Kaspersky
Security Cloud

Содержание

Часто задаваемые вопросы

Начало работы

Как установить новую версию программы поверх старой

Как настроить рекомендуемые параметры программы во время установки

Как активировать программу

Как создать учетную запись My Kaspersky

Как удаленно управлять защитой ваших устройств

Отчеты и обновления

Как просмотреть отчет о работе программы

Как запустить обновление баз и модулей программы

Защита компьютера

Как посмотреть информацию о состоянии защиты компьютера

Как восстановить операционную систему после заражения

Как запустить полную проверку компьютера на вирусы

Как запустить быструю проверку компьютера на вирусы

Как настроить проверку на защищенных сайтах

Оптимизация работы операционной системы

Как очистить компьютер от редко используемых программ и расширений браузера

Как оптимизировать работу программы для компьютерных игр

Как применить настройки программы на другом компьютере

Как исправить небезопасные настройки операционной системы

Защита покупок и денежных переводов

Как защитить ваши покупки в интернете

Как настроить Безопасные платежи

Защита личных данных

Как проверить, была ли утечка информации о вас в интернет

Как настроить Безопасные платежи для определенного сайта

Как запретить сайтам собирать данные о вас

Как защитить ваши пароли в интернете

Как запустить программу защиты паролей Kaspersky Password Manager

Защита детей

Как защитить ваших детей от киберугроз

Как скачать и установить программу защиты детей Kaspersky Safe Kids

Адаптивная защита

Что такое Новости безопасности

Как защитить вашу домашнюю сеть Wi-Fi

Kaspersky Security Cloud

Kaspersky Security Cloud – это наше новое решение, основанное на запатентованной технологии адаптивной защиты. Программа подстраивается под ваши действия и дает персональные рекомендации о том, как лучше защитить себя и своих близких. Например, когда вы подключаетесь к сетям Wi-Fi, совершаете покупки и вводите пароли в интернете, программа предлагает вам включить наиболее подходящий для этого компонент защиты.

Вы можете использовать Kaspersky Security Cloud на устройствах на базе Microsoft Windows, macOS (недоступно в тарифном плане Free), Android и iOS.

При использовании Kaspersky Security Cloud ваше устройство должно быть подключено к учетной записи My Kaspersky. *My Kaspersky* – это единая учетная запись для управления защитой ваших устройств. Владелец подписки Family также может делиться защитой с членами своей семьи и друзьями. Каждому пользователю, защищенному по подписке Family, нужно будет создать свою учетную запись My Kaspersky.

Kaspersky Security Cloud имеет три тарифных плана.

Ознакомьтесь с Лицензионными соглашениями для программ из таблицы ниже .

Тарифный план Free	Тарифный план Personal	Тарифный план Family
защита до 3 устройств	защита от 3 до 5 устройств	защита до 10 устройств
Kaspersky Security Cloud (базовая защита)	Kaspersky Security Cloud (полная версия)	Kaspersky Security Cloud (полная версия)
Kaspersky Internet Security для Android (бесплатная версия)	Kaspersky Internet Security для Android (премиум-версия)	Kaspersky Internet Security для Android (премиум-версия)
Kaspersky Secure Connection* (стандартная версия)	Kaspersky Secure Connection* (стандартная версия)	Kaspersky Secure Connection* (стандартная версия)
Kaspersky Password Manager (бесплатная версия)	Kaspersky Password Manager (премиум-версия)	Kaspersky Password Manager (премиум-версия)
		Kaspersky Safe Kids (премиум-версия)

*Обратите внимание, что на мобильных устройствах программа Kaspersky Secure Connection входит в состав программы Kaspersky Security Cloud. Удалите программу Kaspersky Secure Connection, чтобы программа Kaspersky Security Cloud работала корректно. После удаления Kaspersky Secure Connection настройки программы не будут сохранены. Подписка на расширенную версию программы Kaspersky Secure Connection будет продолжать работать в программе Kaspersky Security Cloud.

Что нового

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

В Kaspersky Security Cloud появились следующие новые возможности и улучшения:

- Улучшен компонент Веб-Антивирус:

    - Улучшены тексты уведомлений при переходе на фишинговые и возможно фишинговые сайты.
    - При отключенной проверке HTTPS-трафика защита реализуется с помощью расширения Kaspersky Protection.
- Улучшено взаимодействие пользователя со Службой технический поддержки. В программу добавлена ссылка на чат со Службой технической поддержки (доступно не во всех версиях программы).
- Исправлена уязвимость при создании файлов браузера Mozilla Firefox.
- Обновлен значок программы-установщика в новой стилистике бренда.
- Оптимизирована работа компонента Устройства в моей сети. Запуск проверки сети выполняется через 15 минут после установки программы.
- Реализован переход на облегченную версию портала My Kaspersky из программы.
- Добавлена возможность скрывать окно проверки съемных дисков.
- Добавлена поддержка Microsoft Windows 10 21H1.
- Исправлена уязвимость произвольного удаления файлов при сохранении отчета о работе программы для Службы технической поддержки.
- Исправлена уязвимость произвольного удаления файлов при удалении служебной информации и отчетов о работе программы.
- Улучшен поиск несовместимого программного обеспечения, препятствующего корректной работе Kaspersky Security Cloud.
- Реализован режим работы программы "Не беспокоить". В этом режиме программа не показывает некоторые виды уведомлений, если пользователь занят.

Функциональность, удаленная в текущей и предыдущих версиях программы

Kaspersky Security Cloud 4:

- Удалена функциональность Application Advisor.
- Удалена функциональность IM-Антивирус.
- Удалена функциональность Режим безопасных программ.
- 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.

Kaspersky Security Cloud 2:

- В компоненте Менеджер программ удалена функциональность Контроль изменений настроек операционной системы.
- 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 программы.

Аппаратные и программные требования

Общие требования

- 1500 МБ свободного места на жестком диске.
- Процессор с поддержкой инструкций SSE2.
- Подключение к интернету (для установки и активации программы, использования Kaspersky Security Network, а также обновления баз и программных модулей).
- 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 .

Требования для операционных систем

Операционная система	Процессор	Свободная оперативная память	Ограничения
Microsoft Windows 11 Home	1 ГГц или выше	2 ГБ (для 64-разрядной операционной системы)	Kaspersky Security Cloud имеет следующие ограничения при установке на все версии Microsoft Windows 11:
Microsoft Windows 11 Enterprise			
Microsoft Windows 11 Pro			

			• 32-разрядная операционная система не поддерживается. • Подсистема Windows для Linux 2 (WSL2) не поддерживается. • В контекстном меню объектов не отображаются команды Kaspersky Security Cloud. Чтобы команды отображались, требуется развернуть меню.
Microsoft Windows 10 Home (версии: 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, 21H1, 21H2) Microsoft Windows 10 Enterprise (версии: 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, 21H1, 21H2) Microsoft Windows 10 Pro (версии: 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, 21H1, 21H2)	1 ГГц или выше	1 ГБ (для 32-разрядной операционной системы) или 2 ГБ (для 64-разрядной операционной системы)	Kaspersky Security Cloud имеет следующие ограничения при установке на Microsoft Windows 10: 32-разрядная операционная система не поддерживается в версии 21H2.
Microsoft Windows 8.1 (Service Pack 0 или выше, Windows 8.1 Update) Microsoft Windows 8.1 Pro (Service Pack 0 или выше, Windows 8.1 Update) Microsoft Windows 8.1 Enterprise	1 ГГц или выше	1 ГБ (для 32-разрядной операционной системы) или 2 ГБ (для 64-разрядной операционной системы)	

(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)		
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)		
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)

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

Поддержка браузеров

Браузеры, которые поддерживают установку расширения Kaspersky Protection:

- Microsoft Edge на базе Chromium 77.x – 88.x;
- Mozilla Firefox версий 52.x – 84.x;
- Mozilla Firefox ESR 52.x, 60.x, 68.x, 78.x;
- Google Chrome версий 48.x – 88.x.

Браузеры, которые поддерживают Экранную клавиатуру и Проверку защищенных соединений:

- Microsoft Edge на базе Chromium 77.x – 88.x;
- Mozilla Firefox версий 52.x – 84.x;

- Mozilla Firefox ESR 52.x, 60.x, 68.x, 78.x;
- Google Chrome 48.x – 88.x.

Браузеры, которые поддерживают режим Защищенного браузера:

- Microsoft Internet Explorer 8.0, 9.0, 10.0, 11.0;
- Microsoft Edge на базе Chromium 77.x – 88.x;
- Mozilla Firefox версий 52.x – 84.x;
- Mozilla Firefox ESR 52.x, 60.x, 68.x, 78.x;
- Google Chrome 48.x – 88.x;
- Яндекс.Браузер 18.3.1 – 20.12.0 (есть ограничения).

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

Kaspersky Security Cloud 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 8, Microsoft Windows 8.1, Microsoft Windows 10;
- процессор Intel Celeron 1.66 ГГц или выше;
- 1000 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 1024x600;
- графический чипсет Intel GMA 950 или выше.

Требования для программы Kaspersky Password Manager вы можете найти в справке к этой программе.

Совместимость с другими программами "Лаборатории Касперского"

Программа Kaspersky Security Cloud совместима со следующими программами "Лаборатории Касперского":

- Kaspersky Safe Kids 1.5;
- Kaspersky Password Manager 9.2;
- Kaspersky Software Updater 2.1;
- Kaspersky Virus Removal Tool 2015, 2020;
- Kaspersky Secure Connection 4.0, 5.0, 5.1, 5.2, 5.3.

Как установить программу

Kaspersky Security Cloud устанавливается на компьютер в интерактивном режиме с помощью мастера установки и удаления.

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 шаге установки следует закрыть окно мастера.

Количество и последовательность шагов мастера зависит от региона, в котором вы устанавливаете программу. В некоторых регионах мастер предложит вам принять дополнительные соглашения на обработку персональных данных.

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

Чтобы установить Kaspersky Security Cloud на ваш компьютер,

на установочном диске запустите файл с расширением exe.

Далее установка программы выполняется с помощью стандартного мастера установки и удаления.

В некоторых регионах установочный диск не содержит установочного пакета программы. На установочном диске содержится только файл autorun, при запуске которого открывается окно загрузки программы.

Как установить программу с помощью файла autorun

Чтобы установить Kaspersky Security Cloud с помощью файла autorun, выполните следующие действия:

1. В окне загрузки программы нажмите на кнопку **Скачать и установить**.

   При нажатии на кнопку **Скачать и установить** в "Лабораторию Касперского" отправляется информация о версии вашей операционной системы.

2. Если скачать программу не удалось, по ссылке **Скачать с сайта и установить вручную** перейдите на веб-страницу и скачайте программу вручную.

Далее установка программы выполняется с помощью стандартного мастера установки и удаления.

Для установки Kaspersky Security Cloud вы также можете самостоятельно скачать установочный пакет из интернета. При этом для некоторых языков локализации мастер отображает несколько дополнительных шагов установки.

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

При первом запуске программы Kaspersky Security Cloud с момента ее установки воспроизведение или запись аудио и видео могут быть прерваны в программах записи или воспроизведения аудио и видео. Это необходимо для того, чтобы включилась функциональность контроля доступа программ к устройствам записи звука. Системная служба управления средствами работы со звуком будет перезапущена при первом запуске программы Kaspersky Security Cloud.

Вместе с Kaspersky Security Cloud устанавливается программа Kaspersky Secure Connection, предназначенная для включения безопасного VPN-соединения с помощью Virtual Private Network (VPN). Вы можете удалить Kaspersky Secure Connection независимо от программы Kaspersky Security Cloud. Если в вашей стране запрещено использование VPN, программа Kaspersky Secure Connection не устанавливается.

Поиск более новой версии программы

Перед началом установки мастер проверяет наличие более актуальной версии Kaspersky Security Cloud на серверах обновлений "Лаборатории Касперского".

Если мастер не обнаружит на серверах обновлений "Лаборатории Касперского" более актуальную версию программы, он запустит установку текущей версии.

Если мастер обнаружит на серверах обновлений "Лаборатории Касперского" более актуальную версию Kaspersky Security Cloud, он предложит вам скачать и установить ее на ваш компьютер. Рекомендуется устанавливать новую версию программы, так как в новые версии вносятся улучшения, позволяющие более эффективно защищать ваш компьютер. Если вы откажетесь от установки новой версии, мастер запустит установку текущей версии программы. Если вы согласитесь установить новую версию программы, мастер скопирует файлы установочного пакета на ваш компьютер и запустит установку новой версии.

Начало установки программы

На этом шаге мастер предлагает вам установить программу.

Для продолжения установки нажмите на кнопку **Продолжить**.

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 Kaspersky Security Cloud с установочного пакета, полученного 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 **Принять**. Установка программы на ваш компьютер будет продолжена.

Если условия Лицензионного соглашения не приняты, установка программы не производится.

В некоторых регионах для продолжения установки программы вы также должны принять условия Политики конфиденциальности.

Положение 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 программах и о скачиваемых подписанных программах, 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 программы продолжится.

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

Установка программы

Для некоторых версий Kaspersky Security Cloud, распространяемых по подписке, перед установкой требуется ввести пароль, предоставленный поставщиком услуг.

После ввода пароля начинается установка программы.

Установка программы занимает некоторое время. Дождитесь ее завершения.

По завершении установки мастер автоматически переходит к следующему шагу.

Проверки во время установки программы

Во время установки Kaspersky Security Cloud 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 программ;
  - наличие необходимого для установки свободного места на диске;
  - наличие прав администратора у пользователя, выполняющего установку программы.

  Если какое-либо из перечисленных условий не выполнено, на экран будет выведено соответствующее уведомление.

- *Наличие на компьютере несовместимых программ*. При обнаружении несовместимых программ их список будет выведен на экран, и вам будет предложено удалить их. Программы, которые Kaspersky Security Cloud не может удалить автоматически, нужно удалить вручную.

Во время удаления несовместимых программ потребуется перезагрузка операционной системы, после чего установка Kaspersky Security Cloud продолжится автоматически.

Установка Kaspersky Password Manager

Перед завершением установки Kaspersky Security Cloud предложит вам установить также программу защиты паролей Kaspersky Password Manager. Установка Kaspersky Password Manager может продолжаться после завершения установки Kaspersky Security Cloud, отдельного уведомления о завершении установки Kaspersky Password Manager не выводится.

Рекомендуемые настройки

На этом шаге вы можете просмотреть и изменить настройки Kaspersky Security Cloud, которые специалисты "Лаборатории Касперского" рекомендуют включить до начала использования программы.

Чтобы изменить рекомендуемые настройки, выполните следующие действия:

1. Выберите, какие настройки вы хотите включить или выключить:

   - Оставьте установленным флажок **Включить защиту от рекламных предложений, чтобы устанавливать только нужные программы и блокировать дополнительные установки**, если вы часто скачиваете и устанавливаете программы из интернета. Это поможет вам избежать установки лишних программ.

   - Оставьте установленным флажок **Удалять вредоносные утилиты, рекламные программы, программы автодозвона и подозрительные упаковщики**, если вы хотите, чтобы программа удаляла возможно зараженные объекты.

   - Оставьте установленным флажок **Обнаруживать другие программы, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя**, если вы часто устанавливаете новые программы. Это поможет вам обнаруживать программы, которые могут быть использованы для нанесения вреда компьютеру или вашим данным.

- Оставьте установленным флажок **Посмотреть обзор возможностей программы**, чтобы ознакомиться с новыми и основными возможностями программы.

Если вы не хотите включать рекомендуемые "Лабораторией Касперского" настройки, снимите соответствующие флажки.

2. Нажмите на кнопку **Применить**.

Завершение установки

На этом шаге мастер информирует вас о завершении установки программы.

Нажмите на кнопку **Готово**.

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

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

Подключение к My Kaspersky

Для активации программы вам нужно войти в свою учетную запись My Kaspersky и тем самым подключиться к My Kaspersky. Программа Kaspersky Security Cloud не работает, если ваше устройство не подключено к My Kaspersky. Программа автоматически подключается к My Kaspersky, если ранее вы вводили свои учетные данные в другой программе "Лаборатории Касперского" на данном устройстве. Если программе не удалось автоматически подключить ваше устройство к My Kaspersky, вам нужно вручную ввести данные для входа.

Если у вас есть учетная запись My Kaspersky, выполните следующие действия:

1. Введите адрес электронной почты, который вы использовали при создании учетной записи.

2. Введите пароль от вашей учетной записи.

3. Введите код с картинки и нажмите на кнопку **Продолжить**.

   Этот шаг доступен, если вы несколько раз неправильно ввели адрес электронной почты или пароль.

4. Если на My Kaspersky вы настроили авторизацию по SMS, на ваш телефон будет отправлено сообщение с кодом авторизации. Введите код авторизации в поле ввода и нажмите на кнопку **Продолжить**.

   Если сообщение с кодом авторизации не доставлено, выберите одно из действий:

   - Нажмите на кнопку **Получить новый код** для повторной отправки кода.
   - Нажмите на кнопку **Не получили код**, чтобы прочитать о том, как можно решить эту проблему.

   > В некоторых регионах программа предложит вам прочитать и принять положение о предоставлении данных. Если вы согласны с условиями положения, нажмите на кнопку **Принять и подключить**.

   Программа будет подключена к My Kaspersky.

   - Если вы уже купили подписку и ввели код активации на My Kaspersky, при подключении к My Kaspersky программа будет активирована по подписке.
   - Если программа определила, что у вас есть несколько активных подписок, например на Kaspersky Security Cloud – Personal и Kaspersky Security Cloud – Family, откроется окно **Выберите подписку**. Нажмите на кнопку **Выбрать**, чтобы выбрать подписку, по которой вы будете использовать программу Kaspersky Security Cloud.

