных форматов на всех жестких, сменных и сетевых дисках компьютера, а также вложенные OLE-объекты, компонент Файловый Антивирус не проверяет архивы и установочные пакеты. • **Низкий**. Уровень безопасности файлов, параметры которого обеспечивают максимальную скорость проверки. Компонент Файловый Антивирус проверяет только файлы с определенными расширениями на всех жестких, сменных и сетевых дисках компьютера, компонент Файловый Антивирус не проверяет составные файлы.
Действие при обнаружении угрозы	• **Спрашивать пользователя**. Файловый Антивирус информирует вас об обнаружении зараженного или возможно зараженного объекта и запрашивает дальнейшее действие над ним. Этот вариант доступен, если в разделе **Настройка → Настройки безопасности → Исключения и действия с найденными объектами** снят флажок **Автоматически выполнять рекомендуемые действия**. • **Выбирать действие автоматически**. При обнаружении зараженного или возможно зараженного объекта Файловый Антивирус автоматически выполняет над объектом действие, рекомендуемое специалистами "Лаборатории Касперского". Для зараженных объектов таким действием будет Лечить. Это значение выбрано по умолчанию. Перед лечением или удалением зараженного объекта Файловый Антивирус создает его резервную копию на тот случай, если впоследствии понадобится восстановить объект или появится возможность его вылечить. Этот вариант доступен, если в разделе **Настройка → Настройки безопасности → Исключения и действия с найденными объектами** установлен флажок **Автоматически выполнять рекомендуемые действия**. • **Лечить. Удалять, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то приложение их удаляет. • **Лечить. Блокировать, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то приложение добавляет информацию об обнаруженных зараженных файлах в список обнаруженных объектов. • **Блокировать**. Если выбран этот вариант действия, то компонент Файловый Антивирус автоматически блокирует зараженные файлы без попытки их вылечить. Перед лечением или удалением зараженного файла приложение формирует его резервную копию на тот случай, если впоследствии понадобится восстановить файл или появится возможность его вылечить.
Типы файлов	**Все файлы**. Если выбран этот параметр, приложение проверяет все файлы без исключения (любых форматов и расширений). **Файлы, проверяемые по формату**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы. Перед началом поиска вредоносного кода в файле выполняется анализ его внутреннего заголовка на предмет формата файла (например, TXT, DOC, EXE). В процессе проверки учитывается также расширение файла. **Файлы, проверяемые по расширению**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы. Формат файла определяется на основании его расширения.
Изменить область защиты	По ссылке открывается окно **Область защиты Файлового Антивируса** со списком объектов, которые проверяет Файловый Антивирус. Вы можете добавить в список объекты или удалить добавленные вами объекты. Чтобы исключить объект из проверки, не обязательно удалять объект из списка, достаточно снять флажок напротив названия объекта.
Машинное обучение и сигнатурный анализ	При методе проверки Сигнатурный анализ используются базы Kaspersky Endpoint Security, содержащие описания известных угроз и методы их устранения. Защита с использованием этого метода проверки обеспечивает минимально допустимый уровень безопасности. В соответствии с рекомендациями специалистов "Лаборатории Касперского" метод проверки Сигнатурный анализ всегда включен.

Настройка	Описание
Эвристический анализ	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.
Проверять только новые и измененные файлы	Проверка только новых файлов и тех файлов, которые изменились после предыдущей проверки. Это позволит сократить время выполнения проверки. Такой режим проверки распространяется как на простые, так и на составные файлы.
Проверять архивы	Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива).
Проверять дистрибутивы	Проверка сторонних дистрибутивов.
Проверять файлы офисных форматов	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты. Приложение проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка.
Не распаковывать составные файлы большого размера **Максимальный размер файла**	Если флажок установлен, то приложение не проверяет составные файлы, размеры которых больше заданного значения. Если флажок снят, приложение проверяет составные файлы любого размера. Приложение проверяет файлы больших размеров, извлеченные из архивов, независимо от состояния флажка.
Распаковывать составные файлы в фоновом режиме **Минимальный размер файла**	Если флажок установлен, приложение предоставляет доступ к составным файлам, размер которых превышает заданное значение, до проверки этих файлов. При этом приложение в фоновом режиме распаковывает и проверяет составные файлы. Приложение предоставляет доступ к составным файлам, размер которых меньше данного значения, только после распаковки и проверки этих файлов. Если флажок снят, приложение предоставляет доступ к составным файлам только после распаковки и проверки файлов любого размера.
Режим проверки	**Интеллектуальный**. Режим проверки, при котором Файловый Антивирус проверяет объект на основании анализа операций, выполняемых над объектом. Например, при работе с документом Microsoft Office приложение Kaspersky Small Office Security проверяет файл при первом открытии и при последнем закрытии. Все промежуточные операции перезаписи файла из проверки исключаются. **При доступе и изменении**. Режим проверки, при котором Файловый Антивирус проверяет объекты при попытке их открыть или изменить. **При доступе**. Режим проверки, при котором Файловый Антивирус проверяет объекты только при попытке их открыть. **При выполнении**. Режим проверки, при котором Файловый Антивирус проверяет объекты только при попытке их запустить.
Использовать технологию iSwift	Технология, представляющая собой развитие технологии iChecker для компьютеров с файловой системой NTFS. Технология iSwift имеет ограничение: она привязана к конкретному местоположению файла в файловой системе и применима только к объектам, расположенным в файловой системе NTFS. При обновлении версии приложения Kaspersky Small Office Security, технология iSwift включается для всех типов проверки, даже если ранее она была выключена.
Использовать технологию iChecker	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз приложения Kaspersky Small Office Security, дату предыдущей проверки файла, а также изменение настроек проверки. Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной приложению структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).
Исключения	Объекты, исключаемые из проверки. Указываются по ссылке **Исключения**, в окне **Исключения**.
Приостановка работы Файлового Антивируса	Временная автоматическая приостановка работы Файлового Антивируса в указанное время или во время работы с указанными приложениями. Чтобы запланировать паузу, нажмите **Приостановить работу Файлового Антивируса**.

Настройки AMSI-защиты

Настройка	Описание
Проверять архивы	Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива).
Проверять дистрибутивы	Проверка сторонних дистрибутивов.
Проверять файлы офисных форматов	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты. Приложение проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка.
Не распаковывать составные файлы большого размера **Максимальный размер файла**	Если флажок установлен, то приложение не проверяет составные файлы, размеры которых больше заданного значения. Если флажок снят, приложение проверяет составные файлы любого размера. Приложение проверяет файлы больших размеров, извлеченные из архивов, независимо от состояния флажка.

Окно Добавление / изменение персональных данных

Типы персональных данных

По ссылкам в поле **Название поля** подставляется соответствующий тип персональных данных.

Название поля

Описание, которое отображается в списке записей персональных данных (например, *Домашний телефон*, *Рабочий телефон*, *Почтовый индекс*).

Можно подставить описание персональных данных автоматически по нужной ссылке с типом персональных данных.

Значение

Персональные данные, пересылка которых запрещается или разрешается.

Отчет о пересылке персональных данных

В верхней части окна отображается имя учетной записи пользователя, отчет о действиях которого приводится в этом окне.

Контроль включен / выключен  / 

Переключатель позволяет включать / выключать контроль действий пользователя с помощью Веб-Контроля.

В зависимости от того контролирует ли действия пользователя Веб-Контроль, переключатель имеет следующий вид:

 – Веб-Контроль контролирует действия пользователя.

 – Веб-Контроль не контролирует действия пользователя.

Контроль действий пользователя выполняется в соответствии с заданными для него настройками Веб-Контроля.

В окне можно просмотреть информацию об употреблении выбранным пользователем ключевых слов и попытках пересылки персональных данных.

Сегодня

При нажатии на кнопку отображается отчет о действиях пользователя, совершенных за сегодняшний день.

Кнопки 

При нажатии на кнопки отображаются отчеты за предыдущий и следующий период.

День / Неделя / Месяц

Период, за который формируется отчет. Можно сформировать отчет за следующие периоды: день, неделя, месяц.

Кнопка 

При нажатии на кнопку открывается окно настройки Веб-Контроля на разделе **Контроль содержимого**. В этом разделе можно указать ограничения пересылки персональных данных.

Список заблокированных персональных данных

Содержит перечень персональных данных в отправленных и полученных выбранным пользователем сообщениях за отчетный период.

Данные

Графа содержит персональные данные, которые содержались в отправленных или полученных сообщениях.

Для заблокированных персональных данных также указывается тип информации, запрещенной к пересылке.

Ресурс

В графе отображается сайт, через который пользователь пытался отправить или получить сообщение с персональными данными, запрещенными к пересылке.

Статус

Если пересылка сообщения была заблокирована Веб-Контролем, в графе отображается значение *Заблокировано*.

Дата

Графа содержит дату отправки или получения сообщения, содержащего персональные данные, запрещенные к пересылке.

Выбор уровня контроля пользователя

Эта функция доступна только пользователям устаревшей линейки продуктов. Новым пользователям мы рекомендуем установить Kaspersky Safe Kids.

Сбор статистики

При нажатии на кнопку к учетной записи выбранного пользователя применяется уровень контроля с предустановленными по умолчанию настройками. Этот уровень контроля предусматривает только сбор статистики о действиях выбранного пользователя. Ограничения на использование приложений и интернета не установлены.

Выборочные ограничения

К учетной записи выбранного пользователя применяются ограничения, настроенные вручную.

Сильные ограничения

При нажатии на кнопку к учетной записи выбранного пользователя применяется уровень контроля, накладывающий существенные ограничения на использование компьютера и интернета. Этот уровень контроля предусматривает следующие правила использования приложений и интернета:

- разрешено использование интернета;
- разрешено посещение только сайтов, относящихся к категориям "Общение в сети", "Компьютерные игры";
- запрещена загрузка файлов всех типов;
- включен контроль использования компьютера, ограничения использования не установлены;
- включен контроль использования приложений, ограничения использования не установлены;
- включен контроль использования игр, ограничения установлены в соответствии с рейтинговой системой.

Слабые ограничения

При нажатии на кнопку к учетной записи выбранного пользователя применяется уровень контроля, накладывающий небольшие ограничения на использование компьютера и интернета. Этот уровень контроля предусматривает следующие правила использования приложений и интернета:

- разрешено использование интернета;
- разрешено посещение только сайтов, относящихся к категориям "Общение в сети", "Интернет-магазины, банки и платежные системы", "Компьютерные игры";
- включен контроль использования компьютера, ограничения использования не установлены;
- включен контроль использования приложений, ограничения использования не установлены;
- включен контроль использования игр, ограничения установлены в соответствии с рейтинговой системой.

Настройки по умолчанию

При нажатии на кнопку к учетной записи выбранного пользователя применяется профиль с предустановленными по умолчанию настройками. Этот профиль предусматривает следующие правила использования приложений и интернета:

- разрешено использование интернета;
- разрешено посещение только сайтов, относящихся к категориям "Общение в сети", "Интернет-магазины, банки и платежные системы", "Компьютерные игры";
- включен безопасный поиск;
- включен контроль использования компьютера, ограничения использования не установлены;
- включен контроль использования приложений, ограничения использования не установлены;
- включен контроль запуска игр, ограничения запуска не установлены;
- включен контроль защищенных SSL-соединений в браузерах.

Импорт

По ссылке открывается окно для выбора файла, содержащего настройки Веб-Контроля. После выбора файла эти настройки применяются к учетной записи выбранного пользователя.

Экспорт

По ссылке открывается окно для сохранения текущих настроек Веб-Контроля в файл.

Окно Добавить / Изменить маску веб-адреса

Маска веб-адреса

Адрес или маска адреса сайта, доступ к которому требуется разрешить ли запретить.

Действие

Позволяет разрешить или запретить доступ пользователя к сайту.

Можно выбрать один из следующих вариантов:

- **Разрешить**. При выборе этого варианта Веб-Контроль разрешает пользователю доступ к сайту, даже если он относится к запрещенной категории или включено блокирование всех сайтов.
- **Запретить**. При выборе этого варианта Веб-Контроль запрещает пользователю доступ к сайту, даже если он относится к разрешенной категории.

Тип

Позволяет указать область, на которую распространяется разрешение или запрет доступа к сайту.

Можно выбрать один из следующих вариантов:

- **Маска сайта**. При выборе этого варианта Веб-Контроль разрешает или запрещает пользователю доступ ко всем веб-страницам указанного сайта.

  Например, если в поле **Маска веб-адреса** указан адрес example.com, то Веб-Контроль будет разрешать или запрещать доступ ко всем веб-страницам сайта example.com: news.example.com, market.example.com, mail.example.com.

- **Указанный веб-адрес**. При выборе этого варианта Веб-Контроль разрешает или запрещает пользователю доступ только к конкретной странице сайта, указанной в поле **Маска веб-адреса**.

  Например, если в поле **Маска веб-адреса** указан адрес mail.example.com/login, Веб-Контроль будет разрешать или запрещать доступ только к указанной странице авторизации для входа в почтовый ящик интернет-почты. На другие страницы сайта это правило распространяться не будет.

Применить шаблон

Позволяет применить к исключению один из существующих шаблонов с заданным набором настроек.

Можно выбрать один из следующих вариантов:

- **Весь сайт** – при выборе этого варианта Веб-Контроль разрешает или запрещает доступ к домену, указанному в поле **Маска веб-адреса**. Например, если в поле **Маска веб-адреса** указан адрес example.com, Веб-Контроль будет разрешать или запрещать доступ ко всем веб-страницам домена example.com: news.example.com, market.example.com, mail.example.com.

- **Указанная веб-страница** – при выборе этого варианта Веб-Контроль разрешает или запрещает доступ к конкретной странице, указанной в поле **Маска веб-адреса**, и ко всем веб-адресам, содержащим эту страницу. Например, если в поле **Маска веб-адреса** указан адрес example.com/hl, Веб-Контроль будет разрешать или запрещать доступ как к этой странице, так и к содержащим ее веб-адресам, например, example.com/hl/example1.html.

- **Указанный веб-адрес** – при выборе этого варианта Веб-Контроль разрешает или запрещает доступ к конкретному веб-адресу, указанному в поле **Маска веб-адреса**. Например, если в поле **Маска веб-адреса** указан адрес mail.example.com/login, Веб-Контроль будет разрешать или запрещать доступ только к указанной странице авторизации для входа в почтовый ящик интернет-почты. На другие страницы сайта это правило распространяться не будет.

Веб-Контроль. Исключения

В этом окне вы можете сформировать список исключений из заданных настроек Веб-Контроля. Настройки доступа к сайтам, добавленным в список исключений, действуют как при блокировке сайтов по категориям (кнопка выбора **Блокировать доступ к сайтам из выбранных категорий**), так и при блокировке всех сайтов (кнопка выбора **Блокировать доступ ко всем сайтам**).

Например, можно разрешить доступ к сайтам из категории "Общение в сети", но добавить в список исключений сайт example.com с запретом доступа. В этом случае Веб-Контроль разрешает доступ ко всем социальным сетям, кроме сайта example.com. Также можно установить блокирование всех сайтов и добавить в список исключений сайт интернет-почты, доступ к которому разрешен. В этом случае Веб-Контроль предоставляет пользователю доступ только к сайту интернет-почты.

Список исключений

Список содержит перечень веб-адресов, доступ к которым разрешен или запрещен вне зависимости от установленных настроек Веб-Контроля.

С помощью контекстного меню веб-адреса в списке можно изменить веб-адрес или удалить его из списка, а также разрешить или запретить доступ к сайту.

Маска веб-адреса

Адрес или маска адреса сайта, доступ к которому разрешен или запрещен.

Тип

В графе указана область применения запрета или разрешения доступа к сайту.

Если в графе установлено значение *Маска сайта*, разрешение или запрет доступа применяется ко всем страницам сайта.

Если в графе установлено значение *Указанный веб-адрес*, разрешение или запрет доступа применяется только к указанной странице сайта.

Действие

В графе указано, разрешен или запрещен доступ к сайту.

Если в графе установлено значение *Разрешено*, Веб-Контроль разрешает доступ к сайту.

Если в графе установлено значение *Запрещено*, Веб-Контроль запрещает доступ к сайту.

Изменить

При нажатии на кнопку открывается окно **Изменить**, где вы можете изменить маску веб-адреса или адрес веб-сайта, выбранного в списке исключений, и настройки доступа к нему.

Кнопка доступна, если в списке исключений выбрана маска веб-адреса.

Удалить

При нажатии на кнопку приложение удаляет выбранную маску веб-адреса из списка исключений.

Кнопка доступна, если в списке исключений выбрана маска веб-адреса.

Добавить

При нажатии на кнопку открывается окно добавления маски веб-адреса, в котором можно добавить адрес или маску адреса веб-сайта в список исключений.

Окно Ограничения использования приложения

В этом окне можно настроить ограничения времени использования выбранного приложения.

В блоке **Рабочие дни** вы можете указать ограничения времени использования приложения по рабочим дням.

Разрешить доступ не более <N> часов в день

Флажок включает / выключает ограничение времени использования приложения в рабочие дни.

Если флажок установлен, Веб-Контроль ограничивает суммарное время использования приложения для выбранного пользователя. Ограничение времени использования приложения (в часах) указывается в раскрывающемся списке рядом с флажком.

Если флажок снят, Веб-Контроль не ограничивает использование приложения по рабочим дням.

В блоке **Выходные дни** вы можете указать ограничения времени использования приложения по выходным дням.

Разрешить доступ не более <N> часов в день

Флажок включает / выключает ограничение времени использования приложения в выходные дни.

Если флажок установлен, Веб-Контроль ограничивает суммарное время использования приложения для выбранного пользователя. Ограничение времени использования приложения (в часах) указывается в раскрывающемся списке рядом с флажком.