   > Если вы еще не купили подписку, программа будет активирована по тарифному плану Kaspersky Security Cloud – Free.

Если у вас нет учетной записи на My Kaspersky

Если у вас нет учетной записи на My Kaspersky, выполните следующие действия:

1. Введите адрес электронной почты в поле **Адрес электронной почты** и нажмите на кнопку рядом с полем ввода.

2. Если программа не определила автоматически ваш регион, вам будет предложено его выбрать. От выбранного региона зависит, какие программы и какие способы оплаты вы сможете использовать. Выберите ваш регион и нажмите **Подтвердить**.

3. Введите пароль в поле **Пароль** и нажмите на кнопку рядом с полем ввода.

   Пароль должен состоять не менее чем из 8 символов, содержать хотя бы одну цифру, заглавную и строчную буквы.

4. Установите флажок **Я соглашаюсь предоставить "Лаборатории Касперского" адрес своей электронной почты для получения персональных маркетинговых предложений**, если вы хотите получать уведомления от "Лаборатории Касперского" на адрес электронной почты.

   В некоторых версиях программы этот флажок называется **Я подтверждаю, что разрешаю АО "Лаборатория Касперского" использовать мой адрес электронной почты, имя и фамилию, чтобы оповещать меня по электронной почте о персонализированных специальных предложениях, обзорах, опросах, напоминать о незавершенных заказах, отправлять актуальные новости и события** или **Я подтверждаю, что разрешаю АО "Лаборатория Касперского" использовать мой адрес электронной почты, чтобы оповещать меня по электронной почте о персонализированных специальных предложениях, обзорах, опросах, напоминать о незавершенных заказах, отправлять актуальные новости и события.**

5. Укажите свое имя в поле **Ваше имя**.

6. Укажите свою фамилию в поле **Ваша фамилия**.

7. Нажмите на кнопку **Создать**.

   На указанный вами адрес электронной почты будет отправлено письмо со ссылкой, по которой необходимо перейти для активации учетной записи My Kaspersky.

8. Перейдите по ссылке для активации учетной записи My Kaspersky в полученном письме.

Состав полей при создании учетной записи формируется специалистами "Лаборатории Касперского" и может меняться.

Активация программы

Для того чтобы пользоваться функциями программы и связанными с программой дополнительными услугами, нужно активировать программу.

Активация программы выполняется на My Kaspersky. Если вы приобрели подписку на сайте My Kaspersky, программа активируется автоматически, когда вы подключаете устройство к My Kaspersky.

Если вы приобрели подписку на программу способом, который не предполагает автоматическую активацию программы, вам нужно добавить код активации на сайте My Kaspersky.

Чтобы добавить код активации Kaspersky Security Cloud, выполните следующие действия:

1. Войдите на My Kaspersky .
2. Перейдите в раздел **Лицензии**.
3. В разделе **Лицензии** введите код активации для программы Kaspersky Security Cloud.
4. Нажмите на кнопку **Добавить**.

   Программа будет активирована автоматически, когда вы подключите устройство к My Kaspersky.

Если вы купили программу в коробке, следуйте инструкции, которая входит в поставку.

Завершение активации

Мастер информирует вас об успешном завершении активации Kaspersky Security Cloud.

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

Ошибка установки программы на операционных системах Windows 7 и Windows Server 2008 R2

Программа Kaspersky Security Cloud не может быть установлена на операционные системы Microsoft Windows 7 и Microsoft Windows Server 2008 R2, если не установлены следующие обновления операционной системы:

1. KB4490628 (обновление от 12 марта 2019);
2. KB4474419 (обновление от 23 сентября 2019).

Ошибка установки появляется в связи с тем, что компания Microsoft обновила алгоритм подписания модулей и драйверов сторонних программ. Теперь модули и драйверы сторонних программ (в том числе "Лаборатории Касперского") подписываются с помощью алгоритма хеширования SHA256. Вам необходимо установить обновления KB4490628 и KB4474419, чтобы модули и драйверы Kaspersky Security Cloud могли быть подписаны с помощью алгоритма хеширования SHA256.

Вы можете установить обновления следующими способами.

Установка обновления через Центр обновления Windows

Если на вашем компьютере отключена автоматическая установка обновлений, выполните следующие действия:

1. В меню **Пуск** выберите пункт **Панель управления** → **Система и безопасность** → **Центр обновления Windows**.

Откроется окно **Центр обновления Windows**.

2. В окне **Центр обновления Windows** в меню слева выберите пункт **Настройка параметров**.
3. В открывшемся окне в блоке **Важные обновления** выберите пункт **Устанавливать обновления автоматически (рекомендуется)**.

Все необходимые обновления будут автоматически скачаны и установлены на вашем компьютере.

Установка обновления Service Pack 1 вручную, если оно не установлено

Если ваш компьютер работает на базе операционной системы Windows 7 Service Pack 0 или Windows Server 2008 R2 Service Pack 0, сначала необходимо установить обновление Service Pack 1 (KB976932).

Чтобы установить обновление Service Pack 1, выполните следующие действия:

1. Перейдите по ссылке в каталог обновлений Microsoft .
2. Выберите версию операционной системы вашего компьютера и нажмите на кнопку **Download**.
3. Скачайте обновление к себе на компьютер по ссылке в открывшемся окне.
4. Установите обновление.

Установка обновления KB4490628 вручную

Чтобы установить обновление KB4490628 вручную, выполните следующие действия:

1. Перейдите по ссылке в каталог обновлений Microsoft .

2. Выберите версию операционной системы вашего компьютера и нажмите на кнопку **Download**.

3. Скачайте обновление к себе на компьютер по ссылке в открывшемся окне.

4. Установите обновление.

Установка обновления KB4474419 вручную

Чтобы установить обновление KB4474419 вручную, выполните следующие действия:

1. Перейдите по ссылке в каталог обновлений Microsoft .

2. Выберите версию операционной системы вашего компьютера и нажмите на кнопку **Download**.

3. Скачайте обновление к себе на компьютер по ссылке в открывшемся окне.

4. Установите обновление.

После установки обновлений перезагрузите компьютер и запустите установку программы Kaspersky Security Cloud заново.

Как обновить программу

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

Также программа автоматически обновляется, если вы устанавливаете новую версию программы поверх старой.

При наличии действующей подписки на предыдущую версию Kaspersky Security Cloud вам не понадобится активировать программу: мастер установки и удаления автоматически получит информацию о подписке на использование предыдущей версии Kaspersky Security Cloud и применит ее во время установки Kaspersky Security Cloud.

Во время скачивания обновления программа 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, программа предложит вам заново прочитать и принять их.

Программа может быть обновлена, если на вашем компьютере установлены следующие версии Kaspersky Security Cloud:

- Kaspersky Security Cloud 1;
- Kaspersky Security Cloud 2;
- Kaspersky Security Cloud 3.

Ограничения при обновлении предыдущей версии программы

Обновление программы Kaspersky Security Cloud имеет следующие ограничения:

- При обновлении предыдущей версии Kaspersky Security Cloud следующие настройки программы заменяются настройками по умолчанию:
  - настройки отображения Kaspersky Security Cloud;
  - расписание проверки;
  - участие в Kaspersky Security Network;
  - уровень защиты Файлового Антивируса;
  - уровень защиты Почтового Антивируса;
  - настройки Анти-Баннера;

- источники обновлений;
- список доверенных веб-адресов;
- настройки Проверки ссылок.

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

Установка поверх других программ "Лаборатории Касперского"

Программа может быть установлена поверх следующих программ "Лаборатории Касперского":

- Kaspersky Free;
- Kaspersky Anti-Virus;
- Kaspersky Internet Security;
- Kaspersky Total Security.

Во время установки Kaspersky Security Cloud удаляет установленную программу Kaspersky Anti-Virus, Kaspersky Internet Security или Kaspersky Total Security. Лицензия на удаленную программу не может быть применена в программе Kaspersky Security Cloud. Вы можете установить программу, которую вы удалили, на другое устройство и использовать по действующей лицензии. Настройки удаляемой программы не сохраняются.

Во время установки Kaspersky Security Cloud удаляет установленную программу Kaspersky Free. Настройки программы Kaspersky Free не сохраняются.

При установке Kaspersky Security Cloud поверх программы Kaspersky Total Security резервные копии файлов сохраняются, но не отображаются в Kaspersky Security Cloud. Вы можете добавить резервные копии файлов в Kaspersky Security Cloud вручную.

Установка программы из командной строки

Вы можете установить Kaspersky Security Cloud 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.

Как защитить ваше мобильное устройство

В вашем тарифном плане доступна защита мобильных устройств на операционных системах Android и iOS.

Чтобы защитить ваше мобильное устройство, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Защита смартфонов**.
3. Отсканируйте QR-код с помощью QR-сканера вашего мобильного устройства.

На вашем мобильном устройстве откроется магазин Google Play или App Store на странице загрузки программы "Лаборатории Касперского". После того как вы загрузите и установите программу на мобильное устройство, программа автоматически подключится к My Kaspersky и начнет защищать ваше устройство.

Как подготовить программу к работе

Для полноценной поддержки браузеров программой Kaspersky Security Cloud в браузерах должно быть установлено и включено расширение Kaspersky Protection. Kaspersky Security Cloud с помощью расширения Kaspersky Protection внедряет в веб-страницу, открытую в Защищенном браузере, и в трафик скрипт. Программа использует этот скрипт для взаимодействия с веб-страницей и для передачи данных в банки, чьи сайты защищаются с помощью компонента Безопасные платежи. Программа защищает передаваемые скриптом данные с помощью цифровой подписи. Kaspersky Security Cloud может внедрять скрипт без использования расширения Kaspersky Protection.

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

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

Расширение Kaspersky Protection не устанавливается в браузеры Microsoft Edge на базе Chromium, Mozilla Firefox и Google Chrome автоматически. Если в браузере не установлено расширение Kaspersky Protection, то при запуске браузера программа предложит вам перейти на страницу загрузки расширения и установить Kaspersky Protection вручную.

Поддержка Яндекс.Браузера

При использовании Яндекс.Браузера работают следующие компоненты программы:

- Защищенный браузер;
- Проверка ссылок;
- Веб-Антивирус;
- Анти-Фишинг.

Компоненты Защита от сбора данных и Анти-Баннер работают, но недоступны для настройки в Яндекс.Браузере.

Поддержка Internet Explorer

Начиная с версии Kaspersky Security Cloud 4, расширение Kaspersky Protection не поддерживает браузер Internet Explorer. Если вы хотите продолжать использовать расширение Kaspersky Protection в программе Internet Explorer, вы можете вернуться на предыдущую версию программы.

Как удалить программу

В результате удаления Kaspersky Security Cloud компьютер и ваши персональные данные окажутся незащищенными.

Удаление Kaspersky Security Cloud выполняется с помощью мастера установки и удаления.

Как удалить программу в операционной системе Windows 7

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

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

[Как удалить программу в операционной системе Windows 8 и выше]

Чтобы запустить мастер в операционной системе Microsoft Windows 8 и выше, выполните следующие действия:

1. На начальном экране по правой клавише мыши на плитке Kaspersky Security Cloud вызовите панель инструментов.
2. Нажмите на кнопку **Удалить** в панели инструментов.
3. В открывшемся окне выберите в списке Kaspersky Security Cloud.
4. Нажмите на кнопку **Удалить** в верхней части списка.

Ввод пароля для удаления программы

Чтобы удалить Kaspersky Security Cloud, требуется ввести пароль для доступа к настройкам программы. Если вы по каким-либо причинам не можете указать пароль, удаление программы будет невозможно.

Этот шаг отображается только в случае, если был установлен пароль на удаление программы.

Сохранение данных для повторного использования

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

Вы можете сохранить следующие данные:

- **Информация о лицензии** – данные, позволяющие в дальнейшем не активировать устанавливаемую программу, а использовать ее по уже действующей лицензии, если срок действия лицензии не истечет к моменту установки.

- **Файлы карантина** – файлы, проверенные программой и помещенные на карантин.

  > После удаления Kaspersky Security Cloud с компьютера файлы на карантине недоступны. Для работы с этими файлами нужно установить Kaspersky Security Cloud.

- **Настройки работы программы** – параметры работы программы, установленные во время ее 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.

- **Базы Анти-Спама** – базы с образцами спам-сообщений, добавленных пользователем.

- **Виртуальные сейфы** – файлы, которые вы помещали на хранение в сейфы.

Подтверждение удаления программы

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

Завершение удаления

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

После завершения удаления Kaspersky Security Cloud вы можете указать причины удаления программы на сайте "Лаборатории Касперского". Для этого требуется перейти на сайт "Лаборатории Касперского" по кнопке **Заполнить форму**.

> 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.

Лицензирование программы

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

О Лицензионном соглашении

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

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

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

О подписке

Подписка определяет настройки программы Kaspersky Security Cloud (срок действия подписки, количество защищаемых устройств). С подпиской связан уникальный код активации вашего экземпляра Kaspersky Security Cloud.

Существуют три вида тарифных планов:

Kaspersky Security Cloud – Free. Этот тарифный план дает вам право на использование базового набора функций защиты бесплатно. Вы можете устанавливать и использовать программу одновременно на трех устройствах, подключенных к одной учетной записи My Kaspersky. Подробно о том, какие функции защиты вы можете использовать на тарифном плане Free, вы можете прочитать в разделе Сравнение тарифных планов Kaspersky Security Cloud. Подписка на тарифный план Free продляется автоматически. Вам не требуется выполнять никаких действий.

- Kaspersky Security Cloud – Personal. Этот тарифный план дает вам право на использование всех функций программы, кроме защиты детей с помощью программы Kaspersky Safe Kids. Этот тарифный план рассчитан на использование программы одним человеком и не дает возможности поделиться программой с вашими друзьями или родственниками.

- Kaspersky Security Cloud – Family. Этот тарифный план дает вам право неограниченного использования всех функций программы, включая защиту детей с помощью программы Kaspersky Safe Kids. Если вы приобрели подписку на тарифный план Family, вы можете поделиться правом на использование программы с близкими людьми (друзьями, родственниками, коллегами по работе).

Тарифные планы Personal и Family имеют функцию автопродления подписки. Если вы активировали функцию автопродления на сайте нашего партнера или на сайте "Лаборатории Касперского", по истечении срока действия подписки она будет автоматически продлена без вашего участия. Подписка на тарифный план Free продляется автоматически. Вам не требуется выполнять никаких действий.

Если у вас не активирована функция автопродления или по каким-то причинам программе не удалось автоматически продлить вашу подписку (истек срок действия банковской карты или банковская карта была заблокирована), по окончании срока действия подписки на тарифные планы Personal или Family программа может перейти на тарифный план Free, если такой переход предусмотрен в вашем тарифном плане. В этом случае чтобы продолжить работу программы по тарифному плану Personal или Family, вам необходимо продлить подписку вручную на сайте "Лаборатории Касперского" или на сайте нашего партнера.

Подписка на тарифный план Personal и Family включают в себя право на получение следующих видов услуг:

- Использование программы на одном или нескольких устройствах.

  > Количество устройств, на которых вы можете использовать программу, определяется условиями Лицензионного соглашения.

- Обращение в Службу технической поддержки "Лаборатории Касперского".
- Получение прочих услуг, предоставляемых вам "Лабораторией Касперского" или ее партнерами, в течение срока действия подписки.

Перед приобретением подписки вы можете ознакомиться с пробной версией Kaspersky Security Cloud без выплаты вознаграждения. Пробная версия Kaspersky Security Cloud выполняет свои функции в течение короткого ознакомительного периода. После окончания ознакомительного периода Kaspersky Security Cloud для продолжения использования программы требуется приобрести подписку.

Как отозвать подписку с устройства

О том, как отозвать подписку Kaspersky Security Cloud с устройства или отправить подписку на устройство, вы можете прочитать в справке My Kaspersky.

О подписках, приобретённых в магазинах App Store и Google Play

Если вы приобрели подписку на Kaspersky Security Cloud в одном из магазинов приложений App Store или Google Play для использования на устройствах на базе Microsoft Windows, по истечении срока действия подписки на программу Kaspersky Security Cloud вам необходимо снова купить подписку в магазине приложений App Store или Google Play. В этом случае вы не сможете автоматически продлить подписку на сайтах наших партнеров или на сайте "Лаборатории Касперского".

Также вы можете приобрести пробную версию Kaspersky Security Cloud в магазинах App Store и Google Play и пользоваться программой бесплатно в течение ознакомительного периода. Обратите внимание, что по истечении ознакомительного периода программа Kaspersky Security Cloud автоматически переходит в платный режим и с вашей банковской карточки будут списаны средства за использование программы. Если вы не хотите пользоваться платной версией программы, вы должны отменить автоматический переход с пробной версии на платную версию до того, как закончится ознакомительный период.

Сравнение тарифных планов Kaspersky Security Cloud

Вы можете работать с Kaspersky Security Cloud по трем тарифным планам.

В таблице ниже можно узнать, какие функции Kaspersky Security Cloud доступны в каждом тарифном плане. Если в графе с названием тарифного плана указано значение "есть", это значит, что функциональность доступна в этом тарифном плане. Если в графе с названием тарифного плана указано значение "нет", функциональность недоступна.

Тарифные планы Kaspersky Security Cloud

Функциональность	Free	Personal	Family
Файловый Антивирус	есть	есть	есть
Проверка на вирусы	есть	есть	есть
Обновление баз и программных модулей	есть	есть	есть
Защита от рекламных программ и программ-шпионов	есть	есть	есть
Веб-Антивирус	есть	есть	есть
Почтовый Антивирус	есть	есть	есть
Эвристический анализ	есть	есть	есть
Защита от руткитов	есть	есть	есть

Защита от эксплойтов	есть	есть	есть
Мониторинг активности	есть	есть	есть
Защита от фишинга	есть	есть	есть
Проверка репутации файлов в Kaspersky Security Network	есть	есть	есть
Дополнительные средства защиты и управления	есть	есть	есть
Проверка ссылок	есть	есть	есть
Виртуальная клавиатура	есть	есть	есть
Защита ввода данных с аппаратной клавиатуры	нет	есть	есть
Диск аварийного восстановления	есть	есть	есть
Защита паролем настроек программы	есть	есть	есть
Производительность	есть	есть	есть
Менеджер задач	есть	есть	есть
Игровой режим	есть	есть	есть
Угрозы и исключения	есть	есть	есть
Самозащита	есть	есть	есть
Карантин	есть	есть	есть
Уведомления	есть	есть	есть
Настройка отображения программы	есть	есть	есть
My Kaspersky	есть	есть	есть

Восстановление после заражения	есть	есть	есть
Контроль программ	нет	есть	есть
Сетевой экран	нет	есть	есть
Защита от сетевых атак	есть	есть	есть
Анти-Спам	нет	есть	есть
Анти-Баннер	нет	есть	есть
Безопасные платежи	нет	есть	есть
Защита от сбора данных	нет	есть	есть
Устранение следов активности	есть	есть	есть
Защита веб-камеры	нет	есть	есть
Уведомление при подключении к небезопасной сети Wi-Fi	нет	есть	есть
Мониторинг сети	нет	есть	есть
Менеджер программ	нет	есть	есть
Kaspersky Password Manager	есть	есть	есть
Удаление неиспользуемых данных	есть	есть	есть
Необратимое удаление данных	есть	есть	есть
Обновление программ	нет	есть	есть
Очистка компьютера	нет	есть	есть
Настройка браузера	есть	есть	есть

Виртуальные сейфы	нет	есть	есть
Резервное копирование	нет	есть	есть
My Kaspersky	есть	есть	есть
Новости безопасности	есть	есть	есть
Устройства в моей сети	нет	есть	есть
Защита детей в интернете	нет	нет	есть
Защита ваших паролей в интернете	нет	есть	есть
Безопасное VPN-соединение	есть	есть	есть
Защита смартфонов	есть	есть	есть
Диагностика жесткого диска	нет	есть	есть
Проверка учетных записей	нет	есть	есть

Ознакомительный режим работы компонентов Защита от сбора данных, Безопасные платежи, Защита веб-камеры, Обновление программ и Проверка учетных записей

Если вы используете тарифный план Free, такие компоненты как Защита от сбора данных, Безопасные платежи, Защита веб-камеры и Обновление программ работают в ознакомительном режиме и могут обнаруживать соответствующие события, например, сбор информации о ваших действиях в интернете или использование веб-камеры. В ознакомительном режиме компоненты не чаще одного раза в неделю показывают уведомления о результатах своей работы. Если вас заинтересуют возможности Защиты от сбора данных, Безопасных платежей, Защиты веб-камеры или Обновления программ, вы сможете перейти к использованию тарифных планов Personal или Family, в которых эти компоненты доступны в полнофункциональном режиме.

Компонент Проверка учетных записей в тарифном плане Free работает в режиме ручной проверки учетной записи My Kaspersky. Автоматическая проверка этой и других учетных записей доступна только в тарифных планах Personal и Family.

О коде активации

Код активации – это код, который вы получаете, приобретая подписку на использование Kaspersky Security Cloud. Этот код необходим для активации программы.

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

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

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

Отсчет срока действия подписки начинается с даты активации программы. Если вы приобрели подписку, допускающую использование Kaspersky Security Cloud на нескольких устройствах, то отсчет срока действия подписки начинается с даты первого применения кода активации.

Если вы приобрели подписку с автопродлением, срок действия подписки начинается с момента покупки.

Если код активации был потерян или случайно удален после активации программы, то для его восстановления обратитесь в Службу технической поддержки "Лаборатории Касперского" .

Как приобрести подписку

Вы можете приобрести подписку на сайте My Kaspersky, на других сайтах "Лаборатории Касперского" или у наших партнеров. При приобретении подписки вы получите код активации, с помощью которого нужно активировать программу. В программе Kaspersky Security Cloud нельзя использовать резервный код активации.

Чтобы приобрести подписку на сайте My Kaspersky, выполните следующие действия:

1. Войдите на My Kaspersky .
2. Перейдите в раздел **Магазин**.
3. Выберите программу в списке программ и нажмите на кнопку **Купить**.
4. Следуйте инструкциям на сайте.

Чтобы приобрести подписку через интерфейс программы, выполните следующие действия:

1. Откройте главное окно программы.
2. Выполните одно из следующих действий:
   - Нажмите на кнопку **Купить** в главном окне программы.
   - По ссылке **Отсутствует** в главном окне программы перейдите в окно **Подписка** и нажмите на кнопку **Купить подписку**.

   В браузере по умолчанию откроется сайт "Лаборатории Касперского" или одного из наших партнеров. Следуйте инструкциям на сайте.

Как продлить подписку

Чтобы продлить подписку, выполните следующие действия:

1. Откройте главное окно программы.

2. По ссылке **Истекла** перейдите в окно **Подписка**.

3. Нажмите на кнопку **Продлить подписку**.

В браузере по умолчанию откроется сайт "Лаборатории Касперского" или одного из наших партнеров. Следуйте инструкциям на сайте.

При продлении подписки код активации сохраняется и подписка будет активирована автоматически в течение часа с момента продления.

Как активировать другую подписку, если подписка была отозвана или истекла

Если ваша подписка на программу Kaspersky Security Cloud была отозвана или истекла, вы можете выбрать другую подписку.

Чтобы выбрать другую подписку, выполните следующие действия:

1. Откройте главное окно программы.

2. По ссылке **Отозвана** или **Истекла** (в зависимости от статуса подписки) перейдите в окно **Подписка**.

3. В окне **Подписка** по ссылке **У меня есть подписка** перейдите в окно **Доступные подписки**.

4. Нажмите на кнопку **Выбрать** напротив подписки, по которой вы хотите использовать программу Kaspersky Security Cloud.

Если на My Kaspersky у вас нет активных подписок, программа предложит вам приобрести подписку.

Предоставление данных

Этот раздел содержит информацию о том, какие данные вы предоставляете в "Лабораторию Касперского" при использовании версии программы 3.0. Подраздел Сохранение данных в отчет о работе программы содержит данные, которые хранятся локально на вашем компьютере и не отправляются в "Лабораторию Касперского".

По ссылкам ниже вы можете ознакомиться с данными для предыдущих версий программы:

Предоставление данных для версии 2.0

Предоставление данных для версии 1.0

Предоставление данных в рамках Лицензионного соглашения

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

Вы соглашаетесь в автоматическом режиме предоставлять указанную ниже информацию посредством установленного вами программного обеспечения (далее ПО), правообладателем которого является АО "Лаборатория Касперского" (далее "Лаборатория Касперского", Правообладатель), в "Лабораторию Касперского" для повышения уровня оперативной защиты и формирования наиболее подходящих предложений информационного и рекламного характера, для улучшения качества работы ПО и своевременного выявления и исправления ошибок, связанных с механизмом установки, удаления и обновления ПО, для учета количества пользователей:

- Информация об установленном ПО Правообладателя: полная версия ПО; идентификатор обновления ПО; тип установленного ПО; идентификатор установки ПО (PCID); дата и время установки ПО; идентификатор ПО, полученный из лицензии; идентификатор ПО, для которого предназначена лицензия; локализация ПО; признак участия в KSN; идентификатор ребрендинга ПО; статус установки/удаления ПО; код ошибки установки; идентификатор ПО; код ребрендинга ПО; тип установки (новая установка, обновление); типы сторонних приложений, которые были предложены к установке при установке ПО; типы сторонних приложений, которые были выбраны к установке при установке ПО; типы сторонних приложений, которые были установлены в процессе установки ПО; идентификатор пользователя на сайте правообладателя; время, затраченное на установку ПО, в секундах; признак прерывания установки пользователем; идентификатор ПО; код партнерской организации, для которой был выполнен ребрендинг ПО; информация, указывающая на элемент интерфейса, из которого пользователь решил приобрести ПО; тип пользовательского сценария; имя партнера;

- Прочая информация: протокол, используемый для передачи данных в KSN; время задержки отправки статистики; идентификатор маркетинговой компании; версия протокола взаимодействия между ПО и маркетинговыми сообщениями; идентификатор страницы; тип регистрации на My Kaspersky; идентификатор элемента управления в пользовательском интерфейсе; идентификатор действия пользователя; адрес электронной почты пользователя, который он вводил при оформлении заказа в интерфейсе ПО; тип запроса; размер содержимого запроса; идентификатор протокола; тип сжатия данных; идентификатор выбора пользователя в маркетинговой компании; выбор пользователя в маркетинговой компании; тип области, в которой произошло событие; список идентификаторов контента, которые прочитал пользователь;

- Информация о пользовательском окружении: признак включения компонента Device Guard (windows); идентификатор устройства; внешний IP-адрес; уникальный идентификатор устройства; тип ОС (сервер, рабочая станция, контроллер домена); версия ОС, номер сборки ОС, номер обновления ОС, редакция ОС, расширенная информация о редакции ОС; версия пакета обновления ОС; семейство операционной системы; тип аппаратной платформы; дополнительная информация о функциях ОС; тип устройства (ноутбук, настольный ПК, планшет); версия браузера; дата и время на устройстве пользователя;

- Информация об обрабатываемом объекте: контрольная сумма (MD5) обрабатываемого объекта; контрольная сумма (SHA256) обрабатываемого объекта; контрольная сумма частей проверяемого объекта для быстрого обнаружения вредоносной программы или легальной программы, которая может быть использована для нанесения вреда компьютеру или данным пользователя; публичный ключ сертификата; отпечаток цифрового сертификата проверяемого объекта и алгоритм хеширования; название обнаруженной вредоносной программы или легальной программы, которая может быть использована для нанесения вреда устройству или данным пользователя; временная метка сработавшей записи в антивирусных базах ПО; идентификатор сработавшей записи в антивирусных базах ПО; тип сработавшей записи в антивирусных базах ПО; размер обрабатываемого объекта; имя обрабатываемого объекта; путь к обрабатываемому объекту; код каталога файлов; идентификатор уязвимости, найденной в настройках ПО; тип контрольной суммы обрабатываемого объекта;

- Информация об обращении к веб-сервису: обрабатываемый веб-адрес; номер порта; веб-адрес источника запроса к веб-службе (referer); IP-адрес (IPv4) веб-службы, на который осуществлялось обращение; тип сертификата;

- Информация о лицензии и прочих соглашениях: тип юридического соглашения, условия которого были приняты пользователем в ходе использования ПО; версия юридического соглашения, условия которого были приняты пользователем в ходе использования ПО; признак принятия пользователем условий юридического соглашения в ходе использования ПО; дата и время согласия пользователя с условиями юридического Соглашения в ходе использования ПО; дата активации ПО; серийный номер лицензионного ключа ПО; идентификатор

лицензии ПО; идентификатор информационной модели, примененной при предоставлении лицензии на использование ПО; тип используемой лицензии ПО; срок действия лицензии на использование ПО; количество дней, оставшихся до истечения срока действия лицензии на использование ПО; полное название партнерской организации, у которой был размещен заказ на лицензию на использование ПО; информация о пробной версии ПО; текущий статус лицензионного ключа ПО; номер заказа, по которому приобретена лицензия на использование ПО; идентификатор позиции предложения в прайс-листе, по которому приобретена лицензия на использование ПО; номер заказа на покупку лицензии на использование ПО у партнера; идентификатор страны, в которой находится партнер, продавший лицензию на использование ПО; данные о лицензии для идентификации группы пользователей в компании, которая приобрела лицензию, по комментарию в свойствах лицензии; дата и время истечения срока действия лицензии на использование ПО; текущий статус подписки; причина текущего статуса / изменения подписки; тип подписки ПО; дата и время окончания подписки ПО; данные о лицензии ПО для идентификации группы пользователей по дополнительным параметрам подписочной лицензии; данные о лицензии ПО для идентификации группы пользователей по дополнительным параметрам подписочной лицензии; данные о лицензии ПО для идентификации группы пользователей по дополнительным параметрам подписочной лицензии; количество дней, прошедших после активации ПО; количество дней, прошедших после истечения срока действия лицензионного ключа ПО; информация об ошибках активации ПО; категория ошибки активации ПО; код ошибки активации ПО; приобретенные коды активации; набор идентификаторов ПО, которое может быть активировано на устройстве пользователя; код активации ПО; код активации ПО, используемый в настоящее время; заголовок лицензии на использование ПО; идентификатор регионального центра активации; дата и время создания лицензионного ключа ПО; тип лицензии, с помощью которой активировано ПО; идентификатор товарной позиции ПО;

- Информация для взаимодействия с Веб-порталом: идентификатор учетной записи My Kaspersky; признак подключения ПО к My Kaspersky; уникальный идентификатор устройства на сайте My Kaspersky; подпись ответа инфраструктуры My Kaspersky; страница на сайте My Kaspersky, на которую направляет ссылка из ПО; страна и регион веб-службы "Лаборатории Касперского", с которого была загружена пробная версия ПО; время последнего изменения статуса; версия протокола, по которому осуществляется управление настройками ПО с сайта My Kaspersky; статус защиты устройства; статус использования компонентов защиты; статус задач проверки; статус задачи обновления баз и программных модулей; список проблем безопасности; содержимое раздела рекомендации для списка проблем; статус лицензии, по которой используется ПО; режим работы ПО; информация об обновлении баз и программных модулей; список игнорируемых проблем безопасности; идентификатор пользователя, который выдается после успешной аутентификации пользователя на My Kaspersky; одноразовый пароль для автоматического подключения ПО, загруженного из учетной записи My Kaspersky; одноразовый пароль для регистрации устройства на My Kaspersky; имя компьютера в сети (доменное имя); тип устройства, подключенного к My Kaspersky; причина отключения от My Kaspersky; тип токена; данные для получения токена аутентификации для сеанса;

- Информация об обновлении локальных баз: идентификатор запуска обновления ПО.

Для улучшения качества работы продукта, а также для формирования наиболее подходящих предложений информационного и рекламного характера Вы соглашаетесь предоставлять следующую информацию в "Лабораторию Касперского":

- Информацию об установленном на компьютере аппаратном обеспечении, в том числе данные о модели, производителе, модели и объеме жесткого диска (HDD), объеме физической и виртуальной памяти, производителе оперативной памяти, производителе материнской платы, производителе и названии программы BIOS, производителе видеокарты и объеме видеопамяти, производителе и типе сетевого адаптера, его скорости передачи данных, производителе и названии монитора, уникальный идентификатор установки ПО на компьютер и уникальный идентификатор компьютера.

- Данные о подключенных к компьютеру USB устройствах: класс/модель USB устройства, производитель устройства и название, дата последнего подключения устройства к компьютеру.

- Информацию об устройствах, поддерживающих UPnP протокол, в том числе название производителя и имя устройства, а также дата последнего подключения.

- Данные о загрузке системы, в том числе размер свободной и используемой памяти, размер свободного места на диске.

- Сведения обо всех установленных программах, включающие название и версию установленного приложения, версии установленных обновлений, название издателя, дату и полный путь установки на компьютере, конфигурация (настройки) приложения (в т.ч. браузеров).

- Информацию об установленной на компьютере версии операционной системы (ОС) и установленных пакетов обновлений, а также имя компьютера в сети (локальное и доменные имена), региональные настройки ОС (включая данные о часовом поясе, раскладки клавиатуры по умолчанию, язык интерфейса), настройки UAC, настройки сетевого экрана ОС, настройки родительского контроля ОС, настройки Windows Update, информация о переменных окружения и учетной записи пользователя.

- Названия и размещение любых файлов на компьютере.

- Информацию об активностях на компьютере Пользователя, в том числе текущая дата и время, и время, прошедшее с момента последней активности пользователя, а также данные о запущенных процессах в системе(идентификатор процесса в системе (PID), имя процесса,

время запуска, данные об учетной записи, от которой запущен процесс, о программе и команде, запустившей процесс, полный путь к файлам процесса и командная строка запуска, описание продукта, к которому относится процесс (название, описание, производитель), название активного окна и время его активации.

- Информацию о посещенных веб-сайтах, в том числе URL-адреса, введенные в браузер пользователем, поисковые запросы, введенные пользователем в поисковых системах, и URL-адреса, на которые были переходы из поисковых систем, время посещения URL, идентификатор типа URL и параметры URL, статистические параметры посещенных URL, в том числе язык и распределение слов в тексте.