Если флажок снят, Веб-Контроль не ограничивает использование приложения по выходным дням.

В блоке **Перерывы в работе** вы можете настроить периодическое блокирование доступа к приложению в течение суток.

Делать перерыв каждые <N> часов в течение <N> минут

Флажок включает / выключает периодическое блокирование работы приложения с указанной длительностью, чтобы обеспечить отдых пользователя.

Если флажок установлен, Веб-Контроль блокирует работу приложения с периодичностью, указанной в раскрывающемся списке **<ЧЧ:ММ>**. Доступ блокируется на промежуток времени, указанный в раскрывающемся списке **<N> минут**.

В блоке **Точное время использования** отображается таблица времени использования приложения. С помощью таблицы вы можете составить почасовое расписание использования приложения пользователем в течение недели.

Таблица времени использования приложения

С помощью таблицы можно указать дни недели и часы, когда пользователю разрешено пользоваться приложением. Строки таблицы соответствуют дням недели, графы – интервалам в один час на временной шкале. В зависимости от установленных в операционной системе региональных настроек временная шкала может иметь 24- и 12-часовое представление. Цвета ячеек таблицы отражают установленные ограничения: красный цвет означает, что использование приложения запрещено, серый – использование приложения разрешено. При нажатии на ячейку таблицы цвет ячейки изменяется. При наведении на ячейку курсора мыши под таблицей отображается временной интервал, которому соответствует ячейка.

Окно Список персональных данных

Список персональных данных

Список содержит персональные данные пользователя, пересылку которых необходимо контролировать.

Название поля

В графе отображается тип персональных данных (например, *Номер банковской карты*, *Домашний телефон*).

Значение

В графе отображаются персональные данные (например, номер банковской карты, телефон), упоминание которых необходимо отслеживать в переписке.

Изменить

При нажатии на кнопку открывается окно, в котором вы можете изменить запись с персональными данными.

Удалить

Кнопка позволяет удалить выбранную запись из списка.

Добавить

При нажатии на кнопку открывается окно, в котором вы можете добавить в список персональных данных новую запись.

Отчет о заблокированных сайтах и загрузках

Сегодня

При нажатии на кнопку отображается отчет о действиях пользователя, совершенных за сегодняшний день.

Кнопки 

При нажатии на кнопки отображаются отчеты за предыдущий и следующий период.

День / Неделя / Месяц

Период, за который формируется отчет. Можно сформировать отчет за следующие периоды: день, неделя, месяц.

Кнопка

При нажатии на кнопку открывается окно настройки Веб-Контроля на разделе **Интернет**. В этом разделе можно ограничить выбранному пользователю время использования интернета и доступ к сайтам и ограничить скачивание файлов.

Заблокированные сайты и загрузки

Список содержит перечень сайтов, открытие которых было запрещено Веб-Контролем, а также перечень файлов, скачивание которых было заблокировано.

Список содержит следующую информацию:

- название заблокированного сайта или файла;
- причина, по которой пользователю заблокирована попытка доступа (например, *Сайт из запрещенной категории*);
- дата открытия сайта или скачивания файла.

Отчет о запускавшихся приложениях

В верхней части окна отображается имя учетной записи пользователя, отчет о действиях которого приводится в этом окне.

Контроль включен / выключен  / 

Переключатель позволяет включать / выключать контроль действий пользователя с помощью Веб-Контроля.

В зависимости от того контролирует ли действия пользователя Веб-Контроль, переключатель имеет следующий вид:

 – Веб-Контроль контролирует действия пользователя.

 – Веб-Контроль не контролирует действия пользователя.

Контроль действий пользователя выполняется в соответствии с заданными для него настройками Веб-Контроля.

В окне **Отчет о запускавшихся приложениях** вы можете получить информацию о запуске приложений за отчетный период для выбранной учетной записи.

Сегодня

При нажатии на кнопку отображается отчет о действиях пользователя, совершенных за сегодняшний день.

Кнопки 

При нажатии на кнопки отображаются отчеты за предыдущий и следующий период.

День / Неделя / Месяц

Период, за который формируется отчет. Можно сформировать отчет за следующие периоды: день, неделя, месяц.

Кнопка

При нажатии на кнопку открывается окно настройки Веб-Контроля на разделе **Приложения**. В этом разделе можно указать ограничения запуска и использования приложений.

Часто используемые приложения

Содержит перечень приложений, которые запускались пользователем наиболее часто в течение отчетного периода. Также в списке отображается информация о длительности использования приложений.

Заблокированные приложения

Содержит перечень приложений, запуск которых был заблокирован Веб-Контролем. Приложения отображаются в порядке их запуска, начиная с последних.

По ссылке **Еще <N>** можно перейти к просмотру других приложений, запуск которых был заблокирован.

Все используемые приложения

Содержит перечень всех приложений, которые пользователь запускал в течение отчетного периода. Также в списке отображается информация о длительности использования приложений.

Приложения сгруппированы по категориям (например, "Игры" или "IM-клиенты").

При нажатии на кнопку ⌄ можно просмотреть список приложений в категории.

При нажатии на кнопку › список приложений в категории сворачивается в одну строку.

Блокировать игры по категориям

В этом окне можно разрешить или запретить запуск игр в зависимости от их содержимого. Тип категоризации содержимого игр (набор флажков) соответствует рейтингам PEGI или ESRB. Тип категоризации игр выбирается автоматически в зависимости от вашего местоположения. При необходимости можно установить тип категоризации игр вручную в настройках компонента Веб-Контроль.

Если флажок напротив категории установлен, Веб-Контроль блокирует запуск игр, относящихся к этой категории.

Если флажок напротив категории снят, Веб-Контроль разрешает запуск игр, относящихся к этой категории.

Запуск игры разрешен, если ее содержимое относится к категориям, каждая из которых разрешена.

Окно Область действия пароля

Управление Веб-Контролем

Флажок включает / выключает запрос пароля при попытке пользователя открыть окно Веб-Контроля.

Управление Резервным копированием

Флажок включает / выключает запрос пароля при попытке пользователя открыть окно **Резервное копирование**.

Настройка приложения

Флажок включает / выключает запрос пароля при попытке пользователя сохранить изменения настроек приложения.

Завершение работы приложения

Флажок включает / выключает запрос пароля при попытке пользователя завершить работу приложения.

Удаление приложения

Флажок включает / выключает запрос пароля при попытке пользователя удалить приложение.

Создать пароль

Кнопка, при нажатии на которую доступ к указанным функциям приложения ограничивается паролем.

Веб-Контроль. Общая статистика

В верхней части окна отображается имя учетной записи пользователя, отчет о действиях которого приводится в этом окне.

Контроль включен / выключен  / 

Переключатель позволяет включать / выключать контроль действий пользователя с помощью Веб-Контроля.

В зависимости от того контролирует ли действия пользователя Веб-Контроль, переключатель имеет следующий вид:

 – Веб-Контроль контролирует действия пользователя.

 – Веб-Контроль не контролирует действия пользователя.

Контроль действий пользователя выполняется в соответствии с заданными для него настройками Веб-Контроля.

Профиль: <настройки профиля>

По ссылке можно изменить настройки Веб-Контроля, которые требуется применить к текущей учетной записи.

В блоке **Компьютер** можно просмотреть информацию о времени использования компьютера выбранным пользователем, а также перейти к просмотру отчета об использовании компьютера и настройке Веб-Контроля. Статистика использования компьютера отображается за период времени, указанный в отчете о времени работы за компьютером. По умолчанию отображается статистика за текущие сутки.

Подробнее

По ссылке открывается окно **Отчет об использовании компьютера**. В окне можно получить информацию об использовании компьютера выбранным пользователем.

Настройка

По ссылке открывается окно. В этом окне вы можете указать время, в течение которого выбранному пользователю можно находиться за компьютером.

В блоке **Приложения** отображается информация о приложениях, которые выбранный пользователь использовал в последнее время. Статистика использования приложений отображается за период времени, указанный в отчете о запускаемых приложений. По умолчанию отображается статистика за текущие сутки.

Подробнее

По ссылке открывается окно **Отчет о запускавшихся приложениях**. В окне вы можете получить информацию о приложениях, которые запускал выбранный пользователь, и времени их использования.

Настройка

По ссылке открывается окно. В этом окне вы можете указать приложения, с которыми выбранный пользователь может работать.

Блок **Интернет** содержит статистику посещений сайтов и отчет о времени, которое провел пользователь на этих сайтах. Также вы можете посмотреть общее количество заблокированных попыток посещения запрещенных сайтов.

Статистика посещения веб-ресурсов отображается за период времени, указанный в отчете о времени работы в интернете. По умолчанию отображается статистика за текущие сутки.

Подробнее

По ссылке открывается окно **Отчет об использовании интернета**. В окне можно получить информацию о веб-ресурсах, которые посещал выбранный пользователь.

Настройка

По ссылке открывается окно. В этом окне вы можете указать время, в течение которого выбранному пользователю можно пользоваться интернетом.

В блоке **Контроль содержимого** отображается информация об количестве заблокированных попыток передачи персональных данных.

Статистика отображается за период времени, указанный в отчете о контроле содержимого. По умолчанию отображается статистика за одну неделю.

Подробнее

По ссылке открывается окно. В окне можно получить информацию о том, какие персональные данные пытался передать выбранный пользователь, общаясь в социальных сетях.

Настройка

По ссылке открывается окно. В этом окне вы можете указать персональные данные, использование которых в переписке выбранного пользователя вы хотите контролировать.

В этом разделе справки

Отчет об использовании компьютера

Отчет о запускавшихся приложениях

Отчет об использовании интернета

Отчет о пересылке персональных данных

Отчет о заблокированных сайтах и загрузках

Отчет об использовании интернета

В верхней части окна отображается имя учетной записи пользователя, отчет о действиях которого приводится в этом окне.

Контроль включен / выключен  / 

Переключатель позволяет включать / выключать контроль действий пользователя с помощью Веб-Контроля.

В зависимости от того контролирует ли действия пользователя Веб-Контроль, переключатель имеет следующий вид:

 – Веб-Контроль контролирует действия пользователя.

 – Веб-Контроль не контролирует действия пользователя.

Контроль действий пользователя выполняется в соответствии с заданными для него настройками Веб-Контроля.

В окне **Отчет об использовании интернета** вы можете получить информацию о сайтах, которые посещал выбранный пользователь за отчетный период.

Сегодня

При нажатии на кнопку отображается отчет о действиях пользователя, совершенных за сегодняшний день.

Кнопки 

При нажатии на кнопки отображаются отчеты за предыдущий и следующий период.

День / Неделя / Месяц

Период, за который формируется отчет. Можно сформировать отчет за следующие периоды: день, неделя, месяц.

Кнопка

При нажатии на кнопку открывается окно настройки Веб-Контроля на разделе **Интернет**. В этом разделе можно ограничить выбранному пользователю время использования интернета и доступ к сайтам и ограничить скачивание файлов.

Самые посещаемые сайты

Отчет показывает список сайтов, которые пользователь часто посещал в течение отчетного периода, и количество посещений.

Потрачено

Общее время, проведенное выбранным пользователем в интернете за отчетный период.

Заблокировано веб-ресурсов

Перечень сайтов, открытие которых было запрещено Веб-Контролем, а также перечень файлов, скачивание которых было заблокировано.

Показать все

По ссылке открывается окно с информацией о количестве заблокированных загрузок файлов и переходов на сайты.

Категории сайтов

Содержит перечень категорий сайтов. Для каждой категории сайтов указано количество посещений, заблокированных или разрешенных Веб-Контролем:

- красным цветом отображается количество переходов на сайты, заблокированных Веб-Контролем;
- серым цветом отображается количество переходов на сайты, разрешенных Веб-Контролем.

Отчет об использовании компьютера

В верхней части окна отображается имя учетной записи пользователя, отчет о действиях которого приводится в этом окне.

Контроль включен / выключен  / 

Переключатель позволяет включать / выключать контроль действий пользователя с помощью Веб-Контроля.

В зависимости от того контролирует ли действия пользователя Веб-Контроль, переключатель имеет следующий вид:

 – Веб-Контроль контролирует действия пользователя.

 – Веб-Контроль не контролирует действия пользователя.

Контроль действий пользователя выполняется в соответствии с заданными для него настройками Веб-Контроля.

В окне **Отчет об использовании компьютера** вы можете получить информацию о времени использования компьютера за отчетный период для выбранной учетной записи.

Сегодня

При нажатии на кнопку отображается отчет о действиях пользователя, совершенных за сегодняшний день.

Кнопки 

При нажатии на кнопки отображаются отчеты за предыдущий и следующий период.

День / Неделя / Месяц

Период, за который формируется отчет. Можно сформировать отчет за следующие периоды: день, неделя, месяц.

Кнопка

При нажатии на кнопку открывается окно настройки Веб-Контроля на разделе **Компьютер**. В этом разделе можно указать ограничения использования компьютера по времени.

Отчет об использовании компьютера

Содержит информацию о периодах и длительности использования компьютера за отчетный период.

Розовым цветом отображаются промежутки времени, в которые компьютер использовался выбранной учетной записью.

Зеленым цветом отображается текущий период времени (сутки, неделя или месяц).

Красной линией отображается текущее время сегодняшнего дня (если выбран период *День* или *Неделя*).

Окно Управление приложениями

Запуск / Ограничения

По ссылкам изменяется способ отображения приложений в списке:

- По ссылке **Запуск** приложения в списке распределяются по двум группам: **Запрещен** и **Разрешен**.
- По ссылке **Ограничения** приложения в списке распределяются по группам доверия. Например, доверенные приложения будут располагаться в группе **Доверенные**.

Очистка

По ссылке приложение Kaspersky Small Office Security удаляет из списка несуществующие приложения.

Вид

В раскрывающемся списке можно выбрать вид отображения приложений и процессов.

- **Развернуть все**. При выборе этого варианта в списке отображаются все приложения, установленные на компьютере.
- **Свернуть все**. При выборе этого варианта в списке отображаются группы доверия.

В раскрывающемся списке можно выбрать способ отображения приложений и процессов:

- **Показывать как список**. При выборе этого варианта приложения / процессы отображаются в виде списка.
- **Показывать как дерево**. При выборе этого варианта приложения / процессы отображаются в виде иерархической структуры в соответствии с последовательностью вызова процессов.

В раскрывающемся списке также можно выключить отображение системных приложений, приложений "Лаборатории Касперского" и несетевых приложений:

- **Скрывать системные приложения**. При выборе этого элемента в общем списке приложений и процессов не отображаются приложения, необходимые для работы операционной системы. По умолчанию системные приложения скрыты.
- **Скрывать Kaspersky Small Office Security**. При выборе этого элемента в общем списке приложений и процессов не отображаются приложения "Лаборатории Касперского". По умолчанию приложения "Лаборатории Касперского" скрыты.
- **Показывать только сетевые приложения**. При выборе этого элемента в общем списке приложений и процессов отображаются только сетевые приложения. Сетевые приложения – это приложения, предназначенные для организации совместной работы группы пользователей на разных компьютерах.

Список приложений

В списке содержатся приложения, установленные на вашем компьютере. Для каждого приложения в списке отображается информация о статусе, цифровой подписи, группе доверия, популярности приложения среди пользователей KSN и времени последнего запуска.

По двойному щелчку мышью на строке приложения или процесса открывается окно **Правила приложения**. В окне можно настроить правила для контроля действий приложения.

По правой клавише мыши на строке приложения открывается контекстное меню. Из контекстного меню можно выполнить следующие действия:

- открыть окно **Правила приложения**, в котором можно настроить разрешения для действий приложения;
- разрешить или запретить запуск приложения;
- переместить приложение в другую группу доверия;
- установить для приложения настройки контроля активности, предусмотренные по умолчанию (сбросить настройки приложения);
- удалить приложение из списка;
- открыть папку, содержащую исполняемый файл приложения.

Приложения в списке объединены в группы и подгруппы. По правой клавише мыши на строке группы открывается контекстное меню. Из контекстного меню можно выполнить следующие действия:

- открыть окно **Правила группы**, в котором можно настроить разрешения для действий приложения из этой группы, используемые по умолчанию;
- создать подгруппу внутри группы; по умолчанию к подгруппе применяются правила, указанные для группы, в которую она входит;
- добавить приложение в группу; по умолчанию к приложению применяются правила, указанные для группы, в которую она входит;
- установить для группы и всех входящих в нее подгрупп и приложений настройки контроля активности, предусмотренные по умолчанию (сбросить настройки группы);
- установить для подгрупп и приложений, входящих в группу, настройки контроля активности, предусмотренные по умолчанию, оставив настройки группы без изменений (сбросить настройки подгрупп и приложений);
- удалить входящие в группу подгруппы и приложения.

Приложение

В графе отображается название приложения.

Ограничения

В графе отображается группа доверия, в которую помещено приложение. Группа доверия определяет правила использования приложения на компьютере: запрет или разрешение запуска, доступ приложения к файлам и системному реестру, ограничения сетевой активности приложения.

Популярность

В графе отображается уровень популярности приложения среди участников Kaspersky Security Network (KSN). Уровень популярности соответствует числу участников KSN, использующих приложение.

Сеть

В этой графе можно выбрать действие при попытке приложения получить доступ к сети.

В таблице ниже приведено описание действий Kaspersky Small Office Security, если приложение или группа приложений пытается получить доступ к сети.