В соответствии с описанием в Руководстве пользователя основные функциональные возможности ПО заключаются в защите пользователя от известных угроз информационной безопасности. Для обеспечения этих основных функциональных возможностей в процессе использования Вами ПО Правообладателю необходимо получать и обрабатывать следующую информацию:

- Информацию о компоненте Антиспам: эвристически определенный IP-адрес отправителя по заголовкам received и SMTP-сессии; наиболее вероятный IP-адрес отправителя спама; контрольная сумма обрабатываемого объекта (MD5); контрольные суммы вложений; определяемые текстовые категории сообщения электронной почты; веб-адреса, обнаруженные в обрабатываемом сообщении электронной почты; метаинформация и части обрабатываемого электронного сообщения для проверки в службах правообладателя;

- Информацию о пользовательском окружении: название Wi-Fi сети; контрольная сумма (MD5 с модификатором) MAC-адреса точки доступа; контрольная сумма (SHA256 с модификатором) MAC-адреса точки доступа; тип аутентификации Wi-Fi сети; тип шифрования сети Wi-Fi; идентификатор сети Wi-Fi, посчитанный по MAC-адресу точки доступа; идентификатор сети Wi-Fi, посчитанный по ее названию; идентификатор сети Wi-Fi, посчитанный по ее названию и MAC-адресу точки доступа; уровень сигнала сети Wi-Fi; список доступных Wi-Fi сетей и их параметры; настройки DHCP (контрольные суммы: локального IP-адреса шлюза, DHCP IP, DNS1 IP, DNS2 IP, маски подсети); настройки протокола DHCP (контрольные суммы: локального IPv6-адреса шлюза, DHCP IPv6, DNS1 IPv6, DNS2 IPv6, маски подсети); веб-адрес службы, используемой для получения доступа в интернет; первые 5 байт MAC-адреса устройства; идентификатор ОС; информация о режиме контроля устройств в сети Wi-Fi; идентификатор устройства, посчитанный по идентификатору пользователя на сайте My Kaspersky; статус подключенного устройства к Wi-Fi сети; тип устройства; производитель устройства или сетевой карты;

- Информацию об обрабатываемом объекте: контрольная сумма от имени пользователя; количество запусков ПО с момента последней отправки контрольной суммы файла; формат обрабатываемого объекта; группирующий уровень важности; ссылка на статью базы знаний; признак обработки настройки; количество обнаруженных уязвимостей в настройках безопасности; признак возможности

удаленного исправления обнаруженных уязвимостей в настройках безопасности; идентификатор применяемого правила; категория важности параметров безопасности;

- Прочую информацию: версия отправляемой статистики; дата и время получения запроса от приложения (GMT); факт обнаружения использования устройства ребенком; метод обнаружения устройств в сети; версия компонента для обнаружения устройств в сети;

- Информацию об обновлении локальных баз: значение фильтра TARGET для задачи обновления;

- Информацию об установленном ПО Правообладателя: идентификатор службы KSN, к которой обращается ПО.

Если Вы решаете использовать функцию Adaptive Security, Вы соглашаетесь на автоматическую передачу информации, необходимой для разработки рекомендаций по повышению безопасности. Данные рекомендации будут отображаться на веб-портале в учетной записи, к которой привязано ПО. Информация об отображаемых рекомендациях может использоваться службой технической поддержки только при обработке запроса Пользователя.

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

В целях выявления новых угроз информационной безопасности и их источников, повышения уровня защиты информации Пользователей ПО, а также для улучшения качества работы продукта информацию, определенную в Положении об использовании Kaspersky Security Network. Данную функцию автоматической передачи информации можно отключить при установке ПО, а также можно как включить, так и выключить во время работы ПО.

Полученные данные Правообладатель вправе использовать для формирования отчетов по рискам информационной безопасности.

В том случае, если Вы не хотите, чтобы информация, которую Kaspersky Security Network получает от Пользователя, отсылалась Правообладателю, Вы не должны активировать или должны отключить Kaspersky Security Network.

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

Этот раздел содержит информацию о том, какие данные передаются в "Лабораторию Касперского", если у вас установлена версия программы, предназначенная для использования на территории Европейского союза, Великобритании, Бразилии, а также резидентами штата Калифорния. **Приведенная в этом разделе информация не содержит персональных данных Пользователя и служит для обеспечения работы ПО Правообладателя, если не указано иное**.

Для повышения уровня оперативной защиты, для улучшения качества работы ПО и своевременного выявления и исправления ошибок, связанных с механизмом установки, удаления и обновления ПО, а также для учета количества пользователей, вы соглашаетесь в автоматическом режиме при использовании ПО передавать следующие данные в "Лабораторию Касперского":

- Информация об установленном ПО Правообладателя: полная версия ПО; идентификатор обновления ПО; тип установленного ПО; статус установки/удаления ПО; код ошибки установки; идентификатор ПО; идентификатор ребрендинга ПО; локализация ПО; код ребрендинга ПО; тип ОС (сервер, рабочая станция, контроллер домена); тип установки (новая установка, обновление); время, затраченное на установку ПО, в секундах; признак прерывания установки пользователем.

- Прочая информация: протокол, используемый для передачи данных в KSN.

- Информация о пользовательском окружении: признак включения компонента Device Guard (Windows); семейство операционной системы; версия ОС, номер сборки ОС, номер обновления ОС, редакция ОС, расширенная информация о редакции ОС; тип аппаратной платформы; дополнительная информация о функциях ОС; тип устройства (ноутбук, настольный ПК, планшет); первые 5 байт MAC-адреса устройства.

- Информация об обрабатываемом объекте: публичный ключ сертификата; отпечаток цифрового сертификата проверяемого объекта и алгоритм хеширования; название обнаруженной вредоносной программы или легальной программы, которая может быть использована для нанесения вреда устройству или данным пользователя; временная метка сработавшей записи в антивирусных базах ПО; идентификатор сработавшей записи в антивирусных базах ПО; тип сработавшей записи в антивирусных базах ПО; контрольная сумма от имени пользователя.

- Информация об обращении к веб-службе: обрабатываемый веб-адрес; IP-адрес (IPv4) веб-службы, на который осуществлялось обращение; тип сертификата.

- Информация о лицензии и прочих соглашениях: идентификатор товарной позиции ПО; тип используемой лицензии ПО; срок действия лицензии на использование ПО; количество дней, оставшихся до истечения срока действия лицензии на использование ПО; полное название партнерской организации, у которой был размещен заказ на лицензию на использование ПО.

В целях улучшения качества защиты Пользователя при проведении платежных операций в интернете вы соглашаетесь в автоматическом режиме предоставить финансовому сайту информацию о наименовании и версии ПО и настройке кастомизации ПО, идентификатор состояния плагина ПО в используемом для обращения к финансовому сайту браузере, идентификатор использования безопасного или обычного браузера.

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.

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, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. В окне **Настройка** выберите раздел **Защита**.
4. В разделе **Защита** выберите компонент Kaspersky Security Network.

   Откроется окно **Kaspersky Security Network**.

5. По ссылке **Положение о Kaspersky Security Network** откройте текст Положения о Kaspersky Security Network.

Сохранение данных в отчет о работе программы

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

Файлы отчетов могут содержать следующие персональные данные:

- IP-адрес устройства пользователя;
- история посещения сайтов;
- заблокированные ссылки;
- история переписки в социальных сетях;
- 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.

При использовании компонентов Защита детей, Устройства в моей сети и Новости безопасности вы предоставляете следующие данные:

- идентификатор сети Wi-Fi, статус сети Wi-Fi, идентификатор устройства, хеш от MAC-адреса устройства, статус устройства;
- информация о посещаемых сайтах;
- информация о том, сколько раз запускался исполняемый файл на компьютере (популярность файла).

Файлы отчетов хранятся локально на вашем компьютере и не передаются в "Лабораторию Касперского". Путь к файлам отчетов: %allusersprofile%\Kaspersky Lab\AVP21.3\Report\Database.

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 программе Kaspersky Security Cloud включена самозащита. Если самозащита выключена, файлы отчетов не защищаются.

Сохранение данных для Службы технической поддержки

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

- Данные, которые отображаются в интерфейсе программы:
  - адрес электронной почты, используемый для подключения к My Kaspersky;
  - адреса сайтов, которые были добавлены в исключения (отображаются в компонентах Веб-Антивирус, Анти-Баннер, Защита от сбора данных, 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 Security Cloud 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 **Положение о предоставлении данных** в окне **Мониторинг проблем**.

Об использовании программы на территории Европейского союза, Великобритании, Бразилии, а также резидентами штата Калифорния

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

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

Кроме этого, мастер установки и удаления предложит вам принять следующие соглашения 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 программах и о скачиваемых подписанных программах, 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.

- Положение об обработке данных при использовании Анти-Спама. Это положение позволяет специалистам "Лаборатории Касперского" получать данные для улучшения работы компонента Анти-Спам.

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 → Защита → Kaspersky Security Network**.

Для чего нужен My Kaspersky

My Kaspersky – это сайт "Лаборатории Касперского", предназначенный для централизованного хранения информации и управления программами "Лаборатории Касперского", которые вы используете.

На My Kaspersky вы можете:

- просматривать информацию о лицензиях и сроках их действия;
- управлять защитой компьютера удаленно;
- безопасно хранить и синхронизировать пароли и другую личную информацию, если вы используете Kaspersky Password Manager;
- защитить ваших детей от опасностей, связанных с использованием программ и интернета, если вы используете Kaspersky Safe Kids;
- скачивать приобретенные программы;
- обратиться в Службу технической поддержки за помощью;
- узнавать о новых программах и специальных предложениях "Лаборатории Касперского".

Чтобы иметь доступ к возможностям My Kaspersky, нужна учетная запись.

Подробную информацию о работе с My Kaspersky вы найдете в Справке My Kaspersky .

Об учетной записи My Kaspersky

Учетная запись My Kaspersky требуется для работы с программой Kaspersky Security Cloud.

Если у вас еще нет учетной записи My Kaspersky, вы можете создать ее на сайте или в окне подключения к сайту в программе Kaspersky Security Cloud. Вы также можете использовать для входа на сайт учетные данные других ресурсов "Лаборатории Касперского".

При создании учетной записи My Kaspersky вам нужно указать действующий адрес электронной почты и придумать пароль. Пароль должен состоять не менее чем из восьми символов и содержать хотя бы одну цифру, одну заглавную и одну строчную латинские буквы. Пробелы не допускаются.

> Если введенный пароль слишком простой или распространенный, учетная запись не будет создана.

После создания учетной записи на указанный вами адрес электронной почты будет выслано сообщение, содержащее ссылку для активации вашей учетной записи.

Об удаленном управлении защитой компьютера

Если на компьютере установлена программа Kaspersky Security Cloud и компьютер подключен к My Kaspersky, вы можете управлять защитой этого компьютера удаленно.

Чтобы удаленно управлять защитой компьютера, вам нужно войти в My Kaspersky под своей учетной записью и перейти в раздел **Устройства**.

В разделе **Устройства** вы можете:

- просматривать список проблем безопасности на компьютере и удаленно устранять их;
- проверять компьютер на вирусы и другие программы, представляющие угрозу;
- обновлять базы и программные модули;
- настраивать компоненты программы Kaspersky Security Cloud.

Если проверка компьютера запущена из My Kaspersky, то Kaspersky Security Cloud обрабатывает обнаруженные объекты в автоматическом режиме без вашего участия. В случае обнаружения вируса или другой программы, представляющей угрозу, программа Kaspersky Security Cloud попытается выполнить лечение без перезагрузки компьютера. Если лечение без перезагрузки компьютера невозможно, на My Kaspersky в списке проблем защиты компьютера появляется сообщение о том, что для лечения компьютера требуется перезагрузка.

Если на My Kaspersky в списке обнаруженных объектов более 10 элементов, то они группируются. В этом случае через My Kaspersky обнаруженные объекты можно обработать только одновременно, без возможности просмотреть каждый объект. Для просмотра отдельных объектов в этом случае рекомендуется использовать интерфейс программы, установленной на компьютере.

Как перейти к удаленному управлению защитой компьютера

Чтобы перейти к удаленному управлению защитой компьютера, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части главного окна программы перейдите по ссылке **My Kaspersky**.

В окне браузера по умолчанию откроется страница входа на My Kaspersky.

Как настроить интерфейс программы

Этот раздел содержит информацию о том, как настроить интерфейс Kaspersky Security Cloud.

Как сменить значок программы

Чтобы сменить значок программы, выполните следующие действия:

1. Откройте главное окно программы.

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

   Откроется окно **Настройка**.

3. Выберите раздел **Интерфейс**.

4. В блоке **Значок программы** выберите один из вариантов:

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

Как сменить тему оформления программы

> Смена темы оформления программы доступна не во всех регионах.

Чтобы сменить тему оформления программы, выполните следующие действия:

1. Откройте главное окно программы.

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

   Откроется окно **Настройка**.

3. Выберите раздел **Интерфейс**.

4. В блоке **Тема оформления** установите флажок **Использовать альтернативную тему оформления**.

5. Нажмите на кнопку **Выбрать** и укажите путь к zip-архиву или папке, в котором содержатся файлы с альтернативной темой оформления.

После добавления альтернативная тема оформления будет применена после перезапуска программы.

Об уведомлениях программы

Уведомления программы, появляющиеся в области уведомлений панели задач, информируют о событиях, происходящих в процессе работы программы 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 Security Cloud или в режиме Connected Standby в Windows 8. Уведомления компонента Контроль программ автоматически закрываются по истечении 500 секунд. Уведомления о запуске программы автоматически закрываются по истечении 1 часа. При автоматическом закрытии уведомления Kaspersky Security Cloud выполняет действие, рекомендованное по умолчанию.

Уведомления не отображаются в течение первого часа работы программы в случае приобретения компьютера с предустановленной программой Kaspersky Security Cloud (OEM-поставка). Программа обрабатывает обнаруженные объекты в соответствии с рекомендуемыми действиями. Результаты обработки сохраняются в отчете.

Как настроить уведомления программы

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

Как настроить получение уведомлений

Чтобы создать правила уведомлений, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Интерфейс**.
4. В блоке **Уведомления** по ссылке **Настройка уведомлений** перейдите в окно настройки уведомлений.
5. Слева в списке выберите компонент.
6. В правой части окна отобразится список событий, которые могут произойти во время работы этого компонента.
7. 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 программы 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 программы* для элемента **Аудит системы** и компонента **Контроль программ**).

- **Важные**. При выборе этого варианта в отчет будут сохраняться *Критические события* (включая *События, связанные со сбоями в работе программы* для элемента **Аудит системы** и компонента **Контроль программ**) и *Предупреждения*.

- **Информационные**. При выборе этого варианта в отчет будут сохраняться все события.

Как настроить получение уведомлений о новостях и специальных предложениях "Лаборатории Касперского"

Если вы хотите быть в курсе последний новостей из мира компьютерной безопасности, а также получать специальные предложения "Лаборатории Касперского", выполните следующие действия:

1. Откройте главное окно программы.

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

   Откроется окно **Настройка**.

3. Перейдите в раздел **Интерфейс**.

4. В блоке **Уведомления о новостях** установите флажок **Получать информационные и рекламные сообщения "Лаборатории Касперского"**, если вы хотите получать уведомления о новостях компьютерной безопасности.

5. В блоке **Информационные материалы** выполните следующие действия:

   - Установите флажок **Отображать информацию о специальных предложениях**, если вы хотите получать наиболее выгодные предложения при посещении сайтов "Лаборатории Касперского".

   - Установите флажок **Получать информационные и рекламные сообщения по истечении срока действия лицензии** (подписки), если вы хотите получать уведомления о новостях безопасности от "Лаборатории Касперского" после истечения срока действия лицензии (подписки).

Как настроить сопровождение уведомлений звуковыми сигналами

1. Откройте главное окно программы.

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

   Откроется окно **Настройка**.

3. Выберите раздел **Интерфейс**.

4. В блоке **Уведомления** установите флажок **Сопровождать уведомления звуковыми сигналами**.

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

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

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

Чтобы настроить изменение значка программы в области уведомлений в зависимости от статуса программы, выполните следующие действия:

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

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

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

Как защитить доступ к управлению Kaspersky Security Cloud с помощью пароля

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

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

Чтобы создать пароль администратора `KLAdmin` Kaspersky Security Cloud, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Интерфейс**.
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 **OK**.

Забытый пароль восстановить нельзя. Если пароль забыт, для восстановления доступа к настройкам Kaspersky Security Cloud 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 **Интерфейс** в блоке **Защита паролем** нажмите на кнопку **Добавить**.

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

2. По ссылке **Выбрать пользователя** откройте 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 **Интерфейс** в блоке **Защита паролем** 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**, программа 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.

Как ускорить работу компьютера

В процессе длительной эксплуатации компьютера работа операционной системы может замедляться. К замедлению работы приводит большое количество лишних файлов и ошибок реестра Windows, скопившихся за время работы.

Также к замедлению работы операционной системы могут приводить установленные, но редко используемые программы. Многие из этих программ могут запускаться непосредственно при загрузке операционной системы и значительно замедляют ее работу. Вы можете даже не подозревать, что какая-то программа запустилась и работает в фоновом режиме, используя ресурсы компьютера.

Чтобы ускорить работу компьютера, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Ускорить компьютер**.
3. В открывшемся окне **Ускорить компьютер** выполните следующие действия:

   - В блоке **Ускорить работу компьютера** нажмите на кнопку **Начать** (или **Посмотреть**, если поиск уже выполнялся).

     Программа выполнит поиск и предоставит вам отчет следующего содержания:

     - **Неиспользуемые файлы системы**. Нажмите на блок, чтобы просмотреть подробный отчет о том, какие файлы операционной системы не используются. Нажмите на кнопку **Очистить**, чтобы удалить эти файлы.
     - **Ошибки реестра Windows**. Нажмите на блок, чтобы просмотреть подробный отчет о том, какие ошибки реестра Windows вы можете исправить без риска повредить операционную систему. Нажмите на кнопку **Исправить**, чтобы исправить найденные ошибки.