Действия производимые приложением Kaspersky Small Office Security

Действие	Описание
Наследовать	Приложение или группа приложений наследует реакцию из вышестоящей группы.
Разрешить	Kaspersky Small Office Security разрешает приложениям, входящим в выбранную группу, доступ к сети.
Запретить	Kaspersky Small Office Security запрещает приложениям, входящим в выбранную группу, доступ к сети.
Спрашивать пользователя	Если в разделе **Настройка → Настройки производительности → Оптимизация производительности компьютера** установлен флажок **Автоматически выполнять рекомендуемые действия**, приложение Kaspersky Small Office Security автоматически выбирает действие с этим ресурсом по правилам, созданным специалистами "Лаборатории Касперского". По сноске вы можете прочитать, какое именно действие будет выбрано. Если этот флажок снят, приложение спрашивает пользователя, предоставлять этому приложению доступ к сети или нет.
Записывать в отчет	Помимо заданной реакции, Kaspersky Small Office Security записывает в отчет информацию о попытке доступа приложения к сети.

Запуск

В графе с помощью переключателя можно разрешить или запретить запуск выбранного приложения. По умолчанию запуск приложения разрешен или запрещен в зависимости от ограничений группы, в которую входит приложение.

О защите компьютера

Набор доступных функций защиты может различаться в зависимости от тарифного плана.

Приложение Kaspersky Small Office Security обеспечивает комплексную защиту от вирусов, сетевых атак, фишинга, кражи персональных данных и других видов киберугроз. Для решения задач комплексной защиты в составе приложения Kaspersky Small Office Security предусмотрены различные функции и компоненты защиты.

Каждый тип угроз обрабатывается отдельным компонентом защиты. Вы можете включать и выключать компоненты защиты, а также настраивать их работу.

В дополнение к постоянной защите, реализуемой компонентами защиты, рекомендуется периодически выполнять проверку вашего компьютера на присутствие вирусов и других приложений, представляющих угрозу. Это необходимо делать для того, чтобы исключить возможность распространения вредоносных приложений, которые не были обнаружены компонентами защиты, например, из-за установленного низкого уровня защиты или по другим причинам.

Для поддержки приложения Kaspersky Small Office Security в актуальном состоянии необходимо обновление баз и модулей приложения.

Файловый Антивирус

Файловый Антивирус позволяет избежать заражения файловой системы компьютера. Компонент запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы на вашем компьютере и на всех присоединенных дисках. Приложение Kaspersky Small Office Security перехватывает каждое обращение к файлу и проверяет этот файл на присутствие известных вирусов и других приложений, представляющих угрозу. Дальнейшая работа с файлом возможна только в том случае, если файл не заражен или был успешно вылечен программой. Если файл по каким-либо причинам невозможно вылечить, он будет удален. При этом копия файла будет помещена на карантин. Если на место удаленного файла поместить зараженный файл с таким же именем, в карантине сохраняется только копия последнего файла. Копия предыдущего файла с таким же именем не сохраняется.

Защита от сетевых атак

Компонент Защита от сетевых атак запускается при старте операционной системы и отслеживает во входящем трафике активность, характерную для сетевых атак. Обнаружив попытку атаки на компьютер, приложение Kaspersky Small Office Security блокирует любую сетевую активность атакующего компьютера в отношении вашего компьютера.

Интернет-защита

Интернет-защита перехватывает и блокирует выполнение скриптов, расположенных на сайтах, если эти скрипты представляют угрозу безопасности компьютера. Интернет-защита также контролирует весь веб-трафик и блокирует доступ к опасным сайтам.

Почтовый Антивирус

Почтовый Антивирус проверяет входящие и исходящие почтовые сообщения на вашем компьютере. Письмо будет доступно адресату только в том случае, если оно не содержит опасных объектов.

Сетевой экран

Сетевой экран обеспечивает безопасность вашей работы в локальных сетях и в интернете. Компонент фильтрует всю сетевую активность согласно правилам двух типов: правилам для приложений и пакетным правилам.

Мониторинг активности

Компонент Мониторинг активности отменяет в операционной системе изменения, вызванные вредоносной и другой активностью приложений.

Компонент защищает от вредоносных приложений, в том числе от:

- эксплойтов;
- приложения блокировки экрана;
- приложений-шифровальщиков, которые шифруют данные;
- криптоджекинга;
- приложений-вымогателей, которые шифруют данные или блокируют доступ к файлам или системе, а затем требуют выкуп за восстановление файлов или доступа к этим файлам.

Не рекомендуется выключать этот компонент.

Анти-Фишинг

Приложение Kaspersky Small Office Security защищает вас от перехода на фишинговые сайты. Фишинговый сайт – это поддельный сайт, который выглядит как сайт банка, платежной системы, криптовалютной торговой платформы или как любой другой сайт. Отличить фишинговый сайт от настоящего по внешним признакам довольно сложно. Переход на фишинговый сайт может привести к краже паролей, данных банковских карт и других персональных данных.

Удаление следов активности / Восстановление настроек

В этом окне отображается процесс удаления следов вашей активности в операционной системе или восстановления настроек. Выполнение обеих задач занимает некоторое время. Для подтверждения операции может потребоваться перезагрузка компьютера.

Настройки Безопасных платежей

Включить / выключить Безопасные платежи

Включение компонента Безопасные платежи.

Кнопка отображается, если компонент Безопасные платежи выключен.

Узнать больше

По ссылке открывается окно браузера на странице с более подробной информацией о компоненте.

В блоке **При первом обращении к сайтам банков или платежных систем** вы можете выбрать действие, которое Kaspersky Small Office Security выполняет при обращении к указанным типам сайтов.

Открывать в защищенном режиме браузера

Если приложение обнаруживает попытку доступа к указанному сайту, то открывает этот сайт в защищенном режиме браузера. В обычном браузере, использованном для обращения к сайту, отображается сообщение о запуске защищенного режима браузера.

Спрашивать пользователя

Если приложение обнаруживает попытку доступа к указанному сайту, то предлагает запустить защищенный режим браузера либо открыть сайт при помощи обычного браузера.

Не открывать в защищенном режиме браузера

Когда вы обращаетесь к указанному сайту, приложение не использует защищенный режим браузера. Сайт открывается в обычном браузере.

Для перехода к сайтам из окна Безопасных платежей использовать

В раскрывающемся списке укажите, какой браузер нужно использовать при переходе к сайтам, указанным в окне Безопасных платежей.

Уведомлять об уязвимостях в операционной системе

Если флажок установлен, приложение будет выполнять поиск уязвимостей в операционной системе и предлагает устранить их.

Создать ярлык для Безопасных платежей

По ссылке на рабочем столе создается ярлык для запуска Безопасных платежей. Ярлык позволяет открыть окно со списком сайтов банков или платежных систем, при обращении к которым используется защищенный режим браузера.

В 64-разрядной версии Windows 8, Windows 8.1 и Windows 10 для защиты браузера используется аппаратная виртуализация.

Окно Обновление баз

Обновить

Кнопка, при нажатии на которую запускается обновление баз и модулей приложения.

Последнее обновление: <время последнего обновления>

По ссылке открывается окно **Подробные отчеты**, в котором можно просмотреть информацию о выполненных обновлениях баз и модулей приложения.

Режим запуска: <название режима запуска>

По ссылке открывается окно **Настройки обновления**. В окне можно настроить режим запуска обновлений.

Кнопка

При нажатии на кнопку обновление отменяется, и базы и модули приложения остаются в прежнем состоянии.

Кнопка отображается во время обновления баз и модулей приложения.

Загружено: <совокупный размер загруженных файлов>

По ссылке открывается окно **Подробные отчеты**, в котором можно просмотреть информацию о выполненных обновлениях баз и модулей приложения.

Ссылка отображается во время обновления баз и модулей приложения.

Обзор вирусной активности в мире

По ссылке открывается окно браузера на странице securelist.com, содержащей обзор вирусной активности на текущий момент.

Оптимизация производительности компьютера

Настройка	Описание
Запускать Kaspersky Small Office Security при включении компьютера (рекомендуется)	Если флажок установлен, то приложение Kaspersky Small Office Security запускается после загрузки операционной системы и защищает компьютер пользователя в течение всего сеанса работы. Если флажок не установлен, то приложение Kaspersky Small Office Security не запускается после загрузки операционной системы до того момента, как пользователь запустит приложение вручную. Защита компьютера выключена и данные пользователя могут находиться под угрозой.
Экономия заряда батареи	Если флажок установлен, то режим экономии питания аккумулятора включен. Приложение Kaspersky Small Office Security откладывает выполнение задач, для которых задан запуск по расписанию. По мере необходимости вы можете самостоятельно запускать задачи проверки и обновления.
Режим "Не беспокоить"	Если флажок установлен, приложение Kaspersky Small Office Security не показывает уведомления о событиях во время видео-звонков, во время просмотра фильмов, во время работы с приложениями и клавиатурой. Также в режиме "Не беспокоить" могут быть приостановлены некоторые автоматически запущенные задачи или отложено выполнение запланированных задач, чтобы избежать излишнего потребления ресурсов компьютера.
Режим сосредоточенной работы	Если флажок установлен, приложение не запускает задачи проверки и обновления, не отображает уведомления, когда вы играете или работаете с приложениями в полноэкранном режиме.
Откладывать выполнение задач проверки компьютера при высокой нагрузке на центральный процессор и дисковые системы	Когда приложение Kaspersky Small Office Security выполняет задачи по расписанию, может увеличиваться нагрузка на центральный процессор и дисковые подсистемы, что замедляет работу других приложений. Если флажок установлен, то при увеличении нагрузки приложение Kaspersky Small Office Security приостанавливает выполнение задач по расписанию и высвобождает ресурсы операционной системы для других приложений.
Включить запись дампов	Если флажок установлен, то Kaspersky Small Office Security записывает дампы в случае сбоев в работе. Если флажок снят, то Kaspersky Small Office Security не записывает дампы. Приложение удаляет уже существующие на жестком диске компьютера файлы дампов.
Включить защиту файлов дампов и файлов трассировки	Если флажок установлен, то доступ к файлам дампов предоставляется системному и локальному администраторам, а также пользователю, включившему запись дампов. Доступ к файлам трассировки предоставляется только системному и локальному администраторам. Если флажок снят, доступ к файлам дампов и файлам трассировки имеет любой пользователь.

Исключения и действия с найденными объектами

Настройка	Описание
Автоматически выполнять рекомендуемые действия	Если флажок снят, основные компоненты приложения Kaspersky Small Office Security работают в интерактивном режиме. Это значит, что приложение Kaspersky Small Office Security запрашивает ваше решение при выборе действия с обнаруженными объектами и угрозами, если в настройках Файлового Антивируса, Интернет защиты, Почтового Антивируса, Мониторинга активности и Предотвращения вторжений выбран вариант действия **Спрашивать пользователя**. Если флажок установлен, приложение Kaspersky Small Office Security выбирает действие автоматически на основе правил, заданных специалистами "Лаборатории Касперского".
Удалять вредоносные утилиты, рекламные приложения, приложения автодозвона и подозрительные упаковщики	Если флажок установлен, приложение Kaspersky Small Office Security удаляет вредоносные утилиты, рекламные приложения, приложения автодозвона и упакованные файлы, которые могут содержать вирусы и другие угрозы, в автоматическом режиме защиты. Функция доступна, если установлен флажок **Автоматически выполнять рекомендуемые действия**.
Применять технологию лечения активного заражения (использует значительные ресурсы компьютера)	Если флажок установлен, при обнаружении вредоносной активности в операционной системе на экране отображается всплывающее уведомление. В уведомлении приложение Kaspersky Small Office Security предлагает провести процедуру лечения активного заражения компьютера. После подтверждения пользователем этой процедуры приложение Kaspersky Small Office Security устраняет угрозу. Завершив процедуру лечения активного заражения, приложение Kaspersky Small Office Security выполняет перезагрузку компьютера. Применение технологии лечения активного заражения требует значительных ресурсов компьютера, что может замедлить работу других приложений. Во время обнаружения приложением активного заражения некоторые функции операционной системы могут быть недоступны (например, запуск модулей процесса, работающего в фоновом режиме). Доступность операционной системы восстановится после завершения лечения активного заражения и перезагрузки компьютера.
Типы обнаруживаемых объектов	Приложение обнаруживает объекты разных типов, такие как, например, вирусы и черви, троянские приложения, рекламные приложения. Подробнее о них читайте в Энциклопедии "Касперского".
Обнаруживать сталкерские приложения	Если флажок установлен, приложение Kaspersky Small Office Security обнаруживает сталкерские приложения, с помощью которых злоумышленники могут получить доступ к вашему местоположению и переписке, а также информации о том, какие сайты и соцсети вы посещаете.
Обнаруживать легальные приложения, которые злоумышленники могут использовать для нанесения вреда компьютеру или вашим данным	Если флажок установлен, приложение Kaspersky Small Office Security обнаруживает легальные приложения, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя. К таким приложениям относятся, например, приложения удаленного администрирования, которые используют системные администраторы; чтобы получать доступ к интерфейсу удаленного компьютера для наблюдения и управления. Kaspersky Small Office Security не обнаруживает приложения удаленного администрирования, которые считаются доверенными.
Многократно упакованные объекты	Если флажок установлен, приложение Kaspersky Small Office Security обнаруживает файлы, которые упакованы несколько раз, в том числе разными упаковщиками. Многократная упаковка затрудняет проверку объектов.

Настройка	Описание

Настроить исключения	По ссылке открывается окно **Исключения** со списком исключений из проверки. *Исключение из проверки* – это совокупность условий, при выполнении которых приложение не проверяет объект на вирусы и другие приложения, представляющие угрозу.
	Вы можете добавлять, изменять и удалять исключения из списка.
	В окне добавления или изменения исключения можно задать условия, в соответствии с которыми объекты должны исключаться из проверки (приложение не будет их проверять):
	• Файл или папка, которые нужно исключить из проверки (в том числе можно исключить исполняемые файлы приложений и процессов). Вы можете использовать маски в соответствии со следующими правилами:
	  • Символ `*` (звездочка) который заменяет любой набор символов (включая пустые символы). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением TXT, расположенным в папках на диске (C:), но не в подпапках.
	  • Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.
	  • Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.
	• Тип объектов, которые должны исключаться из проверки. Введите название типа объекта по классификации Энциклопедии "Касперского" (например, `Email-Worm`, `Rootkit` или `RemoteAdmin`). Вы можете использовать маски с символами `?` (заменяет любой символ) и `*` (заменяет любые несколько символов). Например, если указана маска `Client*`, приложение исключает из проверки объекты типов `Client-IRC`, `Client-P2P` и `Client-SMTP`.
	• Хеш-сумму объекта. Сверка хеш-суммы объекта с указанной в этой настройке позволяет исключить из проверки объект, если он не изменялся.
	• Компоненты защиты, при работе которых действует исключение.
	Вместо удаления исключения из списка можно изменить статус исключения на **Неактивно** (в окне добавления или изменения исключения), в этом случае оно не будет действовать.

Указать доверенные приложения	По ссылке открывается окно со списком доверенных приложений. Приложение Kaspersky Small Office Security не контролирует файловую и сетевую активность доверенных приложений (в том числе и вредоносную), а также обращения этих приложений к системному реестру. Вы можете добавлять, изменять и удалять доверенные приложений из списка. Даже если приложение включено в список доверенных, приложение Kaspersky Small Office Security продолжает проверить исполняемый файл и процесс этого приложения на вирусы и другие угрозы. Если вы хотите, чтобы исполняемый файл и процесс доверенного приложения не проверялись, добавьте их в список исключений. При добавлении или изменении доверенного приложения вы можете указать правила, в соответствии с которыми приложение Kaspersky Small Office Security контролирует активность доверенного приложения, в окне **Исключения для приложения**. В окне **Исключения для приложения** доступны для выбора следующие правила: • Не проверять открываемые файлы. • Не контролировать активность приложений. Не контролируется любая активность приложения в рамках работы Предотвращения вторжений. • Не наследовать ограничения родительского процесса (приложения). Если ограничения родительского процесса или приложения не наследуются, активность приложения контролируется по заданным вами правилам или по правилам группы доверия, в которую входит это приложение. • Не контролировать активность дочерних приложений. • Не блокировать взаимодействие с интерфейсом приложения Kaspersky Small Office Security. Приложению разрешено управлять приложением Kaspersky, используя графический интерфейс приложения Kaspersky. Необходимость разрешить приложению управлять интерфейсом приложение Kaspersky Small Office Security может возникнуть при использовании приложений удаленного доступа к рабочему столу или приложения, обеспечивающего работу устройства ввода данных. К таким устройствам относятся, например, сенсорные панели (тачпады), графические планшеты. • Не проверять весь трафик (или зашифрованный трафик). В зависимости от выбранного варианта (**Не проверять весь трафик** или **Не проверять зашифрованный трафик**) приложение Kaspersky Small

Настройка	Описание
	Office Security исключает из проверки весь сетевой трафик приложения или трафик, передаваемый по протоколу SSL. Значение настройки не влияет на работу Сетевого экрана: Сетевой экран проверяет трафик приложения в соответствии с установленными для него настройками. Исключения влияют на работу Почтового Антивируса и Интернет-защиты. Вы можете уточнить IP-адреса или сетевые порты, на которые должно распространяться ограничение контроля трафика. Если в окне **Исключения для приложения** изменить статус на **Неактивно**, приложение Kaspersky Small Office Security не относит приложение к доверенным. Таким образом можно временно исключить приложение из доверенных, не удаляя из списка.

Настройки сети

Настройка	Описание
Ограничивать трафик при лимитном подключении	Если флажок установлен, приложение ограничивает собственный сетевой трафик в том случае, если подключение к интернету является лимитным. Приложение Kaspersky Small Office Security определяет высокоскоростное мобильное подключение к интернету как лимитное, а подключение по Wi-Fi – как безлимитное. Учет стоимости подключения работает на компьютерах под управлением Windows 8 и выше.
Внедрять в трафик скрипт взаимодействия с веб-страницами	Если флажок установлен, приложение Kaspersky Small Office Security внедряет в трафик скрипт взаимодействия с веб-страницами. Этот скрипт обеспечивает работу таких компонентов как Безопасные платежи, Защита от сбора данных в интернете, Анти-Баннер, Проверка ссылок.
Поддерживать работу DNS поверх HTTPS (DoH)	Если флажок установлен, приложение корректно обрабатывает данные DNS при передаче их по протоколу HTTPS. Мы не рекомендуем снимать этот флажок.
Управлять DoH-серверами	По ссылке открывается окно, в котором вы можете добавить вручную DoH-сервер, через который будет выполняться передача данных DNS в браузере. Здесь вы можете прочитать о том, что такое DNS поверх HTTPS (DoH) и как добавить DoH-сервер.
Контролируемые порты	**Контролировать все сетевые порты**. Режим контроля портов, при котором Почтовый Антивирус и Интернет-защита контролируют все открытые порты вашего компьютера. **Контролировать только выбранные сетевые порты**. Режим контроля портов, при котором Почтовый Антивирус и Интернет защита контролируют выбранные вами порты вашего компьютера. Указать контролируемые сетевые порты можно в окне **Сетевые порты**, которое открывается по ссылке **Выбрать**. Вы также можете указать, при работе каких приложений нужно контролировать все сетевые порты, используемые этими приложениями: • **Контролировать все порты для приложений из списка, рекомендованного "Лабораторией Касперского"**. Список таких приложений задан по умолчанию и входит в комплект поставки приложения Kaspersky Small Office Security. Если установлен этот флажок, приложение Kaspersky Small Office Security контролирует все порты для следующих приложений: • Adobe Acrobat Reader. • Apple Application Support. • Google Chrome. • Microsoft Edge. • Mozilla Firefox. • Internet Explorer. • Java. • mIRC. • Opera. • Pidgin. • Safari. • Агент Mail.ru. • Яндекс.Браузер. • **Контролировать все порты для указанных приложений**. Указать приложения можно в окне **Приложения**, которое открывается по ссылке **Выбрать**.

Настройка	Описание
Сетевые порты	Список портов, которые обычно используются для передачи почты и веб-трафика, включен в комплект поставки приложения Kaspersky Small Office Security. По умолчанию приложение Kaspersky Small Office Security контролирует трафик, проходящий через все порты из этого списка. Вы можете добавить в список порты или удалить их из списка. Если в графе **Статус** в строке порта установлено значение *Активно*, то приложение Kaspersky Small Office Security контролирует трафик, проходящий через этот порт. Если в графе **Статус** в строке порта установлено значение *Неактивно*, то приложение Kaspersky Small Office Security исключает этот порт из проверки, но не удаляет его из списка портов. Изменить статус и другие параметры порта можно в окне по кнопке **Изменить**.
Проверка защищенных соединений	Вы можете выбрать один из режимов проверки защищенных соединений по протоколу SSL: • **Не проверять защищенные соединения**. • **Проверять защищенные соединения по запросу компонентов защиты**. • **Всегда проверять защищенные соединения**. Если выбрано **Проверять защищенные соединения по запросу компонентов защиты**, приложение Kaspersky Small Office Security использует установленный сертификат "Лаборатории Касперского" для проверки SSL-соединений, если этого требуют компоненты Интернет защита и Проверка ссылок. Если эти компоненты выключены, приложение Kaspersky Small Office Security не проверяет SSL-соединения. После того как приложение Kaspersky Small Office Security проверит SSL-соединение, в сертификатах сайтов может не отображаться название организации, на которую зарегистрирован сайт. **Показать сертификаты**. Некоторые известные сайты теперь используют новый корневой сертификат. Мы считаем соединение с такими сайтами безопасным. Данная функция позволяет добавить или удалить этот сертификат из доверенных. Если вы не хотите, чтобы приложение проверяло SSL-соединение с сайтом, вы можете добавить сайт в список исключений по ссылке **Настроить доверенные адреса**.
Переход на домен с ошибкой проверки защищенного соединения	В раскрывающемся списке вы можете выбрать действие, которое выполняет приложение, если на каком-либо сайте возникла ошибка проверки защищенных соединений. • **Игнорировать**. Приложение разрывает соединение с сайтом, на котором возникла ошибка проверки. • **Спрашивать**. Приложение показывает вам уведомление с предложением добавить адрес сайта в список сайтов, на которых возникли ошибки проверки. Адрес сайта будет проверен по базе вредоносных объектов. • **Разрешать и добавлять домен в исключения**. Приложение добавляет адрес сайта в список сайтов, на которых возникли ошибки проверки. Адрес сайта будет проверен по базе вредоносных объектов.
Домены с ошибками проверки	Список доменов, которые не были проверены из-за того, что при подключении к ним возникли ошибки. Адреса доменов были проверены по базе вредоносных объектов.
Настроить доверенные адреса	По ссылке открывается окно **Доверенные адреса** со списком сайтов, которые вы добавили как исключение для компонентов Интернет защита и Проверка ссылок.
Настроить доверенные приложения	Список приложений, активность которых приложение Kaspersky Small Office Security не проверяет в процессе своей работы. Вы можете выбрать виды активности приложения, которые приложение Kaspersky Small Office Security не будет контролировать (например, не проверять сетевой трафик). Приложение Kaspersky Small Office Security поддерживает переменные среды и символы `*` и `?` для ввода маски.
Блокировать соединения по протоколу SSL 2.0	Если флажок установлен, то приложение отслеживает и блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0. Если флажок снят, то приложение не блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0. В этом случае приложение также не отслеживает сетевой трафик, передаваемый по этому протоколу.
Расшифровывать защищенное соединение с сайтом, использующим EV-сертификат	EV-сертификаты (англ. Extended Validation Certificate) подтверждают подлинность веб-сайтов и повышают безопасность соединения. Браузеры сообщают о наличии на веб-сайте EV-сертификата с помощью значка замка в адресной строке браузера. Также браузеры могут полностью или частично окрашивать адресную строку в зеленый цвет. Если флажок установлен, приложение расшифровывает и контролирует защищенные соединения с EV-сертификатом. Если флажок снят, приложение не имеет доступа к содержанию HTTPS-трафика. Поэтому приложение контролирует HTTPS-трафик только по адресу веб-сайта, например, `https://bing.com`. Если вы впервые открываете веб-сайт с EV-сертификатом, защищенное соединение будет расшифровано независимо от того, установлен флажок или нет.

Настройка	Описание
Настройка прокси-сервера	Параметры прокси-сервера для доступа пользователей клиентских компьютеров в интернет. Приложение Kaspersky Small Office Security использует эти параметры в работе некоторых компонентов защиты, в том числе для обновления баз и модулей приложения. Для автоматической настройки прокси-сервера приложение Kaspersky Small Office Security использует протокол WPAD (Web Proxy Auto-Discovery Protocol). В случае если по этому протоколу не удается определить IP-адрес прокси-сервера, приложение использует адрес прокси-сервера, указанный в параметрах браузера Microsoft Internet Explorer.
В приложениях с собственным хранилищем сертификатов для проверки защищенных соединений использовать	Если этот флажок установлен, приложение проверяет зашифрованный трафик в поддерживаемых браузерах и почтовых клиентах. Доступ к некоторым сайтам по протоколу HTTPS может быть заблокирован. Для проверки трафика в браузере Mozilla Firefox и почтовом клиенте Thunderbird должна быть включена проверка защищенных соединений. Если проверка защищенных соединений выключена, приложение не проверяет трафик в браузере Mozilla Firefox и почтовом клиенте Thunderbird. Приложение расшифровывает и анализирует зашифрованный трафик с помощью корневого сертификата "Лаборатории Касперского". Вы можете выбрать хранилище сертификатов, в котором будет находиться корневой сертификат "Лаборатории Касперского": • **Хранилище сертификатов Windows (рекомендуется)**. Это хранилище, в которое корневой сертификат "Лаборатории Касперского" добавляется при установке приложения Kaspersky Small Office Security. • **Собственное хранилище сертификатов**. Некоторые браузеры и почтовые клиенты используют собственное хранилище сертификатов вместо хранилища сертификатов Windows. Если вы выбрали собственное хранилище сертификатов, добавьте корневой сертификат "Лаборатории Касперского" в хранилище вручную через свойства браузера или почтового клиента.

Управление настройками приложения

Настройка	Описание
Импортировать	Извлечь настройки работы приложения из файла формата CFG и применить их.
Экспортировать	Сохранить текущие настройки работы приложения в файл формата CFG.
Восстановить	Вы в любое время можете восстановить настройки приложения, рекомендуемые "Лабораторией Касперского". В результате восстановления настроек для всех компонентов защиты будет установлен уровень безопасности **Оптимальный**.

Сетевой экран

Kaspersky Small Office Security требует включения **Службы определения местоположения** в настройках компьютера для определения Wi-Fi сетей.

Настройка	Описание
Уведомлять об уязвимостях при подключении к сети Wi-Fi	Если флажок установлен, приложение Kaspersky Small Office Security показывает уведомления при обнаружении уязвимостей сети Wi-Fi. Флажок доступен для изменения, если на компьютере не установлено приложение Kaspersky Secure Connection. Если установлен флажок **Запрещать передачу пароля в интернете в незащищенном виде и показывать уведомление**, приложение Kaspersky Small Office Security блокирует передачу пароля в незащищенном текстовом виде при заполнении поля **Пароль** в интернете. По ссылке **Выбрать категории** открывается окно **Категории**, в котором вы можете указать типы уязвимостей сетей Wi-Fi. Приложение будет предупреждать вас о том, что сеть Wi-Fi, к которой вы подключаетесь, имеет указанную уязвимость.
Разрешать подключения на случайный порт для активного режима FTP	Если флажок установлен, Сетевой экран разрешает подключение к вашему компьютеру на случайный порт, если до этого был обнаружен переход в активный режим FTP на управляющем соединении.
Не выключать Сетевой экран до полного завершения работы операционной системы	Если флажок установлен, Сетевой экран не прекращает работу до полной остановки операционной системы.
Блокировать сетевые соединения, если нет возможности запросить действие у пользователя	Если флажок установлен, работа Сетевого экрана не останавливается в то время, когда не загружен интерфейс приложения Kaspersky Small Office Security.
Правила приложений	По ссылке открывается окно **Сетевые правила приложений**. В окне отображается информация, связанная с контролем сетевой активности приложений и групп приложений. Сетевую активность приложений в соответствии с сетевыми правилами приложений и групп приложений регулирует компонент Предотвращение вторжений. Вы можете настроить разрешения на сетевую активность приложения или группы приложений через меню ячейки в графе **Сеть**. Элементы меню описаны в разделе Правила Предотвращения вторжений. Выбрав в контекстном меню строки пункт **Подробности и правила**, вы можете перейти к настройке сетевых правил приложения или группы приложений.

Настройка	Описание
Пакетные правила	По ссылке открывается окно **Пакетные правила**. По умолчанию в окне представлены предустановленные сетевые пакетные правила, которые рекомендованы специалистами "Лаборатории Касперского" для оптимальной защиты сетевого трафика компьютеров под управлением операционных систем Microsoft Windows. Сетевые пакетные правила используются для ввода ограничений на сетевые пакеты независимо от приложения. Такие правила ограничивают входящую и исходящую сетевую активность по определенным портам выбранного протокола передачи данных. Сетевые пакетные правила имеют приоритет над сетевыми правилами приложений.

Настройка	Описание
	[Как добавить или изменить пакетное правило?] 1. Откройте главное окно приложения. 2. Нажмите на кнопку в нижней части главного окна. 3. Откроется окно **Настройка**.

Настройка	Описание

	4. Выберите раздел **Настройки безопасности → Сетевой экран**.
	
	5. Задайте или отредактируйте следующие параметры:
	
	• **Статус**. Сетевой экран применяет только пакетные правила со статусом **Активно**. Вы можете установить статус **Неактивно**, чтобы временно выключить пакетное правило, не удаляя его из списка пакетных правил.
	
	• **Название**. Название правила.
	
	• **Действие**.
	
	  • **Разрешать**. Приложение Kaspersky Small Office Security разрешает сетевое соединение.
	
	  • **Запрещать**. Приложение Kaspersky Small Office Security запрещает сетевое соединение.
	
	  • **По правилам приложения**. Приложение Kaspersky Small Office Security не обрабатывает поток данных в соответствии с пакетным правилом, а применяет правило для приложения (см. **Правила приложений** выше).
	
	• **Направление**.
	
	  • **Входящее**. Приложение Kaspersky Small Office Security применяет правило к сетевому соединению, которое открыл удаленный компьютер.
	
	  • **Исходящее**. Приложение Kaspersky Small Office Security применяет правило к сетевому соединению, которое открыл ваш компьютер.
	
	  • **Входящее / Исходящее**. Приложение Kaspersky Small Office Security применяет правило как к входящему, так и к исходящему пакету или потоку данных, независимо от того, какой компьютер (ваш или удаленный) инициировал сетевое соединение.
	
	  • **Входящее (пакет)**. Приложение Kaspersky Small Office Security применяет правило к пакетам данных, которые принимает ваш компьютер.
	
	  • **Исходящее (пакет)**. Приложение Kaspersky Small Office Security применяет правило к пакетам данных, которые передает ваш компьютер.
	
	• **Протокол**. Протокол, используемый пакетными правилами.
	
	• **Настройки ICMP**. Вы можете указать тип и код проверяемых пакетов данных. Блок настроек доступен, если выбраны протоколы ICMP, ICMPv6.
	
	• **Удаленные порты**. Порты удаленного компьютера.
	
	• **Локальные порты**. Порты вашего компьютера.

Настройка	Описание
	Вы можете указать диапазон удаленных или локальных портов (например, `6660 - 7000`), перечислить порты через запятую или сочетать оба способа (например, `80 - 83,443,1080`). • **Адрес (локальный и удаленный)**. Приложение сохраняет локальные адреса только в том случае, если заполнен список удаленных адресов. В частности, для настройки **Удаленные адреса** необходимо выбрать вариант **Адреса из списка** и добавить хотя бы один адрес. • **Любой адрес**. • **Адреса подсети**. Приложение Kaspersky Small Office Security применяет правило к IP-адресам всех сетей, подключенных в данный момент и имеющих указанный тип (*Публичная*, *Локальная* или *Доверенная*). Тип сети вы можете выбрать в раскрывающемся списке, который отображается ниже, если выбрано **Адреса подсети**. • **Адреса из списка**. Приложение Kaspersky Small Office Security применяет правило к IP-адресам, входящим в заданный диапазон. • **Записывать события в отчет**. Запись событий в отчет приложения Kaspersky Small Office Security. • **Сетевые адаптеры**. Сетевые адаптеры, через которые передаются сетевые пакеты. • **Использовать TTL**. Приложение Kaspersky Small Office Security контролирует передачу сетевых пакетов, у которых время жизни (TTL, Time to Live) не превышает указанного значения. В общем списке пакетных правил приоритет правил определяется сверху вниз, от самого высокого приоритета к самому низкому. Если два правила являются взаимоисключающими, то первым будет выполняться верхнее. Если два правила дополняют друг друга, оба правила будут выполнены. Чтобы изменить положение правила в списке, выберите правило и используйте кнопки **Вверх** и **Вниз** на странице **Пакетные правила**. Для быстрого добавления правила вы можете выбрать один из готовых шаблонов в раскрывающемся списке в нижней части окна.
Доступные сети	По ссылке открывается окно **Сети** со списком сетевых соединений, которые Сетевой экран обнаружил на компьютере.

Настройка	Описание

	В списке вы можете изменить тип сети (*Публичная*, *Доверенная* или *Локальная*) с помощью меню в ячейке **Тип сети**. Настройки сети вы можете изменить в окне **Свойства сети**, которое открывается по двойному щелчку на строке сети.
	
	Сети Интернет по умолчанию присвоен тип *Публичная*. Вы не можете изменить тип и другие настройки сети Интернет.
	
	В окне **Свойства сети** вы можете изменить следующие настройки сети:
	• Название сети.
	• Тип сети.
	• Отображение уведомлений:
	  • о подключении к сети;
	  • об изменении MAC-адреса (например, в случае замены сетевого адаптера);
	  • об изменениях соответствия MAC-адреса и IP-адреса (например, когда сервис DHCP назначает другой IP-адрес).
	• Выбор принтера, который должен предлагаться по умолчанию при подключении к этой сети. Эта настройка отображается, если в операционной системе вашего компьютера установлен принтер.
	• Список дополнительных подсетей (указываются через запятую).

Использование Веб-Контроля

Эта функция доступна только пользователям устаревшей линейки продуктов. Новым пользователям мы рекомендуем установить Kaspersky Safe Kids.

Веб-Контроль позволяет контролировать действия разных пользователей на компьютере и в сети. С помощью Веб-Контроля вы можете ограничивать доступ к интернет-ресурсам и приложениям, а также просматривать отчеты о действиях пользователей.

Пользователи интернета сталкиваются с целым рядом угроз:

- потеря времени и / или денег при посещении чатов, игровых ресурсов, интернет-магазинов, аукционов;
- скачивание файлов, зараженных вредоносными приложениями.

Веб-Контроль позволяет снизить риски, связанные с работой на компьютере и в интернете. Для этого используются следующие функции:

- ограничение использования компьютера и интернета по времени;
- создание списков разрешенных и запрещенных для запуска игр и приложений, а также временное ограничение запуска разрешенных приложений;
- создание списков разрешенных и запрещенных для доступа сайтов, выбор категорий не рекомендованного к просмотру содержимого веб-ресурсов;
- включение режима безопасного поиска с помощью поисковых систем (при этом ссылки на сайты с сомнительным содержимым не отображаются в результатах поиска);
- ограничение скачивания файлов из интернета;
- запрет пересылки определенных персональных данных.