- Нажмите на блок **Ускорить запуск**, чтобы просмотреть отчет о том, автозапуск каких программ замедляет запуск компьютера. Переведите переключатель **Автозапуск** напротив программы в положение **Выкл.** и нажмите на кнопку **Готово**.

- Нажмите на блок **Освободить место**, чтобы освободить место на жестком диске. В открывшемся окне выполните поиск файлов.

  - **Дубликаты файлов**. Нажмите на кнопку **Найти**, чтобы запустить поиск дубликатов файлов. В раскрывающемся списке вы можете указать область поиска. В окне с результатами поиска выберите файлы и нажмите на кнопку **Удалить**.

  - **Большие файлы**. Нажмите на кнопку **Найти**, чтобы запустить поиск больших файлов. В раскрывающемся списке вы можете указать область поиска. В окне с результатами поиска выберите файлы и нажмите на кнопку **Удалить**.

    > Поиск файлов большого размера не работает для файлов, на которые ведут две или более жесткие ссылки в операционной системе.

  - **Неиспользуемые программы**. Нажмите на кнопку **Найти**. Отчет о результатах поиска содержит список программ, которые не использовались больше трех месяцев. Выберите программу и нажмите на кнопку **Удалить**.

Чтобы отправить отзыв о работе функциональности Ускорить компьютер,

в окне **Ускорить компьютер** нажмите на кнопку **Оставить отзыв** и заполните форму обратной связи.

Ваш отзыв необходим специалистам "Лаборатории Касперского", чтобы оценить качество функциональности Ускорить компьютер.

> Экспериментальная функция "Ускорить компьютер" доступна для использования до 30 июля 2021 года.

Эта функциональность доступна не во всех регионах.

Новости безопасности

Этот раздел содержит информацию о новостях безопасности от "Лаборатории Касперского".

О новостях безопасности

Каждый день в мире совершаются массовые кражи паролей, взломы баз данных, мошенничества в интернет-банках. Новости безопасности от "Лаборатории Касперского" предоставляют свежую информацию о таких преступлениях и помогают вам избегать ситуаций, в которых можно стать жертвой злоумышленников. Чтобы новости безопасности, которые вы получаете, были актуальны именно для вас, Kaspersky Security Cloud анализирует информацию о посещаемых вами ресурсах и запускаемых вами приложениях. Эта информация используется только для отбора новостей, которые могут быть важны или интересны для вас.

Новости безопасности выводятся в Центре уведомлений вместе с другими новостями от "Лаборатории Касперского". Уведомления о новостях безопасности появляются в области уведомлений панели задач. Окна уведомлений содержат заголовок новости и краткую рекомендацию по решению проблемы, о которой говорится в этой новости.

В зависимости от степени важности новости могут быть следующих типов:

- *Важная новость* – новость о событиях, которые могут угрожать вашей безопасности (например, новость о массовой краже паролей ВКонтакте). Окна важных новостей – желтые.

- *Новость общего характера* – новость, носящая информационный характер (например, новость об участившихся случаях перехвата данных в интернет-банках при помощи троянских программ). Окна для новостей общего характера – зеленые.

Если на экране появилось уведомление о новости безопасности, вы можете перейти к полному тексту новости, нажав на кнопку **Подробнее** во всплывающем окне, или закрыть всплывающее окно. Вы можете ознакомиться с полным текстом новости в любое время, выбрав эту новость в списке новостей Центра уведомлений.

Если вы не хотите получать новости безопасности на данном устройстве, вы можете отключить отображение новостей в Kaspersky Security Cloud. Если вы не хотите получать новости ни на одном из ваших устройств, вы можете отключить получение новостей на My Kaspersky.

> Новости безопасности не отображаются в течение первого часа работы Kaspersky Security Cloud после установки.

Как включить и выключить новости безопасности

Чтобы включить или выключить новости безопасности, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Уведомления**.
4. Выполните одно из следующих действий:

   - Если вы хотите получать новости безопасности, переведите переключатель **Получать информационные и рекламные сообщения "Лаборатории Касперского"** в положение **Вкл**.
   - Если вы не хотите получать новости безопасности, переведите переключатель **Получать информационные и рекламные сообщения "Лаборатории Касперского"** в положение **Выкл**.

Как включить и выключить получение новостей безопасности на My Kaspersky

Чтобы включить или выключить получение новостей безопасности на My Kaspersky, выполните следующие действия:

1. Откройте главную страницу My Kaspersky.
2. Нажмите на кнопку **Войти** и введите ваш адрес электронной почты, указанный при создании учетной записи, и пароль.
3. Нажмите на кнопку  .

   Откроется окно просмотра уведомлений.
4. В верхней части открывшегося окна просмотра уведомлений нажмите на кнопку  .

   Откроется окно настроек уведомлений.
5. Выполните одно из следующих действий:

   - Если вы хотите включить получение новостей безопасности, установите флажок **Новости безопасности**.
   - Если вы хотите отключить получение новостей безопасности, снимите флажок **Новости безопасности**.

Анализ состояния защиты компьютера и устранение проблем безопасности

О появлении проблем в защите компьютера сигнализирует индикатор, расположенный в верхней части главного окна программы. 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.

Нажав на кнопку **Подробнее** в главном окне программы, вы можете открыть окно **Центр уведомлений**. 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 **Рекомендации** отображаются уведомления о действиях, которые рекомендуется выполнить для оптимизации работы программы и более эффективного ее использования.

В разделе **Показать N игнорируемых уведомлений** отображаются уведомления, к которым было применено действие **Игнорировать**. Проблемы в этом разделе не влияют на цвет индикатора защиты в главном окне программы.

Обновление баз и программных модулей

Этот раздел содержит информацию об обновлении баз и программных модулей.

Об обновлении баз и программных модулей

Пакет установки Kaspersky Security Cloud включает в себя базы и программные модули. С помощью этих баз:

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

Для полной защиты рекомендуется обновить базы и программные модули сразу после установки программы.

Обновление баз и программных модулей выполняется поэтапно:

1. Kaspersky Security Cloud запускает обновление баз и программных модулей согласно указанным настройкам: автоматически, по расписанию или по вашему требованию. Программа обращается к источнику обновлений, где хранится пакет обновлений баз и программных модулей.

2. Kaspersky Security Cloud сравнивает имеющиеся базы с базами, находящимися в источнике обновлений. Если базы отличаются, Kaspersky Security Cloud скачивает отсутствующие части баз.

После этого программа использует обновленные базы и программные модули для проверки компьютера на вирусы и другие программы, представляющие угрозу.

Источники обновлений

Вы можете использовать следующие источники обновлений:

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

Особенности обновления баз и программных модулей

Обновление баз и программных модулей имеет следующие особенности и ограничения:

- 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 баз и программных модулей недоступно в следующих случаях:
    - Истек срок действия подписки, 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 баз и программный модулей, требуется снять флажок **Ограничивать трафик при лимитном подключении** в окне **Настройка → Настройки сети**.

- Программа используется по подписке, и вы приостановили подписку на сайте поставщика услуг.

Установка пакета исправлений

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

Как запустить обновление баз и программных модулей

Чтобы запустить обновление баз и программных модулей, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Обновление баз**.

   Откроется окно **Обновление баз**.

2. В окне **Обновление баз** нажмите на кнопку **Обновить**.

Проверка компьютера

Во время проверки Kaspersky Security Cloud ищет зараженные файлы и вредоносные программы. В зависимости от продолжительности и области поиска выделяют проверку нескольких типов:

- 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 съемных дисков. Проверка съемных 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.
- Поиск уязвимостей. Проверка компьютера на наличие уязвимостей, через которые способны проникнуть вредоносные программы.

После установки Kaspersky Security Cloud мы рекомендуем выполнить полную проверку компьютера.

Как запустить быструю проверку

Во время быстрой проверки Kaspersky Security Cloud по умолчанию проверяет следующие объекты:

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

Чтобы запустить быструю проверку, выполните следующие действия:

1. Откройте главное окно программы.

2. Нажмите на кнопку **Проверка**.

   Откроется окно **Проверка**.

3. В окне **Проверка** выберите раздел **Быстрая проверка**.

4. В разделе **Быстрая проверка** нажмите на кнопку **Запустить проверку**.

Kaspersky Security Cloud начнет быструю проверку компьютера.

Как запустить полную проверку

Во время полной проверки по умолчанию Kaspersky Security Cloud проверяет следующие объекты:

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

Рекомендуется выполнить полную проверку сразу после установки Kaspersky Security Cloud на компьютер.

Чтобы запустить полную проверку, выполните следующие действия:

1. Откройте главное окно программы.

2. Нажмите на кнопку **Проверка**.

   Откроется окно **Проверка**.

3. В окне **Проверка** выберите раздел **Полная проверка**.

4. В разделе **Полная проверка** нажмите на кнопку **Запустить проверку**.

Kaspersky Security Cloud начнет полную проверку компьютера.

Как запустить выборочную проверку

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

Чтобы запустить выборочную проверку, выполните следующие действия:

1. Откройте главное окно программы.

2. Нажмите на кнопку **Проверка**.

   Откроется окно **Проверка**.

3. В окне **Проверка** выберите раздел **Выборочная проверка**.

4. Нажмите на кнопку **Выбрать** и укажите объект в открывшемся окне выбора файла или папки.

5. Нажмите на кнопку **Запустить проверку**.

Как запустить проверку съемных дисков

Съемные диски, которые вы подключаете к компьютеру, могут содержать вирусы и другие программы, представляющие угрозу. Kaspersky Security Cloud проверяет съемные диски, чтобы не допустить заражения вашего компьютера. Вы можете запускать проверку съемных дисков вручную или автоматически при подключении съемного диска к компьютеру. По умолчанию автоматическая проверка съемных дисков включена.

Чтобы проверить съемный диск вручную, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Проверка**.

   Откроется окно **Проверка**.
3. В окне **Проверка** выберите раздел **Проверка съемных дисков**.
4. В раскрывающемся списке выберите внешнее устройство (отображается в виде буквы латинского алфавита) и нажмите на кнопку **Запустить проверку**.

Kaspersky Security Cloud начнет проверку подключенного устройства.

Как запустить проверку файла или папки из контекстного меню

Чтобы запустить проверку файла или папки из контекстного меню, выполните следующие действия:

1. Правой клавишей мыши нажмите на файле или папке, которые нужно проверить.
2. В открывшемся контекстном меню выберите пункт **Проверить на вирусы**.

Kaspersky Security Cloud начнет проверку выбранного файла или папки.

Как включить или выключить фоновую проверку

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

Фоновая проверка запускается в следующих случаях:

- после обновления антивирусных баз;
- через 30 минут после запуска Kaspersky Security Cloud;
- 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.
- Если проверка во время простоя не выполнялась более десяти дней, проверка не прерывается.
- Компьютер (ноутбук) перешел в режим питания от батареи.

При выполнении фоновой проверки Kaspersky Security Cloud не проверяет файлы, содержимое которых расположено в облачном хранилище OneDrive.

Чтобы включить или выключить фоновую проверку, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Проверка**.

   Откроется окно **Проверка**.
3. В окне **Проверка** нажмите на значок ⚙ в блоке **Фоновая проверка**.

   Откроется окно **Настройки фоновой проверки**.

4. В окне **Настройки фоновой проверки** переведите переключать в положение **Вкл** или **Выкл**.

Как создать расписание проверки

Чтобы создать расписание проверки, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Проверка**.

   Откроется окно **Проверка**.
3. В окне **Проверка** выберите тип проверки и нажмите на значок ⚙.
4. В открывшемся окне по ссылке **Расписание проверки** перейдите в окно **Расписание проверки**.
5. 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.

Как выполнить поиск уязвимостей в программах, установленных на вашем компьютере

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

Чтобы запустить поиск уязвимостей, выполните следующие действия:

1. Откройте главное окно программы.

2. Нажмите на кнопку **Больше функций**, расположенную в нижней части главного окна.

   Откроется окно **Инструменты**.

3. Перейдите в раздел **Управление программами**.

4. По ссылке **Поиск уязвимостей** откройте окно **Поиск уязвимостей**.

5. В окне **Поиск уязвимостей** нажмите на кнопку **Начать поиск**.

Kaspersky Security Cloud начнет проверку вашего компьютера на наличие уязвимостей.

Проверка файлов в облачном хранилище OneDrive

На операционной системе Windows 10 RS3 и выше Kaspersky Security Cloud не проверяет файлы в облачном хранилище OneDrive. Если программа 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 Security Cloud 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 программ и скриптов компоненты Контроль программ и Мониторинг активности скачивают программы 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.

Как восстановить удаленный или вылеченный программой файл

Резервные копии файлов, которые были удалены или вылечены программой Kaspersky Security Cloud, 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 программой файл из резервной копии, которая хранится в Карантине.

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

Kaspersky Security Cloud 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 Kaspersky Security Cloud 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 программой файл, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Больше функций**, расположенную в нижней части главного окна.

   Откроется окно **Инструменты**.
3. В окне **Инструменты** перейдите в раздел **Защита**.
4. В разделе **Защита** по ссылке **Карантин** откройте окно **Карантин**.
5. В открывшемся окне **Карантин** выберите нужный файл в списке и нажмите на кнопку **Восстановить**.

Как восстановить операционную систему после заражения

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

О восстановлении операционной системы после заражения

Если вы подозреваете, что операционная система вашего компьютера была повреждена или изменена в результате действий вредоносных программ 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 программ, неправильная настройка операционной системы, системные сбои или применение неправильно работающих программ – 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, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Больше функций**, расположенную в нижней части главного окна.

   Откроется окно **Инструменты**.
3. Перейдите в раздел **Очистка и оптимизация**.
4. По ссылке **Восстановление после заражения** запустите мастер восстановления после заражения.

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 программ**. 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 программ**, 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 предназначена программа Kaspersky Rescue Disk. Вы можете использовать Kaspersky Rescue Disk для проверки и лечения зараженного компьютера, который нельзя вылечить другим способом (например, с помощью антивирусных программ).

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

Защита электронной почты

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

Настройка Почтового Антивируса

Kaspersky Security Cloud 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).

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

Чтобы настроить Почтовый Антивирус, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. Выберите в разделе **Защита** компонент Почтовый Антивирус.

   В окне отобразятся настройки Почтового Антивируса.
4. Убедитесь, что переключатель в верхней части окна, включающий / выключающий Почтовый Антивирус, включен.
5. Выберите уровень безопасности:

   - **Рекомендуемый**. 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.
   - **Высокий**. При установке этого уровня безопасности Почтовый Антивирус проверяет входящие и исходящие сообщения, вложенные архивы, а также проводит эвристический анализ с уровнем детализации **Глубокий**.
6. В блоке **Действие при обнаружении угрозы** выберите действие, которое Почтовый Антивирус будет выполнять при обнаружении зараженного объекта (например, лечить).

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 Kaspersky Security Cloud. В случае удаления объекта Kaspersky Security Cloud создает его резервную копию и помещает на карантин.

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

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

Блокирование нежелательной почты (спама)

Если вы получаете большое количество нежелательной почты (спама), мы рекомендуем включить компонент Анти-Спам и установить для него уровень безопасности **Рекомендуемый**.

Чтобы включить Анти-Спам и установить уровень безопасности Рекомендуемый, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Защита**.
4. Выберите компонент Анти-Спам.

   В окне отобразятся настройки Анти-Спама.
5. Включите Анти-Спам с помощью переключателя.
6. Убедитесь, что в блоке **Уровень безопасности** установлен уровень безопасности **Рекомендуемый**.

Работа компонента Анти-Спам имеет следующие ограничения:

- Компонент Анти-Спам может анализировать только сообщения, скачиваемые с почтового сервера целиком, независимо от используемого протокола.

- Компонент Анти-Спам не проверяет письма, передаваемые по протоколу MAPI.

При переходе на более новую версию программы компонент Анти-Спам выключается. Вы можете включить компонент вручную.

В некоторых версиях программы для включения компонента Анти-Спам вам необходимо принять условия Положения об обработке данных для Анти-Спама.

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 Security Cloud вы можете защитить от кражи свои персональные данные:

- пароли, имена пользователя и другие регистрационные данные;

- номера счетов и банковских карт.

В состав Kaspersky Security Cloud 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 Веб-Антивирус и Анти-Спам. 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.

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 – программ, регистрирующих нажатие клавиш. Экранная клавиатура позволяет избежать перехвата данных, вводимых с клавиатуры.

Многие программы-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).

Для защиты данных, вводимых с помощью Экранной клавиатуры, после установки Kaspersky Security Cloud необходимо перезагрузить компьютер.

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 и Google Chrome. 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.

.

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 Security Cloud.

Как открыть Экранную клавиатуру

Открыть Экранную клавиатуру можно следующими способами:

- из окна программы;

- из панели инструментов браузеров Microsoft Edge на базе Chromium, Mozilla Firefox или Google Chrome;
- 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 Kaspersky Security Cloud отключает функцию автозаполнения полей ввода на сайтах.

- с помощью комбинации клавиш аппаратной клавиатуры.

Запуск Экранной клавиатуры из окна программы

Чтобы открыть Экранную клавиатуру из окна программы, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Больше функций**, расположенную в нижней части главного окна.

   Откроется окно **Инструменты**.
3. Перейдите в раздел **Безопасность данных**.
4. По ссылке **Экранная клавиатура** откройте Экранную клавиатуру.

Запуск Экранной клавиатуры из панели инструментов браузера

Чтобы открыть Экранную клавиатуру из панели инструментов браузера Microsoft Edge на базе Chromium, Mozilla Firefox или Google Chrome, выполните следующие действия:

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**.

Как настроить отображение значка Экранной клавиатуры

Чтобы настроить отображение значка быстрого вызова Экранной клавиатуры в полях ввода на сайтах, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Дополнительно**.

   В окне отобразятся настройки защиты ввода данных.
4. В блоке **Экранная клавиатура** установите флажок **Открывать Экранную клавиатуру по комбинации клавиш CTRL+ALT+SHIFT+P**.

5. Если вы хотите, чтобы значок вызова Экранной клавиатуры отображался в полях ввода на всех сайтах, установите флажок **Показывать значок быстрого вызова в полях ввода**.

6. 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.

7. 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** откройте 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 **Добавить**.

      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".

Защита ввода данных с аппаратной клавиатуры имеет следующие ограничения:

- Защита ввода данных с аппаратной клавиатуры работает только в браузерах Microsoft Edge на базе Chromium, Mozilla Firefox и Google Chrome. Если вы работаете в других браузерах, данные, которые вы вводите с аппаратной клавиатуры, не защищаются от перехвата.
- Защита ввода данных с аппаратной клавиатуры не работает в браузерах, запущенных в программе 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.

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 Security Cloud.

Ограничения защиты ввода данных

Защита ввода данных в Kaspersky Security Cloud имеет следующие ограничения:

- Защита работает только в браузерах Microsoft Edge на основе Chromium, Mozilla Firefox, Mozilla Firefox ESR и Google Chrome 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 браузере.
    - Страница не находится в списке исключений URL-адресов.
    - Страница содержит поле для ввода пароля, при этом в настройках программы установлен флажок для категории Поля ввода паролей на всех сайтах.
    - Чтобы проверить, установлен ли флажок, перейдите в раздел Дополнительно → Защита ввода данных. В блоке Защита ввода данных с аппаратной клавиатуры нажмите Изменить категории.
- 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 Security Cloud и до первой перезагрузки компьютера программа не перехватывает первый введенный пользователем символ (в любой программе).

Если у вас возникли сложности, отправьте запрос с подробным описанием проблемы в техническую поддержку "Лаборатории Касперского" через My Kaspersky.

Инструкцию по работе с My Kaspersky смотрите в справке.

Как изменить настройки защиты ввода данных с аппаратной клавиатуры

Чтобы настроить защиту ввода данных с аппаратной клавиатуры, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. В разделе **Дополнительно** выберите подраздел **Защита ввода данных**.

   В окне отобразятся настройки защиты ввода данных.
4. В нижней части окна в блоке **Защита ввода данных с аппаратной клавиатуры** установите флажок **Защищать ввод данных с аппаратной клавиатуры**.
5. Откройте окно **Настройки Защиты ввода данных** по ссылке **Изменить категории** в нижней части блока **Защита ввода данных с аппаратной клавиатуры**.
6. Установите флажки для категорий сайтов, на которых нужно защищать данные, вводимые с клавиатуры.

7. Если вы хотите включить или выключить защиту ввода данных с клавиатуры на определенном сайте, выполните следующие действия:

    a. Откройте окно **Исключения для защиты ввода с аппаратной 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 **Добавить**.

Указанный сайт появится в списке в окне **Исключения для защиты ввода с аппаратной клавиатуры**. При открытии указанного сайта будет действовать защита ввода данных в соответствии с настройками.

Проверка безопасности сайта

Kaspersky Security Cloud позволяет проверить безопасность сайта, прежде чем вы перейдете по ссылке на этот сайт. Для проверки сайтов используется компонент *Проверка ссылок.*

Компонент Проверка ссылок проверяет ссылки на веб-странице, открытой в браузере Microsoft Edge на базе Chromium, Google Chrome или Mozilla Firefox. Рядом с проверенной ссылкой Kaspersky Security Cloud 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, опасна по данным "Лаборатории Касперского".
При наведении курсора мыши на значок отображается всплывающее окно с более подробным описанием ссылки.

По умолчанию Kaspersky Security Cloud проверяет ссылки только в результатах поиска. Вы можете включить проверку ссылок на любом сайте.

Чтобы настроить проверку ссылок на сайтах, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. В разделе **Защита** выберите подраздел **Веб-Антивирус**.

   В окне отобразятся настройки Веб-Антивируса.
4. По ссылке **Расширенная настройка** раскройте блок дополнительных настроек Веб-Антивируса.
5. В блоке **Проверка ссылок** установите флажок **Проверять ссылки**.
6. Чтобы Kaspersky Security Cloud 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 Security Cloud не будет проверять содержимое указанных веб-страниц.
8. Чтобы Kaspersky Security Cloud проверял содержимое только определенных веб-страниц, выполните следующие действия:

a. Выберите вариант **Только на указанных сайтах**.

b. По ссылке **Настроить проверяемые сайты** откройте 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 Security Cloud проверяет содержимое веб-страницы).

f. Нажмите на кнопку **Добавить**.

Указанная веб-страница появится в списке в окне **Проверяемые сайты**. Kaspersky Security Cloud будет проверять ссылки на этой веб-странице.

9. Если вы хотите указать дополнительные настройки проверки ссылок, в окне **Дополнительные настройки Веб-Антивируса** в блоке **Проверка ссылок** по ссылке **Настроить проверку ссылок** откройте окно **Проверка ссылок**.

10. Чтобы Kaspersky Security Cloud предупреждал о безопасности ссылок на всех веб-страницах, в блоке **Проверяемые ссылки** выберите вариант **Любые ссылки**.

11. Чтобы Kaspersky Security Cloud 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 Security Cloud будет проверять ссылки на указанных веб-страницах и отображать информации о категориях ссылок в соответствии с выбранными настройками.

Как изменить настройки защищенных соединений

Защищенные соединения – это соединения, которые устанавливаются по протоколам SSL и TLS. По умолчанию программа Kaspersky Security Cloud выполняет проверку таких соединений по запросу компонентов защиты, таких как Почтовый Антивирус, Анти-Спам, Безопасные платежи, Проверка ссылок, Защита от сбора данных, Веб-Антивирус и Анти-Баннер.

Чтобы изменить настройки защищенных соединений, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. Перейдите в раздел **Настройки сети**.
4. Выберите вариант действия при подключении к сайтам по защищенному соединению:
   - **Не проверять защищенные соединения**. Программа не проверяет защищенные соединения.
   - **Проверять защищенные соединения по запросу компонентов защиты**. Программа проверяет защищенные соединения, только если на это будет запрос от компонента Проверка ссылок. Этот вариант действия выбран по умолчанию.
   - **Всегда проверять защищенные соединения**. Программа всегда проверяет защищенные соединения.
5. Выберите вариант действия, если возникают ошибки при проверке защищенных соединений:
   - **Игнорировать**. Если выбран этот вариант, программа разрывает соединение с сайтом, на котором возникла ошибка проверки защищенного соединения.
   - **Спрашивать**. Если выбран этот вариант, при возникновении ошибки проверки защищенного соединения с сайтом, программа показывает уведомление, в котором вы можете выбрать вариант действия:

- **Игнорировать**. Если выбран этот вариант, программа разрывает соединение с сайтом, на котором возникла ошибка проверки.

- **Добавить домен в исключения**. Если выбран этот вариант, программа добавляет адрес сайта в список исключений. Программа не проверяет защищенные соединения на сайтах, которые входят в список исключений. Такие сайты отображаются в окне **Исключения**, которое можно открыть по ссылке **Настроить исключения**.

Этот вариант выбран по умолчанию.

- **Добавить домен в исключения**. Если выбран этот вариант, программа добавляет сайт в список исключений. Программа не проверяет защищенные соединения на сайтах, входящих в список исключений. Такие сайты отображаются в окне **Исключения**, которое можно открыть по ссылке **Настроить исключения**.

6. По ссылке **Настроить исключения** откройте окно **Исключения** 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**.

Программа не будет проверять защищенное соединение с этим сайтом. Обратите внимание, что добавление сайта в список исключений означает, что функциональность проверки этого сайта такими компонентами, как Безопасные платежи, Проверка ссылок, Защита от сбора данных, Веб-Антивирус и Анти-Баннер, может быть ограничена.

О безопасном подключении к сетям Wi-Fi

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 незащищенную сеть Wi-Fi, ваши пароли и другие конфиденциальные данные могут передаваться в открытом текстовом виде. Злоумышленники могут перехватить ваши конфиденциальные данные, узнать номер вашей банковской карты и получить доступ к деньгам.

При подключении к сети Wi-Fi программа проверяет эту сеть. Если сеть Wi-Fi небезопасна, программа предлагает включить Безопасное VPN-соединение через специально выделенный сервер, расположенный в указанном вами регионе. Данные с сайта сначала поступают на выделенный сервер. После этого программа передает их на ваше устройство по зашифрованному безопасному VPN-соединению.

Чтобы использовать компонент Безопасное VPN-соединение, вам нужно запустить программу Kaspersky Secure Connection. Программа Kaspersky Secure Connection устанавливается совместно с Kaspersky Security Cloud.

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 региона подключения 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 запустить программу Kaspersky Secure Connection

Kaspersky Secure Connection устанавливается совместно с Kaspersky Security Cloud. 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 Kaspersky Security Cloud.

Чтобы запустить программу Kaspersky Secure Connection из окна Kaspersky Security Cloud, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Безопасное VPN-соединение**.

   Откроется окно **Безопасное VPN-соединение**.
3. Нажмите на кнопку **Открыть**.

Откроется главное окно программы Kaspersky Secure Connection.

Подробную информацию о работе программы Kaspersky Secure Connection вы можете получить в справке для этой программы.

Настройка уведомлений об уязвимостях сети Wi-Fi

Если на вашем компьютере не установлена программа Kaspersky Secure Connection, Kaspersky Security Cloud показывает уведомление при подключении к сетям Wi-Fi и незащищенной передаче пароля в интернете. Вы можете разрешить или запретить подключение и передачу пароля в окне уведомления.

После того как вы установили программу Kaspersky Secure Connection, настройки показа уведомлений при подключении к сетям Wi-Fi и передачи пароля в незащищенном виде становятся неактивными. Настройки уведомления о подключении к сетям Wi-Fi вы можете настроить в программе Kaspersky Secure Connection.

Чтобы настроить уведомления об уязвимостях сети Wi-Fi, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Защита**.
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 установлена программа Kaspersky Secure Connection.
6. 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.

Защита финансовых операций и покупок в интернете

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

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, Kaspersky Security Cloud предлагает открывать такие сайты в Защищенном браузере.

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

Если вы используете браузеры Microsoft Edge на базе Chromium, Google Chrome, Mozilla Firefox или Internet Explorer, Защищенный браузер запускается в новом окне.

Чтобы обеспечить ряд функций Защищенного браузера, программа использует расширение Kaspersky Protection.

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

Запуск Защищенного браузера невозможен при следующих условиях:

- снят флажок **Включить самозащиту** в разделе **Общие** окна настройки программы;
- в браузере выключено выполнение JavaScript.

Запуск Защищенного браузера в Яндекс.Браузере

Kaspersky Security Cloud поддерживает защиту ваших финансовых операций в Яндекс.Браузере с ограничениями. Для запуска Защищенного браузера программа внедряет в веб-страницу (и в трафик) специальный скрипт. Расширение Kaspersky Protection недоступно. Компоненты Защита от сбора данных и Анти-Баннер работают, но недоступны для настройки в Яндекс.Браузере.

Возможности Защищенного браузера

При работе в Защищенном браузере программа предоставляет защиту от следующих видов угроз:

- Недоверенные модули. Проверка на наличие недоверенных модулей выполняется при каждом переходе на сайт банка или платежной системы.
- Руткиты. Проверка на наличие руткитов выполняется при запуске Защищенного 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 браузера

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

Существуют следующие варианты цветовой индикации рамки окна браузера:

- Зеленый цвет рамки. Означает, что все проверки выполнены успешно. Вы можете продолжить работу в Защищенном браузере.
- Желтый цвет рамки. Означает, что во время проверок были обнаружены проблемы безопасности, которые необходимо устранить.

  Программа 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.

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

О защите от создания снимков экрана

Kaspersky Security Cloud блокирует несанкционированное создание снимков экрана программами-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

Kaspersky Security Cloud блокирует несанкционированный доступ программ к буферу обмена во время проведения платежных операций, предотвращая кражу данных злоумышленниками. Блокировка действует только в случае попыток недоверенных программ получить несанкционированный доступ к буферу обмена. Если вы вручную копируете данные из окна одной программы в окно другой программы (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 браузер запущен на операционной системе Microsoft Windows 10, Kaspersky Security Cloud блокирует работу приложений универсальной платформы Windows с буфером обмена.

Как изменить настройки Безопасных платежей

Чтобы настроить Безопасные платежи, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Защита**.
4. Выберите компонент **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 программа, когда вы впервые открываете в браузере сайт банка или платежной системы:
   - Выберите **Запускать Защищенный браузер**, если хотите, чтобы программа открывала сайт в Защищенном браузере.
   - Выберите **Спрашивать пользователя**, если хотите, чтобы при обращении к сайту программа спрашивала у вас, открывать сайт в Защищенном браузере или нет.
   - Выберите **Не запускать Защищенный браузер**, если хотите, чтобы программа не открывала сайт в Защищенном браузере.
7. В блоке **Дополнительно** в раскрывающемся списке **Для перехода к сайтам из окна Безопасных платежей использовать** выберите браузер, который программа будет запускать в режиме Защищенного 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, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Безопасные платежи**.

   Откроется окно **Безопасные платежи**. Если вы впервые открываете окно, Kaspersky Security Cloud предложит вам ознакомиться с тем, как работают Безопасные платежи. Вы можете пропустить обзор.
3. По ссылке **Добавить сайт в Безопасные платежи** откройте поля для добавления информации о сайте.
4. В поле **Сайт для Безопасных платежей** введите адрес сайта, который нужно открывать в Защищенном браузере.

   > Перед адресом сайта должен быть указан протокол HTTPS (например, https://example.com), по умолчанию используемый Защищенным браузером.
5. Выберите способ запуска Защищенного браузера при открытии этого сайта:
   - Если вы хотите, чтобы сайт каждый раз открывался в Защищенном браузере, выберите вариант **Запускать Защищенный браузер**.
   - Если вы хотите, чтобы программа Kaspersky Security Cloud запрашивала, какое действие выполнять при открытии сайта, выберите вариант **Спрашивать пользователя**.
   - Если вы хотите выключить Безопасные платежи для этого сайта, выберите вариант **Не запускать Защищенный браузер**.

6. По ссылке **Добавить описание** откройте поле **Описание** и введите название или описание этого сайта.

7. 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, выполните следующие действия:

1. Откройте главное окно программы.

2. Нажмите на кнопку **Безопасные платежи**.

   Откроется окно **Безопасные платежи**. Если вы впервые открываете окно, Kaspersky Security Cloud предложит вам ознакомиться с тем, как работают Безопасные платежи. Вы можете пропустить обзор.

3. По ссылке **Оставить отзыв** откройте окно, в котором вы можете написать отзыв о работе с Безопасными платежами.

4. Оцените работу Безопасных платежей по 5-балльной шкале, выбрав от 1 до 5 звезд.

5. Если вы хотите добавить к вашему отзыву комментарий, введите текст комментария в поле **Подробнее**.

6. Нажмите на кнопку **Отправить**.

[Как сообщить о проблеме](#)

Чтобы сообщить о проблеме при работе с Защищенным браузером, выполните следующие действия:

1. Нажмите на ссылку **Сообщить о проблеме** в окне всплывающего сообщения **Kaspersky Security Cloud Защищенный браузер** в нижней части Защищенного браузера.

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

2. В раскрывающемся списке **Проблема** 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 браузер запускается не тогда, когда нужно**. Выберите этот элемент, если в Защищенном браузере открываются сайты, не требующие использования Безопасных платежей.
   - **Не получается авторизоваться на сайте**. Выберите этот элемент, если при попытках авторизоваться на сайте, открытом в Защищенном браузере, возникают ошибки.
   - **Не открывается или неправильно отображается сайт**. Выберите этот элемент, если сайты не открываются в Защищенном браузере 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 запущен Защищенный браузер**. Выберите этот элемент, если в Защищенном браузере не создаются скриншоты.

- **Ошибки во время ввода данных с клавиатуры или из буфера обмена**. Выберите этот элемент, если во время ввода данных в Защищенном браузере возникают ошибки.
- **Не печатается страница, открытая в Защищенном браузере**. 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 браузера появляется сообщение "Не установлены важные обновления операционной системы".
- **В качестве Защищенного запускается другой браузер**. Выберите этот элемент, если Защищенный браузер открывается не в том браузере, в котором вы его запустили.
- **Работает с ошибками**. Выберите этот элемент, если при работе Защищенного браузера возникают ошибки.
- **Другое**. 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 **Подробнее**.

4. Нажмите на кнопку **Отправить**.

Если программе не удается отправить отзыв (например, отсутствует соединение с интернетом), программа 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.

Защита ваших паролей в интернете

В этом разделе содержится информация о том, как вы можете защитить свои пароли.

О защите ваших паролей в интернете

Если вы активный пользователь интернета, вам приходится использовать много различных паролей, например, когда вы посещаете сайты банков, социальных сетей, почтовых сервисов. Большое количество паролей создает неудобство, так как вам нужно вспоминать, какой пароль нужно использовать на этом сайте. Часто в такой ситуации пользователи прибегают к простому решению – используют один простой пароль на различных сайтах. Однако такое решение не является безопасным. Простой пароль, который используется на нескольких сайтах, может быть легко взломан или перехвачен злоумышленниками. Если такое произойдет с паролем от сайта банка, вы рискуете лишиться денежных средств.