Вы можете настраивать функции Веб-Контроля для каждой учетной записи пользователя на компьютере отдельно. Если пользователь использует две учетные записи: например, локальную учетную запись операционной системы и учетную запись Microsoft, Веб-Контроль следует настраивать для учетной записи Microsoft.

Вы также можете просматривать отчеты Веб-Контроля о действиях контролируемых пользователей компьютера.

При смене часового пояса или переходе на зимнее или летнее время действуют следующие правила использования компьютера, интернета, а также запуска игр и приложений:

- Если при смене часового пояса не меняется дата, текущий отсчет времени до момента блокировки продолжается без изменений. Такое же правило действует при переходе на зимнее или летнее время.

- Если при смене часового пояса дата меняется в большую или меньшую сторону, израсходованное пользователем время обнуляется, и отчет времени до момента блокировки начинается заново.

Веб-Контроль недоступен, если приложение Kaspersky Small Office Security установлено на файловом сервере.

В этом разделе справки

Переход к настройке Веб-Контроля

Контроль использования компьютера

Контроль использования интернета

Контроль запуска игр и приложений

Контроль содержимого переписки

Просмотр отчета о действиях пользователя

Выбор профиля пользователя

Переход к настройке Веб-Контроля

Чтобы перейти к настройке Веб-Контроля:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Безопасность**.
3. В блоке **Веб-Контроль** нажмите на кнопку **Открыть**.
4. Если доступ к настройкам Веб-Контроля не защищен паролем, приложение предложит задать пароль. Выберите один из предложенных вариантов действия:
   - Если вы хотите защитить паролем доступ к настройкам Веб-Контроля, выполните следующие действия:
     a. Нажмите на кнопку **Создать пароль**. Откроется окно **Настройки интерфейса**.
     b. Установите переключатель **Защита паролем** в положение **Вкл**.
     c. В открывшемся окне заполните поля ввода **Имя пользователя** (рекомендованное значение KLAdmin), **Введите пароль** и **Подтвердите пароль**.
     d. Нажмите на кнопку **Сохранить**.
     e. Чтобы вернуться назад к окну **Веб-Контроль**, нажмите на название предыдущего шага вверху страницы.
   - Если вы не хотите защищать паролем доступ к настройкам Веб-Контроля, по ссылке **Пропустить** перейдите к настройке Веб-Контроля. Откроется окно **Веб-Контроль**.
5. Выберите учетную запись пользователя и по ссылке **Настроить ограничения** перейдите к окну настройки Веб-Контроля.

Контроль запуска игр и приложений

Эта функция доступна только пользователям устаревшей линейки продуктов. Новым пользователям мы рекомендуем установить Kaspersky Safe Kids.

С помощью Веб-Контроля вы можете разрешать или запрещать пользователю запуск игр в зависимости от их возрастной категории. Также вы можете запретить пользователю запуск определенных приложений (например, игр, IM-клиентов) или ограничить время использования приложений.

Как запретить запуск игр, содержимое которых не соответствует возрасту пользователя

Чтобы запретить запуск игр, содержимое которых не соответствует возрасту пользователя:

1. Перейдите в окно настройки Веб-Контроля.
2. В окне настройки Веб-Контроля выберите раздел **Приложения**.
3. Если вы хотите заблокировать запуск всех игр, содержимое которых не соответствует возрасту пользователя, установите флажок **Ограничить запуск игр для возраста младше** и выберите возрастное ограничение в раскрывающемся списке рядом с флажком.
4. Если вы хотите заблокировать запуск игр с определенным содержимым, выполните следующие действия:
   a. Установите флажок **Блокировать игры из категорий для взрослых**.
   b. По ссылке **Выбрать категории игр** перейдите в окно **Блокировать игры по категориям**.
   c. Установите флажки напротив категорий содержимого игр, которые нужно блокировать.
5. Вернитесь в раздел **Приложения**.
6. Если вы хотите воспользоваться рейтинговой системой для блокировки игр, выберите тип рейтингов и категоризации содержимого игр в раскрывающемся списке **Для блокирования игр использовать рейтинговую систему**:
   - **Определять автоматически** – Веб-Контроль выбирает тип рейтингов игр в зависимости от вашего местоположения: европейскую рейтинговую систему (PEGI) или систему рейтингов для США и Канады (ESRB).
   - **PEGI** – при настройке разрешений запуска игр Веб-Контроль использует европейскую рейтинговую систему.
   - **ESRB** – при настройке расширений запуска игр Веб-Контроль использует рейтинговую систему для США и Канады.

Установите переключатель, расположенный в верхней части окна, в положение **Контроль включен**.

Как ограничить запуск определенного приложения

Чтобы ограничить запуск определенного приложения:

1. Перейдите в окно настройки Веб-Контроля.
2. В окне настройки Веб-Контроля выберите раздел **Приложения**.
3. По ссылке **Настроить ограничения** перейдите в окно **Использование приложений**.
4. По кнопке **Добавить приложение** в открывшемся окне выберите исполняемый файл приложения.

   Выбранное приложение появится в списке **Использование приложений**. Приложение Kaspersky Small Office Security автоматически добавит это приложение в определенную категорию, например, *Игры*.
5. Выполните следующие действия:

   - Если вы хотите заблокировать запуск приложения, в раскрывающемся списке напротив названия приложения выберите элемент **Запретить**.
   - Если вы хотите заблокировать запуск всех приложений определенной категории, установите флажок напротив названия категории в списке (например, вы можете заблокировать приложения категории *Игры*).
   - Если вы хотите разрешить запуск приложения, в раскрывающемся списке напротив названия приложения выберите элемент **Разрешить**.
   - Если вы хотите установить ограничения на время использования приложения, в раскрывающемся списке напротив названия приложения выберите элемент **Ограничить**.

     Откроется окно **Ограничение использования приложения**.

     Выполните следующие действия:

     a. Если вы хотите ограничить время использования приложения в рабочие и выходные дни, в блоках **Рабочие дни** и **Выходные дни** установите флажок **Разрешить доступ не более <N> часов в день** и в раскрывающемся списке укажите количество часов в день, в течение которых пользователю разрешено использовать приложение. Также вы можете указать точное время, когда пользователю разрешено / запрещено использовать приложение, воспользовавшись таблицей **Точное время использования**.

     b. Если вы хотите задать перерывы в использовании приложения, в блоке **Перерывы в работе** установите флажок **Делать перерыв <время> в течение <интервал>** и выберите частоту и длительность перерыва в раскрывающихся списках.

     c. Нажмите на кнопку **Сохранить**.
6. Закройте окно **Использование приложений**.

   Установите переключатель, расположенный в верхней части окна, в положение **Контроль включен**  . Веб-Контроль будет применять заданные ограничения при работе пользователя с приложением.

В этом разделе справки

Блокировать игры по категориям

Окно Ограничения использования приложения

Окно Использование приложений

Контроль использования интернета

Эта функция доступна только пользователям устаревшей линейки продуктов. Новым пользователям мы рекомендуем установить Kaspersky Safe Kids.

С помощью Веб-Контроля вы можете ограничить время использования интернета, а также запретить доступ пользователя к избранным категориям сайтов и отдельным сайтам. Кроме того, вы можете запретить пользователю скачивать из интернета файлы определенных типов (например, архивов, видео).

Как ограничить время использования интернета

Чтобы ограничить время использования интернета:

1. Перейдите в окно настройки Веб-Контроля.
2. В окне настройки Веб-Контроля выберите раздел **Интернет**.
3. Если вы хотите ограничить общее время использования интернета по рабочим дням, в блоке **Ограничение доступа в интернет** установите флажок **Ограничивать доступ в рабочие дни до N часов в день** и выберите ограничение по времени в раскрывающемся списке рядом с флажком.
4. Если вы хотите ограничить общее время использования интернета по выходным дням, установите флажок **Ограничивать доступ в выходные дни до N часов в день** и выберите ограничение по времени в раскрывающемся списке рядом с флажком.

Установите переключатель, расположенный в верхней части окна, в положение **Контроль включен** . Веб-Контроль будет ограничивать общее время, проводимое пользователем в интернете, в соответствии с указанными значениями.

Как ограничить посещение определенных сайтов

Чтобы ограничить посещение определенных сайтов:

1. Перейдите в окно настройки Веб-Контроля.
2. В окне настройки Веб-Контроля выберите раздел **Интернет**.
3. Чтобы в результатах поиска не отображалось содержимое "для взрослых", в блоке **Контроль посещения сайтов** установите флажок **Включить безопасный поиск с помощью поисковых систем**.

   При поиске информации на сайтах, таких как Google™, YouTube™ (только для пользователей, не вошедших на сайт youtube.com под своей учетной записью), Bing®, Yahoo!™, Yandex среди результатов поиска не будет присутствовать содержимое "для взрослых".
4. Чтобы запретить доступ к сайтам определенных категорий, выполните следующие действия:
   a. В блоке **Контроль посещения сайтов** установите флажок **Контролировать доступ к сайтам**.
   b. В окне **Блокировать доступ к сайтам из выбранных категорий** по ссылке **Выбрать категории сайтов** перейдите в окно **Блокировать доступ к категориям сайтов**.
   c. Установите флажки напротив категорий сайтов, открытие которых необходимо блокировать.

      Веб-Контроль будет блокировать открытие сайта пользователем, если его содержимое относится к какой-либо из запрещенных категорий.
5. Чтобы запретить доступ к отдельным сайтам, выполните следующие действия:
   a. В блоке **Контроль посещения сайтов** установите флажок **Контролировать доступ к сайтам**.
   b. По ссылке **Настроить исключения** перейдите в окно **Исключения**.
   c. В нижней части окна нажмите на кнопку **Добавить**.

      Откроется окно добавления новой маски веб-адреса.
   d. Введите адрес сайта, посещение которого необходимо запретить, в поле **Маска веб-адреса**.
   e. Выберите область действия запрета в блоке **Область применения**: весь сайт или только указанная веб-страница.
   f. Если вы хотите запретить посещение указанного сайта, в блоке **Действие** выберите вариант **Запретить**.
   g. Нажмите на кнопку **Добавить**.

   Указанный сайт появится в списке в окне **Исключения**. Закройте окно **Исключения**.
6. Установите переключатель, расположенный в верхней части окна, в положение **Контроль включен** .

Веб-Контроль будет блокировать посещение сайтов в соответствии с указанными настройками.

Как запретить скачивание файлов определенных типов

Чтобы запретить скачивание из интернета файлов определенных типов:

1. Перейдите в окно настройки Веб-Контроля.
2. В окне настройки Веб-Контроля выберите раздел **Интернет**.
3. В блоке **Запрет загрузки файлов** установите флажки напротив типов файлов, скачивание которых необходимо блокировать.
4. Установите переключатель, расположенный в верхней части окна, в положение **Контроль включен**  .

Веб-Контроль будет блокировать скачивание файлов указанных типов из интернета.

В этом разделе справки

Веб-контроль. Исключения

Окно Добавить / Изменить маску веб-адреса

Информация о категориях сайтов

Контроль использования компьютера

Эта функция доступна только пользователям устаревшей линейки продуктов. Новым пользователям мы рекомендуем установить Kaspersky Safe Kids.

Веб-Контроль позволяет задать ограничения времени, проводимого пользователем за компьютером. Вы можете указать интервал времени, когда Веб-Контроль должен блокировать доступ к компьютеру (время сна), а также общее ограничение времени использования компьютера в течение дня. Можно указать различные ограничения для рабочих и выходных дней.

Чтобы настроить ограничения времени использования компьютера:

1. Перейдите в окно настройки Веб-Контроля.
2. В окне настройки Веб-Контроля выберите раздел **Компьютер**.
3. Чтобы указать интервал времени, в течение которого Веб-Контроль будет блокировать доступ к компьютеру, в блоках **Рабочие дни** и **Выходные дни** установите флажок **Блокировать доступ с N до N**.
4. В раскрывающемся списке рядом с флажком **Блокировать доступ с N** укажите время начала блокировки.
5. В раскрывающемся списке **до N** укажите время окончания блокировки.

   Веб-Контроль будет блокировать пользователю доступ к компьютеру в течение указанного интервала времени.
6. Расписание времени использования компьютера также можно задать с помощью таблицы. Таблица отображается при нажатии на кнопку  .

   Веб-Контроль будет блокировать пользователю доступ к компьютеру **по расписанию**, заданному в таблице.
7. Чтобы ограничить общее время использования компьютера в течение дня, в блоках **Рабочие дни** и **Выходные дни** установите флажок **Разрешить доступ не более N часов в день** и выберите интервал времени в раскрывающемся списке рядом с флажком.

   Веб-Контроль будет блокировать пользователю доступ к компьютеру, когда общее время использования компьютера в течение дня превысит указанный интервал.
8. Чтобы задать перерывы при использовании компьютера пользователем, в блоке **Перерывы в работе** установите флажок **Делать перерыв <время> в течение <интервал>** и выберите периодичность (например, каждый час) и длительность (например, 10 минут) перерывов в раскрывающихся списках рядом с флажком.
9. Установите переключатель, расположенный в верхней части окна, в положение **Контроль включен**  .

Веб-Контроль будет блокировать доступ пользователя к компьютеру в соответствии с указанными настройками.

Контроль содержимого переписки

Эта функция доступна только пользователям устаревшей линейки продуктов. Новым пользователям мы рекомендуем установить Kaspersky Safe Kids.

С помощью Веб-Контроля вы можете отслеживать и запрещать пользователю употребление в переписке указанных персональных данных (например, фамилии, номера телефона, номера банковских карт).

Как настроить контроль пересылки персональных данных

Чтобы настроить контроль пересылки персональных данных:

1. Перейдите в окно настройки Веб-Контроля.
2. В окне настройки Веб-Контроля выберите раздел **Контроль содержимого**.
3. В блоке **Контроль передачи персональных данных** установите флажок **Запретить передачу персональных данных третьим лицам**.
4. По ссылке **Изменить список персональных данных** перейдите в окно **Список персональных данных**.
5. В нижней части окна нажмите на кнопку **Добавить**.

   Откроется окно добавления персональных данных.
6. Выберите тип персональных данных (например, "номер телефона") по ссылке или введите описание в поле **Название поля**.
7. Укажите персональные данные (например, фамилию, номер телефона) в поле **Значение**.
8. Нажмите на кнопку **Добавить**.

   Персональные данные появятся в списке в окне **Список персональных данных**.
9. Закройте окно **Список персональных данных**.
10. Установите переключатель, расположенный в верхней части окна, в положение **Контроль включен**.

Веб-Контроль будет отслеживать и блокировать употребление указанных персональных данных в переписке через интернет.

В этом разделе справки

Окно Список персональных данных

Окно Добавление / изменение персональных данных

Просмотр отчета о действиях пользователя

Эта функция доступна только пользователям устаревшей линейки продуктов. Новым пользователям мы рекомендуем установить Kaspersky Safe Kids.

Вы можете просмотреть отчеты о действиях каждого пользователя, для которого настроен Веб-Контроль, отдельно для каждой категории контролируемых событий.

Чтобы просмотреть отчет о действиях контролируемого пользователя:

1. Перейдите в окно настройки Веб-Контроля.
2. Выберите учетную запись пользователя и по ссылке **Посмотреть отчет** перейдите к окну отчетов.
3. В блоке с нужным типом ограничения (например, **Интернет**) откройте отчет о контролируемых действиях по ссылке **Подробнее**.

В окне отобразится отчет о контролируемых действиях пользователя.

Правила приложения / Правила группы

Настройка	Описание
Файл (только в окне **Правила приложения**)	Справочная информация о приложении и об исполняемом файле приложения. Приложение Kaspersky Small Office Security получает информацию о приложении как из исполняемого файла приложения, так и из Kaspersky Security Network.
Файлы и системный реестр	Правила доступа к ключам системного реестра и к файлам, связанным с работой операционной системы или с вашими персональными данными. Настройки доступа для операций чтения, записи, создания и удаления можно установить независимо друг от друга, с помощью меню в ячейках соответствующих столбцов таблицы. Элементы меню описаны в разделе Правила Предотвращения вторжений.
Права	Права доступа к процессам и ресурсам операционной системы, права на запуск. Установить права доступа можно с помощью меню в ячейках столбца **Действие**. Элементы меню описаны в разделе Правила Предотвращения вторжений.

Настройка	Описание

Сетевые правила	Правила, в соответствии с которыми приложение Kaspersky Small Office Security регулирует сетевую активность приложения или группы приложений.
	По умолчанию в списке отображаются предустановленные сетевые правила приложений, которые рекомендованы специалистами "Лаборатории Касперского". Вы не можете удалить или изменить предустановленные сетевые правила (кроме изменения действия в столбце **Разрешение**, см. описание доступных действий в разделе Правила Предотвращения вторжений).
	При добавлении правила или его изменении вы можете установить следующие настройки:
	• Действие:
	  • **Разрешать**. Приложение Kaspersky Small Office Security разрешает сетевое соединение.
	  • **Запрещать**. Приложение Kaspersky Small Office Security запрещает сетевое соединение.
	  • **Спрашивать пользователя**. Приложение Kaspersky Small Office Security спрашивает пользователя о разрешении или запрете сетевого соединения, если в разделе **Настройка → Настройки безопасности → Исключения и действия с найденными объектами** снят флажок **Автоматически выполнять рекомендуемые действия]**. Если флажок установлен, действие выбирается автоматически. По сноске в окне приложения вы можете прочитать, какое именно действие будет выбрано.
	• Название.
	• Направление:
	  • **Входящее**. Приложение Kaspersky Small Office Security применяет правило к сетевому соединению, которое открыл удаленный компьютер.
	  • **Исходящее**. Приложение Kaspersky Small Office Security применяет правило к сетевому соединению, которое открыл ваш компьютер.
	  • **Входящее / Исходящее**. Приложение Kaspersky Small Office Security применяет правило как к входящему, так и к исходящему пакету или потоку данных, независимо от того, какой компьютер (ваш или удаленный) инициировал сетевое соединение.
	• Протокол.
	• Параметры ICMP. Вы можете указать тип и код проверяемых пакетов данных. Блок настроек доступен, если выбраны протоколы ICMP, ICMPv6.
	• Удаленные порты (порты удаленного компьютера).
	• Локальные порты (порты вашего компьютера).
	Вы можете указать диапазон удаленных или локальных портов (например, `6660 - 7000`), перечислить порты через запятую или сочетать оба способа (например, `80 - 83,443,1080`).
	• Адрес:
	  • **Любой адрес**.
	  • **Адреса подсети**. Приложение Kaspersky Small Office Security применяет правило к IP-адресам всех сетей, подключенных в данный момент и имеющих указанный тип (*Публичная*, *Локальная* или *Доверенная*). Тип сети вы можете выбрать в раскрывающемся списке, который отображается ниже, если выбрано **Адреса подсети**.
	  • **Адреса из списка**. Приложение Kaspersky Small Office Security применяет правило к IP-адресам, входящим в заданный диапазон. Вы можете указать IP-адреса в поле **Удаленные адреса**, которое отображается ниже, если выбрано **Адреса из списка**.
	• Сетевые адаптеры, через которые передаются сетевые пакеты.
	• Использование TTL. Приложение Kaspersky Small Office Security контролирует передачу сетевых пакетов, у которых время жизни (TTL, Time to Live) не превышает указанного значения.
	• Запись событий в отчет приложения Kaspersky Small Office Security.
	Для быстрого добавления правила вы можете выбрать один из готовых шаблонов в раскрывающемся списке в нижней части окна.

Настройка	Описание
Исключения (только в окне **Правила приложения**)	Вы можете выбрать правила, в соответствии с которыми приложение исключается из проверки: • Не проверять открываемые файлы. • Не контролировать активность приложений. Не контролируется любая активность приложения в рамках работы Предотвращения вторжений. • Не наследовать ограничения родительского процесса (приложения). Если ограничения родительского процесса или приложения не наследуются, активность приложения контролируется по заданным вами правилам или по правилам группы доверия, в которую входит это приложение. • Не контролировать активность дочерних приложений. • Не блокировать взаимодействие с интерфейсом приложения Kaspersky Small Office Security. Приложению разрешено управлять приложением Kaspersky, используя графический интерфейс приложения Kaspersky. Необходимость разрешить приложению управлять интерфейсом приложение Kaspersky Small Office Security может возникнуть при использовании приложений удаленного доступа к рабочему столу или приложения, обеспечивающего работу устройства ввода данных. К таким устройствам относятся, например, сенсорные панели (тачпады), графические планшеты. • Не проверять весь трафик (или зашифрованный трафик). В зависимости от выбранного варианта (**Не проверять весь трафик** или **Не проверять зашифрованный трафик**) приложение Kaspersky Small Office Security исключает из проверки весь сетевой трафик приложения или трафик, передаваемый по протоколу SSL. Значение настройки не влияет на работу Сетевого экрана: Сетевой экран проверяет трафик приложения в соответствии с установленными для него настройками. Исключения влияют на работу Почтового Антивируса и Интернет-защиты. Вы можете уточнить IP-адреса или сетевые порты, на которые должно распространяться ограничение контроля трафика.
История (только в окне **Правила приложения**)	Справочная информация о действиях с приложением, например, о запуске приложения или присвоении группы доверия.

Правила Предотвращения вторжений

Правило – это набор реакций Предотвращения вторжений на действия приложения над различными категориями ресурсов операционной системы и персональных данных.

Возможны следующие реакции Предотвращения вторжений на действия приложения:

- **Наследовать**. Предотвращение вторжений применяет правило к активности приложения, заданное для того статуса, который Предотвращение вторжений присвоило приложению.

  Эта реакция применяется по умолчанию. По умолчанию Предотвращение вторжений наследует права доступа из статуса, который Предотвращение вторжений присвоило приложению.

  Если вы изменили правило для приложения, то в этом случае правило для приложения будет иметь более высокий приоритет, чем правило для статуса, который присвоен приложению.

- **Разрешить**. Предотвращение вторжений позволяет приложению совершать действие.

- **Запретить**. Предотвращение вторжений запрещает приложению совершать действие.

- **Спрашивать пользователя**. Предотвращение вторжений запрашивает решение пользователя, если в разделе **Настройка → Настройки безопасности → Исключения и действия с найденными объектами** снят флажок **Автоматически выполнять рекомендуемые действия**. Если флажок установлен, действие выбирается автоматически. По сноске в окне приложения Kaspersky Small Office Security вы можете прочитать, какое именно действие будет выбрано.

- **Записывать в отчет**. Предотвращение вторжений записывает в отчет информацию об активности приложения и своей реакции. Добавление информации в отчет может быть использовано в комбинации с любым другим действием Предотвращения вторжений.

Настройки Защиты ввода данных

Настройка	Описание
Использовать аппаратную виртуализацию, если она доступна	Если флажок установлен, для работы защищенного режима браузера используется аппаратная виртуализация (гипервизор). Приложение использует технологию гипервизора для дополнительной защиты от сложных вредоносных приложений, которые могут похищать ваши персональные данные с помощью буфера обмена и фишинга. Флажок отображается в 64-разрядной версии Windows 8, Windows 8.1 и Windows 10. Подробнее о том, что такое аппаратная виртуализация и как она работает, вы можете прочитать по ссылке.
Защита с помощью аппаратной виртуализации	Защита ввода данных с аппаратной клавиатуры позволяет избежать перехвата данных, которые вы вводите с клавиатуры на сайтах (см. подробнее в разделе О защите ввода данных с аппаратной клавиатуры). Установите флажки для категорий сайтов, на которых нужно защищать ввод данных с аппаратной клавиатуры. По ссылке **Настройка исключений** можно сформировать списки сайтов, на которых нужно включить или выключить защиту ввода данных с аппаратной клавиатуры вне зависимости от выбранных категорий сайтов. При добавлении исключения вы можете использовать маски.
Экранная клавиатура	Многие приложения-шпионы обладают функциями снятия снимков экрана, которые автоматически передаются злоумышленнику для последующего анализа и извлечения персональных данных пользователя. Экранная клавиатура защищает вводимые персональные данные от перехвата посредством снятия снимков экрана. (Подробнее об Экранной клавиатуре). Вы можете отметить, какими способами открывать Экранную клавиатуру: • **Открывать Экранную клавиатуру по комбинации клавиш CTRL+ALT+SHIFT+P**. • **Показывать значок быстрого вызова в полях ввода**. Значок вызова Экранной клавиатуры отображается в полях ввода пароля на веб-страницах. Установите флажки для категорий сайтов, на которых нужно защищать ввод данных с помощью Экранной клавиатуры. По ссылке **Настройка исключений** в окне **Исключения для Экранной клавиатуры** можно сформировать списки сайтов, на которых нужно включить или выключить отображение значка быстрого вызова Экранной клавиатуры вне зависимости от выбранных категорий сайтов. При добавлении исключения вы можете использовать маски.
Показывать в браузере подсказки для создания сильных паролей	Если флажок установлен, приложение Kaspersky Small Office Security проверяет, насколько надежен пароль, который вы вводите в первый раз в браузере, и уведомляет вас об этом.
Защита от использования одинаковых паролей	Когда вы вводите пароль на сайте, где безопасность пароля особенно важна (например, в социальной сети), приложение Kaspersky Small Office Security предлагает вам включить защиту от использования одинаковых паролей. Если установлен флажок **Предупреждать об использовании одинаковых паролей на сайтах**, защита от использования одинаковых паролей включена. Вы можете **выбрать категории сайтов**, которые нужно защищать от использования одинаковых паролей: сайты банков и платежных систем, сайты социальных сетей, сайты почтовых сервисов.
Удалить сохраненные данные	По ссылке **Удалить сохраненные данные** вы можете удалить все сохраненные ранее пароли.
Проверка надежности пароля учетной записи Windows	Kaspersky Small Office Security проверяет пароль, который используется для получения удаленного доступа к файловому серверу, в соответствии со следующими настройками: • **Сообщать об устаревшем пароле через**. Если с момента смены пароля прошло столько времени, сколько указано в этой настройке, Kaspersky Small Office Security сообщает об устаревшем пароле. • **Рекомендовать изменить пароль через**. Если с момента смены пароля прошло столько времени, сколько указано в этой настройке, Kaspersky Small Office Security рекомендует изменить пароль. • **Сообщать, если минимально разрешенная длина пароля в настройках Windows менее**. В настройках Windows можно указать минимальную длину пароля (например, в Windows 10 это может быть значение в диапазоне от 0 до 14 символов). Kaspersky Small Office Security проверяет значение в настройках Windows, и если оно меньше, чем указано в Kaspersky Small Office Security, приложение сообщает об этом.

Окно Выберите файлы для удаления

Поле для ввода пути к файлу или папке

Поле содержит путь к файлу или папке для необратимого удаления. Файл или папку можно выбрать в дереве, расположенном выше поля ввода, или указать вручную.

Окно Выбор данных для шифрования

Поле для ввода пути к файлу или папке

Поле содержит путь к файлу или папке, которые нужно добавить в секретную папку. Файл или папку можно выбрать в дереве, расположенном выше поля ввода, или указать вручную.

Окно Открыть секретную папку

Пароль для доступа к секретной папке

Пароль для доступа к файлам в секретной папке.

Открыть в Проводнике

При нажатии на кнопку в Проводнике открывается папка со списком файлов и папок, хранящихся в секретной папке.

Окно Удаление секретной папки

Пароль для доступа к секретной папке

Пароль для доступа к файлам в секретной папке.

Удалить секретную папку

При нажатии на кнопку приложение Kaspersky Small Office Security удаляет секретную папку и все файлы в ней.

Файлы и папки, находящиеся в секретной папке, удаляются без возможности восстановления.

Окно переименования секретной папки

Новое название папки

Новое название, которое будет присвоено секретной папке.

Сохранить

При нажатии на кнопку приложение Kaspersky Small Office Security присваивает секретной папке новое название.

Окно изменения пароля от секретной папки

Старый пароль

Текущий пароль от секретной папки.

Новый пароль

Новый пароль от секретной папки.

Подтверждение пароля

Повторный ввод пароля, введенного в поле **Новый пароль**.

Сохранить

При нажатии на кнопку текущий пароль от секретной папки заменяется новым.

Окно выбора файла или секретной папки

Поле для ввода пути к файлу или секретной папке

Поле содержит путь к файлу или секретной папке. Файл или секретную папку можно выбрать в дереве, расположенном выше поля ввода, или указать путь к файлу или секретной папке вручную.

Окно Резервное копирование

Создать новую копию

При нажатии на кнопку запускается мастер создания резервной копии.

Запустить

При нажатии на кнопку запускается создание резервных копий файлов.

Настроить

Нажатие кнопки возобновляет процесс создания задачи резервного копирования.

Остановить

Нажатие кнопки останавливает процесс создания резервной копии. Вы можете возобновить процесс резервного копирования позже.

Продолжить

При нажатии на кнопку возобновляется процесс создания резервной копии.

Отменить

При нажатии на кнопку отменяется процесс создания резервной копии.

Подробнее

По ссылке открывается окно **Отчеты**. В окне отображается детальная информация о выполненных задачах резервного копирования.

Мои хранилища

По ссылке открывается окно со списком доступных хранилищ резервных копий. Из этого окна вы можете перейти к восстановлению файлов из резервных копий в выбранном хранилище, изменению настроек выбранного хранилища или удалению этого хранилища, а также добавить хранилище в список.

Подключить мое хранилище

При нажатии на кнопку открывается окно **Подключение хранилища**, в котором можно подключиться к существующему хранилищу резервных копий.

Окно Выбор папки для резервного копирования

Поле для ввода пути к папке

Поле содержит путь к папке, резервную копию которой нужно создать. Папку можно выбрать в дереве, расположенном выше поля ввода, или указать вручную.

Окно Утилита восстановления

Копировать утилиту восстановления Kaspersky Restore Utility в хранилище

Если флажок установлен, приложение Kaspersky Small Office Security в процессе резервного копирования добавляет в хранилище утилиту восстановления Kaspersky Restore Utility. С помощью этой утилиты вы можете восстановить файлы из резервных копий в тех случаях, когда приложение Kaspersky Small Office Security повреждено или не установлено.

Окно Файлы, выбранные для резервного копирования

Список типов файлов

Содержит названия типов файлов и количество файлов каждого типа.

При выборе элемента списка отображается список всех файлов этого типа.

Список файлов выбранного типа

Содержит информацию о файлах определенного типа, выбранных для резервного копирования: имя файла, расположение и размер.

Если флажок напротив названия файла установлен, приложение создает резервную копию этого файла.

Если флажок напротив названия файла снят, приложение не создает резервную копию этого файла.

Раздел Сетевой диск

Сетевой диск

Путь к сетевой папке, используемой в качестве хранилища резервных копий.

Выбрать

При нажатии на кнопку открывается окно **Выбор папки**. В этом окне можно выбрать сетевую папку, используемую в качестве хранилища резервных копий.

Имя пользователя

Имя учетной записи для доступа к сетевой папке. Имя пользователя указывается в формате *<название компьютера>\<имя пользователя>* (например, *kl-12345\ivanov*).

Пароль

Пароль для доступа к сетевой папке.

Раздел Локальный диск

Список локальных дисков

В списке перечислены локальные диски компьютера. Вы можете выбрать один из локальных дисков в качестве хранилища резервных копий.

Если локальный диск отсутствует в списке, вы можете указать путь к нему в поле, расположенном ниже, или нажать на кнопку **Выбрать** и выбрать локальный диск в открывшемся окне **Выбор папки для резервного копирования**.

Выбрать

При нажатии на кнопку открывается окно **Выбор папки для резервного копирования**. В этом окне можно выбрать локальный диск, используемый в качестве хранилища резервных копий.

Раздел Внешний диск

Список подключенных внешних дисков

В списке перечислены внешние диски, подключенные к компьютеру. Вы можете выбрать один из внешних дисков в качестве хранилища резервных копий.

Если внешний диск отсутствует в списке, вы можете указать путь к нему в поле, расположенном ниже, или нажать на кнопку **Выбрать** и выбрать внешний диск в открывшемся окне **Выбор папки**.

Выбрать

При нажатии на кнопку открывается окно **Выбор папки**. В этом окне можно выбрать внешний диск, используемый в качестве хранилища резервных копий.

Раздел Облачное хранилище

Для использования Облачного хранилища нужно войти на сайт dropbox.com. После нажатия на кнопку **OK** веб-страница с формой входа на сайт dropbox.com откроется автоматически.

Окно Хранилища

Список хранилищ

Содержит созданные хранилища резервных копий. Для каждого хранилища отображается информация об общем и используемом размере хранилища, о расположении хранилища и использующих это хранилище задачах, а также доступные действия.

Посмотреть файлы

При нажатии на кнопку открывается окно со списком наборов резервных копий, хранимых в этом хранилище. В окне вы можете выбрать, из какого набора резервных копий нужно восстановить файлы.

При нажатии на кнопку раскрывается меню, в котором можно выбрать дополнительное действие:

- **Посмотреть файлы** – открыть окно **Резервное копирование**, где вы можете выбрать резервную копию и просмотреть список файлов для резервного копирования.
- **Удалить хранилище** – не использовать этот диск или онлайн-ресурс в качестве хранилища резервных копий файлов, а также удалить из него все резервные копии файлов.
- **Очистить хранилище** – открыть окно **Очистка хранилища**. В этом окне можно выбрать, какие резервные копии файлов следует удалить из хранилища, чтобы освободить место в хранилище.

Добавить

По ссылке открывается окно **Добавление сетевого диска**. В окне вы можете указать настройки сетевого диска, который нужно добавить в список хранилищ.

Подключить мое хранилище

По ссылке открывается окно **Подключение хранилища**. В окне вы можете указать настройки локального, внешнего, сетевого диска или Онлайн-хранилища, которое нужно добавить в список хранилищ.

Окно со списком наборов резервных копий в хранилище

Список наборов резервных копий

Содержит информацию о наборах резервных копий в хранилище:

- название набора резервных копий;
- объем дискового пространства, необходимый для восстановления файлов из этого набора.

Посмотреть файлы

При нажатии на кнопку открывается окно **Выберите файлы для восстановления**. В окне вы можете выбрать резервные копии, из которых нужно восстановить файлы.

Окно Поддержка

Окно содержит информацию, необходимую для обращения в Службу технической поддержки: версию приложения Kaspersky Small Office Security, дату и время выпуска баз и модулей приложения, версию операционной системы, ключ.

Лицензионный ключ

По ссылке **<ключ>** открывается окно **Информация о лицензии**, в котором приведены сведения о действующей лицензии.

Другие версии

По ссылке открывается сайт, с которого вы можете загрузить версию приложения, предназначенную для использования в вашем регионе. Ссылка доступна не во всех версиях приложения.

Ответы на часто задаваемые вопросы

По ссылке открывается окно браузера на странице интерактивной поддержки. Эта страница содержит ответы на вопросы, которые пользователи чаще всего задают специалистам Службы технической поддержки.

Рекомендации по настройке приложения

По ссылке открывается окно браузера на странице сайта Службы технической поддержки, где опубликованы статьи о настройке и использовании приложения Kaspersky Small Office Security.