Проверка надежности паролей

Когда вы создаете пароль на каком-либо сайте, Kaspersky Security Cloud проверяет, насколько надежен этот пароль, и уведомляет вас об этом. Из окна уведомления вы можете перейти в окно загрузки программы Kaspersky Password Manager. Программу Kaspersky Password Manager можно использовать для создания надежного пароля и хранения паролей.

Защита от использования одинаковых паролей

Когда вы вводите пароль на сайте, где безопасность пароля особенно важна (например, в социальной сети), Kaspersky Security Cloud предлагает вам включить защиту от использования одинаковых паролей.

Если защита от использования одинаковых паролей включена, Kaspersky Security Cloud проверяет, использовался ли ранее пароль, который вы вводите в интернете, на сайтах следующих категорий:

- сайты банков и платежных систем;

- социальные сети;
- почтовые сервисы.

Если пароль, который вы вводите, уже использовался на сайтах этих категорий, Kaspersky Security Cloud уведомляет вас об этом и предлагает создать новый пароль. Вы можете выбрать категории сайтов, для которых необходимо контролировать использование одинаковых паролей.

Если вы используете Kaspersky Password Manager

Если вы скачали и установили программу Kaspersky Password Manager, в Kaspersky Security Cloud выключается защита паролей. Защита паролей выполняется программой Kaspersky Password Manager. Программа Kaspersky Password Manager предназначена для безопасного хранения вашей личной информации: паролей, паспортных данных, финансовых или медицинских сведений. Подробнее о том, как защитить ваши пароли, вы можете прочитать в справке для программы Kaspersky Password Manager. Программа Kaspersky Security Cloud не контролирует создание паролей, не проверяет, используете ли вы пароль от сайтов банков, социальных сетей, почтовых сервисов на других сайтах, и не уведомляет о надежности пароля и об использовании пароля на других сайтах.

Программа Kaspersky Security Cloud не уведомляет об использовании пароля от сайтов банков, социальных сетей, почтовых сервисов на других сайтах, если вы скачали и установили программу Kaspersky Fraud Prevention for Endpoints версии 3.5 и выше.

Настройка безопасности паролей

Чтобы изменить настройки безопасности паролей, выполните следующие действия:

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

   Откроется окно **Настройка**.

3. В разделе **Дополнительно** по ссылке **Безопасность паролей** перейдите в окно **Настройки безопасности паролей**.

4. Установите флажок **Показывать в браузере надежность создаваемого пароля**, если вы хотите, чтобы программа Kaspersky Security Cloud проверяла надежность пароля, который вы создаете на сайте, и уведомляла вас об этом.

   Если у вас установлена программа Kaspersky Password Manager, в уведомлении вам будет предложен надежный пароль. Если эта программа не установлена, мы рекомендуем скачать и установить ее, чтобы всегда создавать надежные пароли.

5. Установите флажок **Предупреждать об использовании одинаковых паролей на сайтах**, если вы хотите, чтобы программа Kaspersky Security Cloud проверяла, использовали ли вы ранее пароль, который вы вводите или создаете, на сайтах банков, социальных сетей, почтовых сервисов.

6. По ссылке **Выбрать категории сайтов** перейдите в окно **Категории сайтов**, если вы хотите выбрать категории сайтов, для которых надо контролировать использование одинаковых паролей.

7. Установите флажки для следующих категорий:

   - **Интернет-банки и платежные системы**. Когда вы создаете или вводите пароль в интернете, программа проверяет, использовали ли вы этот пароль на сайтах банков и платежных систем.

   - **Социальные сети**. Когда вы создаете или вводите пароль в интернете, программа проверяет, использовали ли вы этот пароль в социальных сетях.

   - **Почтовые сервисы**. Когда вы создаете или вводите пароль в интернете, программа проверяет, использовали ли вы этот пароль в почтовых сервисах.

Запуск программы защиты паролей Kaspersky Password Manager

Программа Kaspersky Password Manager предназначена для безопасного хранения и синхронизации паролей между вашими устройствами. Kaspersky Password Manager нужно устанавливать независимо от Kaspersky Security Cloud, например, с помощью ярлыка **Kaspersky Passwords**, который создается на Рабочем столе вашего компьютера в процессе установки Kaspersky Security Cloud.

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 Security Cloud.

Как запустить программу Kaspersky Password Manager из окна Kaspersky Security Cloud

Чтобы запустить программу защиты паролей Kaspersky Password Manager, если она уже установлена, выполните следующие действия:

1. Откройте главное окно программы Kaspersky Security Cloud.
2. Нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне нажмите на кнопку **Запустить**.

Откроется окно программы защиты паролей Kaspersky Password Manager.

Как скачать и установить программу Kaspersky Password Manager

Чтобы скачать и установить программу защиты паролей Kaspersky Password Manager,

воспользуйтесь одним из следующих способов:

- кнопкой **Менеджер паролей** в главном окне Kaspersky Security Cloud;
- кнопкой **Узнать больше** в окне **Центр уведомлений** в разделе **Рекомендации** напротив предложения установить Kaspersky Password Manager.

Kaspersky Security Cloud скачает установочный пакет Kaspersky Password Manager и установит программу на ваш компьютер.

Скачанный установочный пакет Kaspersky Password Manager остается на вашем компьютере вне зависимости от того, установлена ли с его помощью на компьютер программа Kaspersky Password Manager.

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

Защита от сбора информации о ваших действиях в интернете

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

О защите от сбора данных

Некоторые сайты используют сервисы отслеживания, чтобы собирать информацию о ваших действиях в интернете. Затем эта информация анализируется и используется для показа вам рекламных объявлений.

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

В *режиме обнаружения* компонент Защита от сбора данных 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 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 интерфейсе Kaspersky Security Cloud или с помощью расширения Kaspersky Protection в браузере.

Защита от сбора данных имеет следующие ограничения:

- Программа 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 Security Cloud 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 Security Cloud применяет то действие, которое задано в настройках Защиты от сбора данных (запрещает или разрешает сбор данных). Программа отображает информацию о попытке сбора данных в отчетах, но не включает эту информацию в статистику Защиты от сбора данных, отображаемую в браузере.

Запрет на сбор данных

Чтобы запретить сбор данных, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. В разделе **Защита** выберите компонент Защита от сбора данных.

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

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

5. Выберите вариант **Запретить сбор данных**.

   Kaspersky Security Cloud 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, выполните следующие действия:

   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, выполните следующие действия:

1. Откройте главное окно программы.

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

   Откроется окно **Настройка**.

3. В разделе **Защита** выберите компонент Защита от сбора данных.

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

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

5. Выберите вариант **Только собирать статистику**.

Kaspersky Security Cloud 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, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. В разделе **Защита** выберите компонент Защита от сбора данных.

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

   Kaspersky Security Cloud 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**.

"Лаборатория Касперского" 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** откройте окно **Исключения Защиты от сбора данных**.

   c. Нажмите на кнопку **Добавить**.

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

      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

Чтобы просмотреть отчет о попытках сбора данных, выполните следующие действия:

1. Откройте главное окно программы.

2. Нажмите на кнопку **Защита приватности**.

   Откроется окно **Защита приватности**.

   В окне **Защита приватности** в блоке **Защита от сбора данных** 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 программы.

Управление защитой от сбора данных в браузере

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

- включать компонент, если он выключен;
- просматривать статистику обнаруженных попыток сбора данных;
- переходить в окно настройки Защиты от сбора данных;
- запрещать или разрешать сбор данных.

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

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

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

Контроль небезопасных настроек операционной системы

В этом разделе вы узнаете, что такое небезопасные настройки операционной системы, как найти и исправить в операционной системе небезопасные настройки.

О небезопасных настройках операционной системы

Когда вы работаете за компьютером, настройки операционной системы могут изменяться в результате ваших действий или действий программ, которые вы запускаете. Изменение настроек операционной системы может представлять угрозу для безопасности компьютера. Например, если в браузере включен автоматический вход в интернет с текущим именем пользователя и паролем, сторонний сайт может похитить ваш пароль.

Небезопасные настройки операционной системы можно разделить на два типа:

- *Критичные настройки*. Такие настройки приравниваются к уязвимостям операционной системы.
- *Рекомендуемые настройки*. Такие настройки рекомендуется исправить, чтобы повысить безопасность операционной системы.

Kaspersky Security Cloud по умолчанию выполняет поиск небезопасных настроек операционной системы не реже чем раз в день. Если программа Kaspersky Security Cloud обнаружила небезопасные настройки операционный системы, она предложит вам исправить их таким образом, чтобы восстановить безопасность операционной системы. Подробную информацию о каждой небезопасной настройке вы можете получить на сайте Службы технической поддержки "Лаборатории Касперского".

По ссылке в окне уведомления вы можете перейти в окно **Контроль небезопасных настроек**, в котором отображаются обнаруженные небезопасные настройки операционной системы. Информация о небезопасных настройках также отображается в Центре уведомлений. Из Центра уведомлений вы можете перейти к просмотру и исправлению небезопасных настроек.

В окне **Контроль небезопасных настроек** вы можете выполнить следующие действия:

- исправить небезопасные настройки операционной системы;
- игнорировать: оставить небезопасные настройки операционной системы без изменений;
- отменить: вернуть в первоначальное состояние ранее исправленные небезопасные настройки операционной системы.

Программа определяет небезопасные настройки операционной системы для всех учетных записей, существующих на вашем компьютере. Вы можете исправлять небезопасные настройки для других учетных записей на компьютере, только если вы вошли в операционную систему под учетной записью администратора.

> Если вы не являетесь администратором компьютера, вы можете игнорировать небезопасные настройки только для вашей учетной записи. Игнорировать небезопасные настройки всех учетных записей может только администратор компьютера.

Вы можете запустить поиск небезопасных настроек вручную или выключить поиск небезопасных настроек.

Вы можете управлять защитой своего компьютера удаленно и отправить команду на исправление небезопасных настроек с My Kaspersky.

Поиск и исправление небезопасных настроек операционной системы

Чтобы найти и исправить небезопасные настройки операционной системы, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Больше функций**, расположенную в нижней части главного окна.

   Откроется окно **Инструменты**.
3. В окне **Инструменты** перейдите в раздел **Защита**.
4. В разделе **Защита** по ссылке **Контроль небезопасных настроек** перейдите в окно **Контроль небезопасных настроек**.
5. Нажмите на кнопку **Начать поиск**.

   Если в результате поиска обнаружены небезопасные настройки, в окне отобразится ссылка **Обнаружено <N> небезопасных настроек операционной системы**.
6. По ссылке перейдите в окно **Контроль небезопасных настроек**.
7. В окне **Контроль небезопасных настроек** выберите действие с небезопасными настройками:

   - Обнаруженные небезопасные настройки. Выполните одно из следующих действий:
     - Нажмите на кнопку **Исправить все**, чтобы исправить все небезопасные настройки.
     - Нажмите на кнопку **Исправить**, чтобы исправить небезопасную настройку.

- Если исправлению небезопасной настройки мешают открытые программы, нажмите на кнопку **Посмотреть**, чтобы ознакомиться со списком мешающих программ.

  Чтобы закрыть программы, мешающие исправить настройку, выполните одно из следующих действий:

  - Нажмите на кнопку ✕ справа от названия мешающей программы, чтобы закрыть программу в штатном режиме. Если программа обнаружит несохраненные изменения, она предложит сохранить их.
  - Нажмите на ссылку **Закрыть принудительно**, чтобы закрыть все мешающие программы без сохранения данных.

- В раскрывающемся списке рядом с кнопкой **Исправить** выберите вариант **Игнорировать**, чтобы оставить небезопасную настройку без изменений.
- В раскрывающемся списке рядом с кнопкой **Исправить** выберите вариант **Подробнее**, чтобы посмотреть информацию о небезопасной настройке на сайте Службы технической поддержки "Лаборатории Касперского".

- Ранее исправленные небезопасные настройки.
  - Нажмите на кнопку **Отменить**, чтобы вернуть исправленную настройку в первоначальное состояние.
  - В раскрывающемся списке рядом с кнопкой **Отменить** выберите вариант **Подробнее**, чтобы посмотреть информацию о небезопасной настройке на сайте Службы технической поддержки "Лаборатории Касперского".

- Проигнорированные настройки. По ссылке **Показать все** напротив сообщения **<N> проигнорированных настроек** откройте список небезопасных настроек, которые вы оставили без изменений, и нажмите на кнопку **Исправить**.

Выключение поиска небезопасных настроек операционной системы

Чтобы выключить поиск небезопасных настроек операционной системы, выполните следующие действия:

1. Откройте главное окно программы.

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

   Откроется окно **Настройка**.

3. В разделе **Производительность** снимите флажок **Выполнять поиск небезопасных настроек операционной системы**.

Kaspersky Security Cloud не будет выполнять поиск небезопасных настроек операционной системы и показывать уведомления о них.

Защита от баннеров при посещении сайтов

Этот раздел содержит информацию о том, как с помощью Kaspersky Security Cloud 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 программ. Анти-Баннер блокирует баннеры из списка известных баннеров, который входит в состав баз Kaspersky Security Cloud. Вы можете управлять блокировкой баннеров через интерфейс Kaspersky Security Cloud 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:

- Если веб-страницу, на которой расположен баннер, не удалось определить, то Kaspersky Security Cloud 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 Kaspersky Security Cloud запрещает или разрешает отображение баннера с учетом информации о веб-странице, которую удалось определить. Программа 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 JavaScript не поддерживаются браузером Internet Explorer, Kaspersky Security Cloud не может заблокировать некоторые баннеры в этом браузере.

Как включить компонент Анти-Баннер

По умолчанию компонент Анти-Баннер выключен. Вы можете включить его в интерфейсе Kaspersky Security Cloud или с помощью расширения Kaspersky Protection в браузере.

Как включить Анти-Баннер в интерфейсе Kaspersky Security Cloud

Чтобы включить компонент Анти-Баннер в интерфейсе Kaspersky Security Cloud, выполните следующие действия:

1. Откройте главное окно программы.

2. Нажмите на кнопку в нижней части окна программы.

   Откроется окно **Настройка**.

3. Выберите раздел **Защита**.

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, выполните следующие действия:

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 Kaspersky Security Cloud. 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 интерфейсе Kaspersky Security Cloud.

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, выполните следующие действия:

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 через интерфейс Kaspersky Security Cloud

Чтобы запретить баннер через интерфейс Kaspersky Security Cloud, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Защита**.
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** откройте 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 **Добавить**.

    Kaspersky Security Cloud 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, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Защита**.
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 **Разрешенные баннеры** откройте окно **Разрешенные баннеры**.
7. В окне **Разрешенные баннеры** нажмите на кнопку **Добавить**.
8. В открывшемся окне в поле **Маска веб-адреса (URL)** введите адрес или маску адреса баннера.
9. Выберите статус **Активно**.
10. Нажмите на кнопку **Добавить**.

Kaspersky Security Cloud 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, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Защита**.
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** откройте 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 **Добавить**.

    Сайт будет добавлен в список сайтов с разрешенными баннерами. Kaspersky Security Cloud не блокирует баннеры на сайтах из этого списка, даже если баннер добавлен в список запрещенных баннеров.

Как настроить фильтры Анти-Баннера

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

   Откроется окно **Настройка**.
3. Выберите раздел **Защита**.
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** откройте 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. Программа 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.

Защита веб-камеры

Этот раздел содержит информацию о том, как предотвратить наблюдение за вами через веб-камеру компьютера.

О доступе программ к веб-камере

Для защиты веб-камеры от несанкционированного доступа предназначен компонент Защита веб-камеры. Если защита веб-камеры включена и установлен флажок **Запретить всем программам доступ к веб-камере**, Kaspersky Security Cloud блокирует доступ к веб-камере всем программам и показывает уведомление о том, что доступ заблокирован.

Если флажок **Запретить всем программам доступ к веб-камере** снят, Kaspersky Security Cloud контролирует доступ к веб-камере в зависимости от того, в какую группу доверия входит программа, запрашивающая доступ. Kaspersky Security Cloud блокирует доступ к веб-камере программам, которые входят в группы доверия "Сильные ограничения" и "Недоверенные".

Вы можете разрешить доступ к веб-камере программам, входящим в группы "Сильные ограничения" и "Недоверенные", в окне настройки Контроля программ. Если к веб-камере пытается подключиться программа, входящая в группу доверия "Слабые ограничения", Kaspersky Security Cloud показывает уведомление и предлагает вам самостоятельно принять решение о том, предоставлять этой программе доступ к веб-камере или нет.

Если к веб-камере пытается подключиться программа, которой разрешен доступ по умолчанию, Kaspersky Security Cloud показывает уведомление. В уведомлении содержится информация о том, что установленная на компьютере программа (например, Skype) сейчас получает изображение с веб-камеры. В раскрывающемся списке уведомления вы можете запретить доступ программы к веб-камере или перейти к настройке доступа программ к веб-камере. Это уведомление не отображается, если на вашем компьютере уже есть программы, запущенные в полноэкранном режиме.

Также в раскрывающемся списке уведомления о получении видеоданных программой вы можете выключить показ уведомлений или перейти к настройке отображения уведомлений.

Kaspersky Security Cloud по умолчанию разрешает доступ к веб-камере программам, для которых требуется ваше разрешение, если графический интерфейс программы находится в процессе загрузки, выгрузки или не отвечает, и вы не можете вручную разрешить доступ.