Форум

По ссылке открывается окно браузера на странице Форума "Лаборатории Касперского", где вы можете просматривать опубликованные темы, оставлять свои комментарии, создавать новые темы, пользоваться поиском.

Мониторинг проблем

По ссылке открывается окно **Мониторинг проблем**. В этом окне можно собрать техническую информацию о работе приложения и создать отчет о состоянии системы.

Запись проблемы

По ссылке вы можете выполнить видео-запись возникшей у вас проблемы.

Окно Очистка хранилища

Резервные копии, созданные до

Удаление из хранилища тех резервных копий файлов, которые были созданы до даты, указанной в поле рядом с флажком.

Устаревшие версии резервных копий

Если флажок установлен, при очистке хранилища резервных копий удаляются устаревшие версии резервных копий. Количество наиболее новых версий резервных копий, которые нужно оставить в хранилище, указывается в поле **Количество версий резервных копий, которые нужно оставить**.

Резервные копии, исходные файлы которых удалены

Флажок включает / выключает удаление из хранилища резервных копий тех файлов, которые удалены с компьютера.

Окно Выбор версии резервной копии для восстановления

Список версий резервных копий

Содержит информацию об имеющихся версиях резервных копий файла. Каждый элемент списка содержит имя файла, номер версии, дату создания версии резервной копии.

По правой клавише мыши отображается контекстное меню элемента списка, содержащее следующие пункты:

- **Открыть** – версия резервной копии файла открывается в окне приложения, соответствующего формату файла.
- **Восстановить версию резервной копии** – открывается окно **Выберите папку**. В окне вы можете выбрать папку, в которую нужно поместить восстановленный файл.

Восстановить файлы

При нажатии на кнопку открывается окно, в котором вы можете изменить настройки восстановления файлов.

Окно Выбор папки

Поле для ввода пути к папке

Поле содержит путь к папке, в которую нужно поместить восстановленные файлы. Папку можно выбрать в дереве, расположенном выше поля ввода, или указать путь к ней вручную.

Окно Восстановление файлов

Остановить

При нажатии на кнопку приложение прекращает восстановление файлов из резервных копий.

Окно Восстановление файлов

Остановить

При нажатии на кнопку приложение прекращает восстановление файлов из резервных копий.

Окно Настройки хранилища

Название хранилища

Поле содержит название хранилища резервных копий.

Окно мастера восстановления из резервной копии

Резервная копия

В раскрывающемся списке можно выбрать данные, которые требуется восстановить.

Дата копирования

В раскрывающемся списке можно выбрать дату и время резервного копирования файлов, которые нужно восстановить. Выбранные файлы будут восстановлены в том состоянии, в котором они находились на эту дату и время.

Поиск

Поле для поиска резервной копии файла по имени файла. Поиск выполняется по мере ввода символов.

Кнопка  /

С помощью кнопки-переключателя можно изменять отображение списка резервных копий файлов: структура папок или алфавитный список файлов.

Список файлов

В списке перечислены резервные копии файлов, доступные для восстановления.

В зависимости от положения переключателя  может отображаться древовидная структура папок либо все резервные копии файлов в алфавитном порядке.

В списке приведена информация об имени резервной копии файла, расположении исходного файла, типе файла, расширении имени файла, размере файла и количестве версий резервных копий этого файла. По ссылке в графе **Версия** открывается окно **Выберите версию, из которой хотите восстановить файл**. В окне вы можете выбрать версию резервной копии, из которой требуется восстановить файл.

Если флажок напротив имени резервной копии файла установлен, приложение восстанавливает этот файл.

Если флажок напротив имени резервной копии файла снят, то приложение не восстанавливает этот файл.

По правой клавише мыши отображается контекстное меню элемента списка, содержащее следующие пункты:

- **Открыть файл** – файл открывается с помощью приложения, предназначенного для работы с файлами этого типа.
- **Восстановить последнюю версию резервной копии** – открывается окно **Выберите папку**, в котором вы можете указать, в какую папку следует восстановить файл из последней версии резервной копии.
- **Версии резервных копий файла** – открывается окно **Выберите версию, из которой хотите восстановить файл**. В окне вы можете выбрать версию резервной копии, из которой требуется восстановить файл.

Версия

По ссылке открывается окно **Выберите версию, из которой хотите восстановить файл**, в котором вы можете просмотреть все версии выбранного файла, доступные для восстановления.

Выбрать другое хранилище

По ссылке открывается окно выбора резервного хранилища.

Восстановить файлы

При нажатии на кнопку открывается окно, в котором вы можете изменить настройки восстановления файлов.

Окно Хранилище не указано

Указать хранилище

При нажатии на кнопку открывается окно **Выберите хранилище с резервной копией**.

В окне требуется указать путь к хранилищу резервных копий. Хранилище может располагаться на локальном, съемном или сетевом диске.

Выберите, что вы хотите восстановить

Резервная копия

Нажатие этой кнопки запускает мастер восстановления из резервной копии.

Секретная папка

Нажатие этой кнопки запускает мастер, позволяющий восстановить доступ к секретной папке.

Список секретных папок, к которым восстанавливается доступ

Открыть

При нажатии на эту кнопку открывается окно, в котором можно ввести пароль для доступа к секретной папке.

Добавить папку

Нажатие этой кнопки возвращает вас в окно выбора секретной папки.

О фишинге

Фишинг – это вид интернет-мошенничества, заключающийся в краже персональных данных пользователей, распространяемый по электронной почте и другим каналам.

Электронные письма представляют собой поддельные уведомления от банков, провайдеров, онлайн-магазинов, электронных платежных систем или других организаций. В письмах получателя заманивают пройти на сайт мошенников под предлогом, например, обновить регистрационные данные или узнать подробнее о товаре или услуге.

Ничего не подозревающий получатель такого письма проходит по указанной ссылке и оказывается на фишинговом сайте, который выглядит как точная копия официального сайта организации.

Пользователь интернета может попасть на фишинговый сайт другими способами, например, перейдя по ссылке в поисковой системе.

Как правило, мошенники могут преследовать разные цели. Одна из них – обманным путем получить конфиденциальные данные пользователей, такие как логины, пароли от аккаунта или криптокошелька и другие регистрационные данные, номера счетов и банковских карт. Пользователь вводит данные в веб-форму на сайте, и мошенники получают доступ к деньгам пользователя. Заражение компьютера вирусами и вредоносными приложениями – еще одна ловушка, которая может поджидать пользователя, перешедшего по фишинговой ссылке.

Как распознать мошеннические письма и сайты

Мошеннические письма и сайты на первый взгляд ничем себя не выдают. Усыпляет бдительность наличие логотипов организаций, идентичных настоящим, или официальных контактных номеров телефонов. В письме могут содержаться ссылки, ведущие на официальный сайт, за исключением основной фишинговой ссылки, по которой пользователь и должен будет пройти на сайт злоумышленника.

Насторожить пользователя могут следующие признаки фишинга:

- Домены фишинговых сайтов внешне похожи на настоящие. Однако, внимательно присмотревшись, пользователь может заметить лишние слова (например, официальный домен www.example.com изменен на www.login-example.com), точки или тире вместо слешей (www.example.com/personal/login изменен на www.example.com.personal.login или www.example.com-personal.login). Стоит обратить внимание, что в теле письма может быть указан настоящий домен организации, но когда пользователь перейдет по ссылке, в адресной строке домен будет иным.

- В электронном письме используется неличное обращение, например "Уважаемый пользователь!" или "Здравствуйте!".

- Графика в электронном письме или на сайте выполнена непрофессионально, в тексте встречаются грамматические ошибки.

- Получателя электронного письма просят незамедлительно подтвердить конфиденциальные данные, пройдя по ссылке, а иногда ввести данные прямо в письме. Причиной такой срочности может быть якобы блокировка или взлом аккаунта, угроза потери данных.

Проверка на фишинг

В приложении Kaspersky Small Office Security предусмотрена проверка содержимого электронных писем и веб-ресурсов на наличие фишинговых ссылок. Ссылки проверяются по базе фишинговых веб-адресов и поддельных криптовалютных бирж, которая регулярно обновляется.

Для дополнительной защиты во время проверки используется эвристический анализ, а также осуществляются запросы к облачным службам Kaspersky Security Network (KSN). Kaspersky Security Network содержит самые актуальные данные о недавно появившихся угрозах, в том числе о фишинговых веб-ресурсах, которые еще не успели попасть в базы "Лаборатории Касперского". Данные, поступающие в KSN, анализируются сотрудниками Вирусной лаборатории в режиме реального времени.

Если вы попали на фишинговый сайт, вы можете сообщить о нем в Kaspersky Security Network с помощью расширения Kaspersky Protection.

О криптоджекинге

Криптоджекинг – это вид киберпреступления, которое заключается в использовании чужих устройств (компьютеров, планшетов, смартфонов и серверов) без ведома их владельцев для скрытого создания (майнинга) криптовалют, например, биткоина.

Как работает криптоджекинг

Преступник взламывает устройство и устанавливает на него специальное программное обеспечение, которое работает в фоне и не вызывает никаких подозрений у пользователя.

Вредоносный код устанавливается следующими способами:

- Пользователь проходит по фишинговой ссылке в почтовом сообщении, в результате чего на устройство загружается код, предназначенный для майнинга.
- Пользователь переходит на сайт, на котором загружаются якобы рекламные баннеры, которые при открытии запускают вредоносный код (JavaScript).

Когда программное обеспечение, предназначенное для криптоджекинга, установлено на устройстве, начинается процесс майнинга, то есть создания криптовалюты. Майнинг требует значительных вычислительных мощностей, что негативно сказывается на работе устройства.

В чем опасность криптоджекинга

Хотя криптоджекинг и не вредит напрямую операционной системе и данным пользователя, он все же может представлять значительную угрозу. Например, криптоджекинг может вызвать перегрев устройства и привести к поломке компьютера или сокращению срока его службы.

Как распознать криптоджекинг

О криптоджекинге могут сигнализировать следующие признаки:

- **Снижение скорости работы устройства**. Криптоджекинг можно заподозрить, если снизилось быстродействие операционной системы, стали медленнее запускаться приложения, быстро расходуется заряд батареи или устройство начало выключаться без видимой причины.
- **Перегрев устройства**. Криптоджекинг расходует большое количество ресурсов, что может приводить к перегреву устройства. Постоянный шум вентиляторов охлаждения может быть признаком того, что на устройстве запущено программное обеспечение, предназначенного для криптоджекинга.
- **Возросшая нагрузка на центральный процессор**. Если вы заходите на сайт, на котором нет видео или аудио-контента, при этом нагрузка на центральный процессор возрастает, это может свидетельствовать о том, что на этом сайте запущен скрипт для криптоджекинга. Проверить уровень загрузки процессора вы можете в Диспетчере задач на закладке **Производительность**.

Как защититься от криптоджекинга

Приложение Kaspersky Small Office Security включает инструменты, которые помогут защитить ваше устройство от криптоджекинга. Сайты, которые вы посещаете, проверяются на наличие встроенного вредоносного кода. В случае обнаружения попытки криптоджекинга, приложение показывает уведомление, в котором вы сможете удалить вредоносный код.

Ссылки проверяются по базе фишинговых веб-адресов и поддельных криптовалютных бирж, которая регулярно обновляется. При попытке перейти по вредоносной ссылке, приложение покажет предупреждение.

Даже если код для криптоджекинга попадет на устройство, приложение Kaspersky Small Office Security определит его как вредоносный и заблокирует его запуск.

Для дополнительной защиты во время проверки используется эвристический анализ, а также осуществляются запросы к облачным службам Kaspersky Security Network (KSN). Kaspersky Security Network содержит самые актуальные данные о недавно появившихся угрозах, в том числе об угрозах криптоджекинга.

О криптомошенничестве

Мошенничество с криптовалютой – это вид киберпреступлений, целью которых является кража криптовалюты, например, биткоинов. За первую половину 2022 года приложения "Лаборатории Касперского" обнаружили почти 200 000 попыток кражи криптовалют и данных криптокошельков пользователей.

Виды криптомошенничества

Существуют следующие виды мошенничества с криптовалютой:

- **Поддельные сайты и криптокошельки**. Мошенники создают поддельный сайт известной криптовалютной биржи или поддельный криптокошелек. Отличить подобный сайт от настоящего не всегда возможно, так как доменное имя и оформление сайта похожи на настоящие. Пользователь заходит на такой сайт и вводит свои данные, которые в итоге попадают в руки мошенников.

- **Криптофишинг**. Мошенники создают фишинговые ссылки, которые ведут на поддельные сайты, криптовалютные биржи и инвестиционные площадки. Затем рассылают их в почтовых сообщениях, а также размещают на других сайтах. Пользователи переходят по таким ссылкам, в результате чего теряют свои данные или средства.

- **Поддельные инвестиции в "новую" криптовалюту**. Мошенники создают фиктивное коммерческое предложение о начале инвестиций в новый проект, например, создание новой криптовалюты. Заинтересованные пользователи переводят средства на указанный криптокошелек, однако никакой новой криптовалюты не создается, а вложенные средства не возвращаются.

- **Поддельные инвестиции в криптовалюте**. Мошенники размещают рекламу в социальных сетях о выгодных вложениях в криптовалюте, обещая увеличить сумму вложений в несколько раз. Вместо полученной выгоды пользователи теряют вложенные средства.

- **Мошенничество при покупке оборудования для майнинга**. Пользователи переводят средства на покупку оборудование для создания (майнинга) криптовалюты, но не получают обещанный товар.

- **Поддельные сайты покупки криптовалют**. Мошенники создают сайт, на котором вы якобы можете приобрести криптовалюту за обычные деньги по хорошему курсу. Вы переводите свои средства, но не получаете криптовалюту.

- **Создание ажиотажного спроса на криптовалюту**. Мошенники создают массированную рекламную компанию по раскрутке какой-либо одной криптовалюты. При этом они обещают, что цена на эту криптовалюту будет расти. Инвесторы в спешке скупают рекламируемую криптовалюту. Затем мошенники быстро продают эту валюту по высокой цене в большом объеме, в результате чего цена на эту криптовалюту может упасть ниже начальной в течение нескольких минут.

Как защититься от мошенничества с криптовалютой

Приложение Kaspersky Small Office Security включает инструменты, которые помогут вам защититься от мошенничества с криптовалютой. Приложение определит, что сайт или криптовалютная биржа является поддельной и уведомит вас об этом.

Ссылки на сайтах и в почтовых сообщениях проверяются по базе фишинговых веб-адресов и поддельных криптовалютных бирж, которая регулярно обновляется. При попытке перейти по вредоносной ссылке, приложение покажет предупреждение.

Для дополнительной защиты во время проверки используется эвристический анализ, а также осуществляются запросы к облачным службам Kaspersky Security Network (KSN). Kaspersky Security Network содержит самые актуальные данные о недавно появившихся угрозах, в том числе об угрозах криптомошенничества.

Профиль

Подключение устройства к Центру управления Kaspersky Small Office Security

В аккаунте Центр управления Kaspersky Small Office Security вы можете просматривать состояние всех устройств, на которых установлено приложение, управлять защитой этих устройств удаленно, управлять лицензиями и хранить коды активации в безопасном месте.

Войти

При нажатии на кнопку открывается окно подключения устройства к аккаунту Центр управления Kaspersky Small Office Security. Кнопка доступна, если вы еще не подключили устройство к вашему аккаунту Центр управления Kaspersky Small Office Security или не подтвердили, что это ваше устройство.

Управлять аккаунтом

При нажатии на кнопку в браузере по умолчанию открывается ваш аккаунт на сайте Центр управления Kaspersky Small Office Security. Кнопка доступна после того, как вы войдете в аккаунт на этом устройстве.

Выйти

При нажатии на кнопку устройство будет отключено от аккаунта Центр управления Kaspersky Small Office Security. Кнопка доступна, если устройство подключено к аккаунту Центр управления Kaspersky Small Office Security.

Подробнее об аккаунте и удаленном управлении защитой компьютеров

Информация о лицензии

Здесь вы можете посмотреть статус лицензии, по которой работает ваше приложение, и количество дней, оставшихся до окончания оплаченного периода.

Подробнее

При нажатии на кнопку открывается окно **Информация о лицензии** с детальной информацией о вашей лицензии. Здесь вы можете найти следующую информацию:

- статус лицензии;
- лицензионный ключ, который может понадобиться при обращении в Службу технической поддержки;
- ссылку на Лицензионное соглашение;
- ссылку на Положение о Веб-Портале;
- дату активации;
- дату истечения срока действия оплаченного периода.

Чтобы открыть другие доступные действия с вашей лицензией, нажмите на кнопку ••• . В зависимости от вашей лицензии и ее статуса список доступных действий различается.

Обновить статус

При нажатии на кнопку можно получить актуальную информацию о статусе вашей лицензии.

Ввести код активации

По кнопке открывается окно ввода кода активации.

Сохранить код активации

При нажатии на эту кнопку открывается окно, в котором вы можете сохранить новый код активации в своем аккаунте Центра управления Kaspersky Small Office Security. В зависимости от вашей лицензии кнопка может быть недоступна.

Более подробную информацию смотрите в разделе Продление лицензии с помощью нового кода активации.

Выбрать другую лицензию

По кнопке открывается окно со списком лицензий, доступных в аккаунте Центр управления Kaspersky Small Office Security и совместимых с вашим приложением.

Кнопка доступна, если устройство подключено к аккаунту Центр управления Kaspersky Small Office Security.

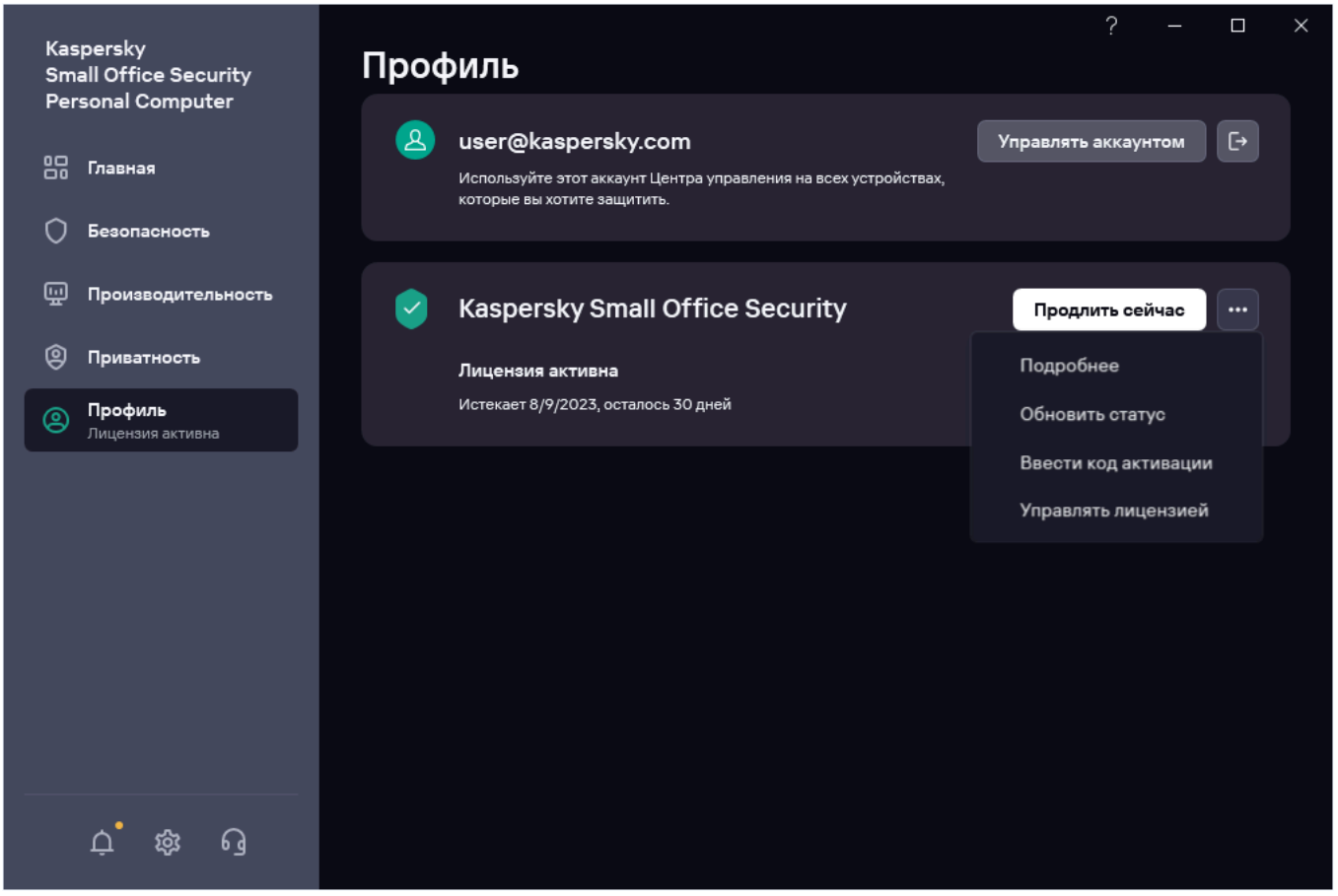
Управлять лицензией

По кнопке открывается ваш аккаунт Центр управления Kaspersky Small Office Security на странице управления лицензией. Кнопка доступна, если вы подключили устройство к аккаунту Центр управления Kaspersky Small Office Security.

Продлить сейчас / Купить сейчас

В зависимости от статуса вашей лицензии вы можете продлить текущую лицензию или купить новую лицензию. Кнопка доступна, если срок действия вашей лицензии истек.

Подробнее о лицензировании приложения



Окно Профиль

Получить разрешение на выполнение действия

В этом окне вы можете выбрать, разрешить приложению выполнить указанное действие или нет.

Можно выбрать один из следующих вариантов:

Запомнить выбор для этого приложения

Эта опция определяет, следует ли запомнить ваш выбор для этого приложения или спрашивать каждый раз.

Разрешить сейчас

Нажатие этой кнопки дает приложению разрешение на выполнение указанного действия.

Запретить сейчас

Нажатие этой кнопки не позволяет приложению выполнить указанное действие.

Дополнительные действия

При нажатии на эту ссылку раскрывается список дополнительных действий.

Сделать доверенным

Нажатие этой кнопки добавляет приложение в список доверенных приложений.

Закрыть и сделать недоверенным

Нажатие этой кнопки закрывает приложение. Приложение не считается доверенным.

Запускается малоизвестное приложение

Это сообщение уведомляет вас о том, что запускается малоизвестное приложение, по которому собрано недостаточно статистики. Вы можете принять решение, разрешить ли запуск приложения на вашем компьютере.

Можно выбрать один из следующих вариантов:

Запустить приложение как доверенное

Нажатие этой кнопки позволяет приложению запускаться на вашем компьютере без каких-либо ограничений. Приложение считается доверенным.

Запустить, ограничив опасную активность

Нажатие этой кнопки позволяет приложению запуститься на вашем компьютере с ограничением опасных действий, которые может выполнять приложение.

Заблокировать запуск

Нажатие этой кнопки предотвратит запуск приложения на вашем компьютере.

Сканирование домашней сети

В этом окне вы можете подтвердить, является ли обнаруженная сеть вашей домашней сетью, чтобы приложение могло проверить ее безопасность.

Можно выбрать один из следующих вариантов:

Да

Нажатие этой кнопки подтверждает, что обнаруженная сеть является вашей домашней сетью.

Нет

Нажатие этой кнопки подтверждает, что обнаруженная сеть не является вашей домашней сетью.

Показывать информацию об устройствах в сети на моих мобильных устройствах

Выбор этого действия позволяет приложению Kaspersky Small Office Security отображать информацию о других устройствах в обнаруженной сети на ваших мобильных устройствах.

Изменились условия обработки данных

Это сообщение уведомляет вас об изменении условий обработки данных.

Хорошо

Нажатие на эту кнопку подтверждает, что вы осведомлены об изменении условий обработки данных.

Восстановить файлы из резервной копии

В этом окне вы можете восстановить файл из резервной копии.

Выберите один из предложенных вариантов действия:

Заменить файл резервной копией

При нажатии на эту кнопку приложение сохраняет существующий файл и помещает на его место файл, восстановленный из резервной копии.

Не восстанавливать этот файл

При нажатии на эту кнопку приложение оставляет существующий файл без изменений, не восстанавливая одноименный файл из резервной копии.

Сохранить оба файла

При нажатии на эту кнопку приложение оставляет существующий файл без изменений и сохраняет файл, восстановленный из резервной копии, под новым именем в этой же папке.

Применять это действие во всех подобных случаях

Если флажок установлен, приложение выполняет выбранное действие в отношении всех восстанавливаемых файлов.

Если у вас возникли проблемы при попытке восстановить файлы из резервной копии, выполните одно из следующих действий:

Повторить попытку

Нажатие на эту кнопку перезапускает текущее действие (извлечение данных из резервного хранилища, сохранение файла и т. д.).

Не восстанавливать этот файл

При нажатии на эту кнопку приложение оставляет существующий файл без изменений, не восстанавливая одноименный файл из резервной копии.

Остановить задачу

При нажатии на кнопку приложение прекращает восстановление файлов из резервных копий.

Повторное сканирование после обновления баз и модулей приложения

Это сообщение уведомляет вас о том, что базы данных и модули приложения требуют обновления. В этом окне вы можете выбрать, проверять ли компьютер после обновления баз и модулей приложения Kaspersky Small Office Security или проверять компьютер не дожидаясь обновления.

Можно выбрать один из следующих вариантов:

Запустить проверку после обновления

Нажатие на эту кнопку запустит проверку вашего компьютера сразу после обновления баз и модулей приложения Kaspersky Small Office Security.

Запустить проверку сейчас

Нажатие на эту кнопку запускает проверку вашего компьютера сразу, не дожидаясь обновления баз и модулей приложения Kaspersky Small Office Security.

Требуется обновление баз и модулей приложения

В этом окне вы можете выбрать, устанавливать ли обновление баз и модулей для приложения Kaspersky Small Office Security или пропустить обновление.

Можно выбрать один из следующих вариантов:

Выполнить обновление

Нажатие на эту кнопку запустит установку обновления баз и модулей приложения Kaspersky Small Office Security.

Пропустить обновление

При нажатии на эту кнопку установка обновления баз и модулей приложения Kaspersky Small Office Security не производится.

Ручная активация приложения

В этом окне вы можете перейти к активации приложения Kaspersky Small Office Security или отложить активацию.

Можно выбрать один из следующих вариантов:

Использовать

При нажатии на эту кнопку запускается активация приложения Kaspersky Small Office Security с помощью введенного кода активации.

Позже

Нажатие на эту кнопку откладывает ручную активацию приложения Kaspersky Small Office Security и закрывает окно.

Да, активировать

При нажатии на эту кнопку запускается активация приложения Kaspersky Small Office Security с помощью введенного кода активации.

Нет, отложить активацию

Нажатие на эту кнопку откладывает ручную активацию приложения Kaspersky Small Office Security и закрывает окно.

Веб-страница пытается открыто передать пароль в сети Wi-Fi

В этом окне вы можете выбрать, разрешить ли передачу пароля в сети Wi-Fi или нет.

Можно выбрать один из следующих вариантов:

Запретить один раз

Нажатие этой кнопки блокирует передачу пароля в сети Wi-Fi.

Всегда разрешать для этого сайта

Нажатие этой кнопки позволяет передать пароль для указанного веб-сайта в сети Wi-Fi.

Обнаружено новое устройство

Это предупреждение уведомляет вас о том, что к вашей сети Wi-Fi подключено новое устройство.

Можно выбрать один из следующих вариантов:

Показать устройства

При нажатии на эту кнопку отображается список устройств, подключенных к вашей сети Wi-Fi.

Закрыть

Нажатие этой кнопки закрывает предупреждение.

Результаты проверки сети

Это предупреждение отображает результаты проверки сети.

Можно выбрать один из следующих вариантов:

Показать сейчас

При нажатии на эту кнопку отображается подробная информация о результатах проверки сети.

Проверять в фоне

Нажатие этой кнопки запустит проверку сети в фоновом режиме.

Узнать

Нажав эту кнопку, вы можете получить информацию о том, как исправить проблемы, обнаруженные в вашей сети.

Закрыть

Нажатие этой кнопки закрывает уведомление.

Проверка жесткого диска

Это предупреждение уведомляет о состоянии жесткого диска вашего компьютера.

Можно выбрать один из следующих вариантов:

Подробнее

При нажатии на эту кнопку отображается дополнительная информация о состоянии жесткого диска вашего компьютера.

Закрыть

Нажатие этой кнопки закрывает предупреждение.

Больше не показывать

Нажатие этой кнопки предотвращает повторное отображение этого предупреждения.

Пароль для архива

В этом окне предлагается указать пароль для архива.

Можно выбрать один из следующих вариантов:

OK

Нажимая на эту кнопку, вы подтверждаете пароль, который вы указали для архива.

Пропустить

Нажав эту кнопку, вы можете пропустить опцию указания пароля для архива.

Пропустить все

Нажатие на эту кнопку отключает отображение данного окна для всех архивов, защищенных паролем, обнаруженных во время текущего сеанса сканирования.

Обнаружено несовместимое программное обеспечение

Это предупреждение уведомляет вас об обнаружении несовместимого программного обеспечения.

Можно выбрать один из следующих вариантов:

Удалить сейчас

Нажав на эту кнопку, вы удалите найденное несовместимое программное обеспечение.

Не сейчас

Нажав на эту кнопку, вы откладываете удаление обнаруженного несовместимого программного обеспечения и закрываете предупреждение.

Обнаружено подозрительное поведение приложения

Это предупреждение уведомляет о том, что приложение было идентифицировано как вредоносное или рекламное программное обеспечение.

Можно выбрать один из следующих вариантов:

Для вредоносного программного обеспечения:

Лечить с перезагрузкой компьютера

Нажатие на эту кнопку лечит зараженный объект и перезагружает компьютер.

Попытаться вылечить без перезагрузки

Нажатие на эту кнопку позволяет вылечить зараженный объект без перезагрузки компьютера.

Для рекламного программного обеспечения:

Разрешить один раз

Нажатие этой кнопки дает одноразовое разрешение на запуск этого приложения на вашем компьютере.

Разрешить и добавить в исключения

При нажатии на кнопку обнаруженные рекламные приложения добавляются в список исключений из сканирования.

Закрыть и удалить приложение

Нажатие этой кнопки удаляет обнаруженное рекламное программное обеспечение с вашего компьютера и закрывает предупреждение.

О менеджере паролей

В этом сообщении отображается информация о Kaspersky Password Manager. Подробную информацию можно найти в онлайн справке для Kaspersky Password Manager.

Можно выбрать один из следующих вариантов:

Подробнее

При нажатии на эту кнопку будет отображена подробная информация о Kaspersky Password Manager.

Больше не напоминать

Нажатие этой кнопки отключает показ этого уведомления.

Установить

Нажатие этой кнопки запустит установку Kaspersky Password Manager на вашем компьютере.

Больше не показывать

Нажатие этой кнопки отключает показ этого уведомления.

Активировать

Нажатие этой кнопки активирует Kaspersky Password Manager на вашем компьютере, чтобы проверить ваши пароли на утечку и синхронизировать их на всех ваших устройствах.

Требуется перезапуск

Это сообщение уведомляет вас о необходимости перезапустить приложение Kaspersky Small Office Security или перезагрузить компьютер.

Можно выбрать один из следующих вариантов:

Перезапустить приложение Kaspersky Small Office Security

Да

Нажатие на эту кнопку перезапускает приложение Kaspersky Small Office Security, чтобы применить обновления.

Нет

Нажатие этой кнопки откладывает перезапуск приложения Kaspersky Small Office Security и закрывает уведомление.

Перезагрузить ваш компьютер:

Перезагрузить

Нажатие этой кнопки перезагружает ваш компьютер, чтобы отключить механизмы отладки.

Отложить

Нажатие этой кнопки откладывает перезагрузку вашего компьютера и закрывает уведомление.

Доступны новые обновления

Уведомление о том, что приложение Kaspersky Small Office Security обнаружило новые обновления для приложений, установленных на вашем компьютере.

Можно выбрать один из следующих вариантов:

Показать

При нажатии на эту кнопку отображается список доступных обновлений.

Не сейчас

Нажатие этой кнопки закрывает уведомление. Если вы нажмете стрелку вниз рядом с этой кнопкой, вы можете отложить оповещение на час, четыре часа или день.

Найдена новая проводная сеть Ethernet

Это сообщение информирует, что приложение Kaspersky Small Office Security обнаружило новую сеть Ethernet. Более подробную информацию смотрите в этой статье.

Можно выбрать один из следующих вариантов:

Нет, запретить доступ к компьютеру извне

Нажатие этой кнопки блокирует все внешние подключения указанной сети, кроме подключений, инициированных с вашего устройства.

Ограничить, разрешив общий доступ

Нажатие этой кнопки позволит вам пользоваться Интернетом и посещать все веб-сайты.

Да, разрешить любую сетевую активность

Эта опция разрешает все соединения в этой сети.

Выберите способ обработки обнаруженного программного обеспечения

В этом окне вы можете выбрать, как обрабатывать вредоносное, рекламное или легальное программное обеспечение, которое может быть использовано злоумышленниками для нанесения ущерба вашему компьютеру или личным данным.

Можно выбрать один из следующих вариантов:

Лечить

Нажатие на эту кнопку лечит зараженный объект.

Удалить

Нажатие этой кнопки удаляет обнаруженное программное обеспечение с вашего компьютера.

В случае удаления объекта приложение Kaspersky Small Office Security создает его резервную копию и помещает на карантин. При необходимости вы можете восстановить удаленные объекты из резервной копии.

Пропустить

При нажатии этой кнопки обнаруженное программное обеспечение пропускается.

После нажатия кнопки **Пропустить** уведомление об обнаруженном объекте останется в Центре уведомлений.

Для обработки объекта необходимо зайти в окно **Центр уведомлений**, нажать на кнопку **Устранить** рядом с объектом и выбрать один из доступных вариантов в раскрывающемся меню. Вы также можете удалить объект, если уверены, что он вам не нужен.

Добавить в исключения

При нажатии на кнопку обнаруженные приложения удаляются из списка исключений из проверки.

Применить ко всем объектам этого типа

Если выбран этот флажок, указанное действие будет применено ко всем объектам данного типа.

Попытка выполнить несанкционированное действие

Это предупреждение уведомляет вас, когда какое-либо приложение или процесс пытается выполнить несанкционированное действие.

Можно выбрать один из следующих вариантов:

Разрешить

Нажатие этой кнопки дает процессу или приложению разрешение на выполнение указанного действия.

Запретить

Нажатие этой кнопки не позволяет процессу или приложению выполнить указанное действие.

Включить Службы определения местоположения на компьютере под управлением Windows 11

На компьютерах под управлением Windows 11, необходимо включить **Службы определения местоположения**, чтобы приложение Kaspersky могло идентифицировать сети Wi-Fi.

Чтобы включить Службы определения местоположения:

1. Перейдите в раздел **Пуск** > **Параметры** > **Конфиденциальность & безопасность** > **Расположение**.
2. Включите настройку **Службы определения местоположения**.
3. Перезагрузите компьютер.