Функциональность защиты доступа к веб-камере имеет следующие особенности и ограничения:

- Программа контролирует видео и статические изображения, полученные в результате обработки данных веб-камеры.
- Программа контролирует аудиосигнал, если он является частью видеопотока, получаемого с веб-камеры.
- Программа Kaspersky Security Cloud 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 веб-камер вы можете по ссылке.

Чтобы защита от несанкционированного доступа к веб-камере работала, должен быть включен компонент Контроль программ.

Защита доступа к веб-камере имеет ограничения, если программа установлена на операционной системе Microsoft Windows 10 Anniversary Update (RedStone 1).

Как изменить настройки доступа программ к веб-камере

Чтобы изменить настройки доступа программ к веб-камере, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. В разделе **Защита** выберите компонент Защита веб-камеры.
4. Настройте доступ программ к веб-камере на вашем компьютере:

- Если вы хотите запретить доступ всех программ к веб-камере, установите флажок **Запретить всем программам доступ к веб-камере**.

- Если вы хотите получать уведомление о том, что веб-камеру использует программа, которой это разрешено, установите флажок **Показывать уведомление, когда веб-камеру использует программа, которой это разрешено**.

Как разрешить доступ программы к веб-камере

Чтобы разрешить доступ программы к веб-камере, выполните следующие действия:

1. Откройте главное окно программы.

2. Нажмите на кнопку **Больше функций**.

   Откроется окно **Инструменты**.

3. В окне **Инструменты** перейдите в раздел **Управление программами**.

4. По ссылке **Контроль программ** откройте окно **Контроль программ**.

5. В окне **Контроль программ** по ссылке **Управление программами** откройте окно **Управление программами**.

6. Выберите в списке программу, которой вы хотите разрешить доступ к веб-камере, и двойным щелчком мыши по названию программы откройте окно **Правила программы**.

7. В окне **Правила программы** перейдите на закладку **Права**.

8. В списке категорий прав выберите пункт **Изменение операционной системы** → **Подозрительные изменения в операционной системе** → **Доступ к веб-камере**.

9. В графе **Действие** нажатием на значок откройте меню и выберите пункт **Разрешить**.

10. Нажмите на кнопку **Сохранить**.

Доступ программы к веб-камере будет разрешен, если снят флажок **Запретить всем программам доступ к веб-камере**.

Если флажок **Запретить всем программам доступ к веб-камере** установлен, Kaspersky Security Cloud блокирует доступ программы к веб-камере независимо от группы доверия и настроенного вручную разрешения.

Проверка учетных записей

Этот раздел содержит информацию о том, как проверить, могли ли данные ваших учетных записей попасть в публичный доступ.

О проверке учетных записей

Работая, делая покупки и общаясь в интернете, большинство пользователей заводит учетные записи на различных сайтах. Всегда есть риск, что злоумышленники взломают сайт и получат доступ к пользовательским данным. Если вы используете один и тот же адрес электронной почты и пароль для входа на разные сайты, вероятность утечки ваших данных увеличивается.

С помощью Kaspersky Security Cloud вы можете проверить ваши учетные записи на предмет возможной утечки. Если при проверке будет обнаружено, что ваши данные могли попасть в публичный доступ, программа уведомит вас об этом и покажет список сайтов, с которых могла произойти утечка данных, даты возможной утечки и категории данных, которые могли попасть в публичный доступ.

Проверка учетных записей осуществляется с использованием регулярно пополняющейся базы сайта www.haveibeenpwned.com. При проверке учетных записей "Лаборатория Касперского" не получает данные в открытом виде, использует их только для указанной проверки и не хранит их. При обнаружении утечки Kaspersky Security Cloud не получает доступа к самим пользовательским данным и предоставляет информацию только о категориях данных, которые могли попасть в публичный доступ.

Kaspersky Security Cloud может уведомить вас о возможной утечке следующих категорий данных:

- **Личные данные**: например, паспортные данные, биометрические данные, данные о возрасте.
- **Банковские данные**: например, номера кредитных карт и банковских счетов, информация о балансе кредитных карт и банковских счетов.
- **История активности**: например, токены аутентификации, история паролей.

По умолчанию Kaspersky Security Cloud пытается проверить ваши учетные записи, когда вы авторизуетесь на том или ином сайте. В момент авторизации ваш адрес электронной почты, используемый для входа на сайт, в зашифрованном виде передается в облако KSN, в котором осуществляется проверка по базе, предоставленной сайтом www.haveibeenpwned.com. Если при попытке проверить вашу учетную запись будет обнаружено, что ваши данные могли попасть в публичный доступ, вы получите соответствующее уведомление. Вы можете отключить проверку учетных записей.

Вы можете добавить до 50 учетных записей для автоматической проверки. Списки учетных записей в Kaspersky Security Cloud на разных устройствах не синхронизируются. Проверка добавленных учетных записей выполняется раз в сутки.

> Добавление учетных записей в список для автоматической проверки может быть недоступно в вашем регионе.

Kaspersky Security Cloud периодически проверяет по базе, предоставленной сайтом www.haveibeenpwned.com, адрес электронной почты, привязанный к вашей учетной записи My Kaspersky. Первая такая проверка осуществляется через двое суток после установки программы. Далее проверка производится каждые 24 часа.

> Компонент Проверка учетных записей в тарифном плане Free позволяет вам вручную проверить только учетную запись My Kaspersky. Автоматическая проверка этой и других учетных записей доступна только в тарифных планах Personal и Family.

Как включить и выключить проверку учетных записей

Чтобы включить или выключить проверку учетных записей, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Защита приватности**.

   Откроется окно **Защита приватности**.
3. Включите / выключите компонент Проверка учетных записей с помощью переключателя.

Как проверить, могли ли ваши данные попасть в публичный доступ

Чтобы проверить, могли ли ваши данные попасть в публичный доступ, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Защита приватности**.

   Откроется окно **Защита приватности**.
3. Выберите раздел **Проверка учетных записей**.

   Откроется окно **Проверка учетных записей**.
4. Укажите адрес вашей электронной почты в поле ввода и нажмите на кнопку **Проверить**.

   Kaspersky Security Cloud начнет проверку указанного адреса по базе, предоставленной сайтом www.haveibeenpwned.com. Если при проверке будет обнаружено, что ваши данные могли попасть в публичный доступ, программа уведомит вас об этом и покажет список сайтов, с которых могла произойти утечка данных, даты возможной утечки и категории данных, которые могли попасть в публичный доступ. Нажав на ссылку с категорией данных, вы получите рекомендации о том, как минимизировать последствия возможной утечки этих данных.

   Используя Kaspersky Security Cloud, вы можете проверить на предмет возможной утечки данных не только свои, но и другие учетные записи, например, учетные записи ваших близких и друзей.

Как создать список учетных записей для автоматической проверки

Чтобы создать список учетных записей для автоматической проверки, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Защита приватности**.

   Откроется окно **Защита приватности**.
3. Выберите раздел **Проверка учетных записей**.

   Откроется окно **Проверка учетных записей**.
4. Выполните одно из следующих действий:

   - В поле ввода укажите электронный адрес учетной записи, которую вы хотите добавить в список для автоматической проверки, и нажмите на кнопку **Проверить**.
   - В списке **Авторизации в интернете** нажмите на значок + напротив выбранной учетной записи.

   Добавленная вами запись отобразится в списке **Проверяем регулярно**.

Добавление учетных записей в список для автоматической проверки может быть недоступно в вашем регионе.

Защита детей

В этом разделе вы узнаете, как вы можете защитить ваших детей в реальном и виртуальном мире.

О защите детей с помощью Kaspersky Safe Kids

Если на вашем компьютере установлена программа Kaspersky Security Cloud, вы имеете возможность бесплатно воспользоваться решением, которое поможет защитить вашего ребенка – *Kaspersky Safe Kids*.

О решении Kaspersky Safe Kids

Kaspersky Safe Kids – мультиплатформенное решение, которое помогает вам следить за безопасностью ребенка в реальном и виртуальном мире. Вы решаете, что будет безопасным для вашего ребенка: какие сайты он может посещать, сколько часов проводить за компьютером или со смартфоном, на какой территории ему разрешено находиться. Программа контролирует, чтобы ребенок соблюдал установленные вами правила.

Kaspersky Safe Kids подходит для устройств под управлением операционных систем Windows, macOS, Android и iOS. Установив Kaspersky Safe Kids на ваши устройства и на устройства, которым пользуется ребенок, вы можете управлять приложением на устройствах ребенка через вашу учетную запись My Kaspersky, а также через приложение в родительском режиме на вашем мобильном устройстве.

Программа Kaspersky Safe Kids доступна в двух версиях: бесплатной и Премиум.

Чтобы использовать программу Kaspersky Safe Kids, вам требуется скачать установочный пакет программы из интернета и вручную установить программу на компьютере.

Установить и настроить программу Kaspersky Safe Kids можно только под учетной записью владельца подписки на Kaspersky Security Cloud.

Если вы используете Kaspersky Safe Kids

Ребенок может выключить Kaspersky Safe Kids средствами Kaspersky Security Cloud. Чтобы этого не произошло, рекомендуется установить пароль на изменение настроек Kaspersky Security Cloud.

Если вы вошли в операционную систему под учетной записью, которая привязана к профилю ребенка в программе Kaspersky Safe Kids, Kaspersky Security Cloud перестает показывать следующие уведомления:

- уведомления о новостях безопасности;
- уведомления о том, что в операционной системе обнаружены небезопасные настройки;
- уведомления о том, что текущее устройство подключилось к сети Wi-Fi;
- уведомления о том, что к домашней сети Wi-Fi подключилось какое-либо устройство;
- уведомления в браузере о том, что пароль, который вы вводите на сайте, недостаточно надежен;
- уведомления о том, что пароль, который вы вводите на сайте, вы уже использовали на другом сайте.

Вы можете включить показ уведомлений, установив флажок **Показывать уведомления в учетной записи ребенка** в окне **Настройки уведомлений** (**Настройка** → **Интерфейс** → **Уведомления**).

> Возможность скачать и запускать программу Kaspersky Safe Kids в интерфейсе Kaspersky Security Cloud зависит от тарифного плана программы Kaspersky Security Cloud. Программа Kaspersky Safe Kids доступна только в программе Kaspersky Security Cloud — Family и недоступна в программе Kaspersky Security Cloud — Personal.

Настройки Родительского контроля не сохраняются и не могут быть использованы в Kaspersky Safe Kids, если вы ранее использовали Родительский контроль в программах Kaspersky Internet Security или Kaspersky Total Security, а потом перешли к использованию программы Kaspersky Security Cloud.

Программа Kaspersky Safe Kids доступна не во всех регионах.

Как запустить программу Kaspersky Safe Kids

Как скачать и установить программу Kaspersky Safe Kids

Чтобы скачать и установить программу Kaspersky Safe Kids, если она не установлена, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Защита детей**.

   Откроется окно **Защита детей**.
3. Нажмите на кнопку **Скачать и установить**.

   Kaspersky Security Cloud скачает установочный пакет Kaspersky Safe Kids и установит программу на ваш компьютер.

Как запустить программу Kaspersky Safe Kids

Чтобы запустить программу Kaspersky Safe Kids, если она установлена, выполните следующие действия:

1. Откройте главное окно программы Kaspersky Security Cloud.
2. Нажмите на кнопку **Защита детей**.
3. В открывшемся окне нажмите на кнопку **Открыть**.

Откроется окно программы Kaspersky Safe Kids.

Использование Kaspersky Safe Kids

Первоначальная настройка и использование программы Kaspersky Safe Kids описаны в справке Kaspersky Safe Kids.

Чтобы перейти к справке Kaspersky Safe Kids, выполните следующие действия:

1. Откройте главную страницу Kaspersky Online Help.

2. В блоке **Kaspersky Safe Kids** в раскрывающемся списке выберите операционную систему устройства, на которое установлена программа.

   Откроется справка Kaspersky Safe Kids для выбранной операционной системы.

3. При необходимости смените язык справки с помощью раскрывающегося списка в верхней части страницы.

Устройства в моей сети

Этот раздел содержит информацию о том, как с помощью Kaspersky Security Cloud узнать, какие устройства подключены к вашей проводной сети Ethernet и сети Wi-Fi.

О компоненте Устройства в моей сети

Подобрав пароль или взломав доступ к вашей домашней сети, злоумышленники могут воспользоваться вашим интернетом или похитить ваши данные. Kaspersky Security Cloud защищает ваши проводные сети Ethernet и сети Wi-Fi от несанкционированного подключения.

Когда устройство подключается к вашей сети, Kaspersky Security Cloud уведомляет вас об этом и спрашивает, хотите ли вы посмотреть устройства, подключенные к этой сети:

- Если вы соглашаетесь, Kaspersky Security Cloud показывает список устройств, подключенных к этой сети, и уведомляет вас, если подключилось новое устройство.

- Если вы отказываетесь, Kaspersky Security Cloud не уведомляет вас о повторных подключениях к этой сети и не отображает список подключенных устройств.

Вы можете отказаться от контроля устройств в вашей сети в любое время. Kaspersky Security Cloud перестанет отображать устройства в этой сети и уведомлять вас о подключении к этой сети новых устройств.

Даже одно незащищенное устройство в домашней сети снижает защиту других ваших устройств. На My Kaspersky вы можете посмотреть, какие программы "Лаборатории Касперского" установлены на других устройствах, подключенных к одной учетной записи My Kaspersky. Если вы и ваши близкие используете программу по тарифному плану Family, вы также сможете увидеть, какие программы "Лаборатории Касперского" установлены на устройствах ваших близких. Вы можете при необходимости перейти на My Kaspersky и установить на свои устройства программы "Лаборатории Касперского".

Вы можете выключить компонент Устройства в моей сети. После выключения компонента Kaspersky Security Cloud больше не уведомляет вас о подключении к вашим сетям.

Узнать о том, какие еще есть способы защиты при подключении к сетям Wi-Fi, вы можете на сайте Технический поддержки .

Как включить и выключить компонент Устройства в моей сети

Чтобы включить или выключить компонент Устройства в моей сети, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Защита**.
4. Выберите компонент Сетевой экран.
5. Выполните одно из следующих действий:

   - Чтобы включить компонент Устройства в моей сети, установите флажок **Показывать устройства, подключенные к моим сетям**.
   - Чтобы отключить компонент Устройства в моей сети, снимите флажок **Показывать устройства, подключенные к моим сетям**.

Как просмотреть устройства в моей сети

Kaspersky Security Cloud отображает следующую информацию об устройствах, подключаемых к вашей сети Wi-Fi или проводной сети Ethernet:

- имя устройства;
- производитель устройства;
- тип устройства (например: компьютер, мобильное устройство, роутер, игровая консоль или видеокамера);
- операционная система, установленная на устройстве;
- MAC-адрес (уникальный сетевой идентификатор устройства);
- IP-адрес устройства;
- время последнего обнаружения отключенных устройств в сети;
- программы "Лаборатории Касперского", установленные на устройстве (для устройств, защищенных по тарифным планам Personal и Family, и подключенных к одной учетной записи на My Kaspersky).

Чтобы просмотреть устройства, подключенные к вашей сети, выполните следующие действия:

1. Откройте главное окно программы.
2. По значку сети в нижней части окна ( или  или  , в зависимости от типа обнаруженной сети) перейдите в окно **Устройства в моей сети**.

   В окне **Устройства в моей сети** отображаются:

   - Устройства, подключенные к вашей сети в данный момент.

- Устройства, которые были подключены к вашей сети какое-то время назад.
- Статус устройств в сети:
  - подключенные устройства обозначаются зеленым цветом;
  - отключенные устройства обозначаются серым цветом;
  - новые устройства отмечены надписью **Новое**.

Чтобы изменить имя устройства, выполните следующие действия:

1. Выберите нужное устройство из списка устройств в окне **Устройства в моей сети**.

   Откроется окно, в котором отображаются сведения об этой устройстве.

2. Введите новое имя устройства в поле **Имя устройства**.

Чтобы изменить тип устройства, выполните следующие действия:

1. Выберите нужное устройство из списка устройств в окне **Устройства в моей сети**.

   Откроется окно, в котором отображаются сведения об этой устройстве.

2. Выберите нужный пункт раскрывающегося списка **Тип устройства**.

Как запретить устройству доступ в сеть

1. Откройте главное окно программы.
2. По значку сети в нижней части окна (или или , в зависимости от типа обнаруженной сети) перейдите в окно **Устройства в моей сети**.

3. В разделе **Моя сеть** перейдите по ссылке **Устройства в моей сети**.

4. В окне **Устройства в моей сети** выберите устройство, которое хотите отключить.

5. В правой части окна найдите MAC-адрес устройства.

6. Заблокируйте MAC-адрес устройства в настройках вашего роутера. Руководство пользователя для вашего роутера смотрите на сайте производителя.

После блокировки MAC-адреса устройство не сможет подключиться к вашей сети.

Как удалить из списка сеть, к которой нет подключения

1. Откройте главное окно программы.

2. По значку сети в нижней части окна (или или , в зависимости от типа обнаруженной сети) перейдите в окно **Устройства в моей сети**.

3. Разверните список сетей и нажмите на кнопку напротив той сети, которую вы хотите удалить.

Сеть будет удалена из списка.

Как отключить уведомления о подключении устройств к моей сети

Чтобы отключить уведомления о подключении устройств к сети, выполните следующие действия:

1. Откройте главное окно программы.

2. По значку сети в нижней части окна (или или , в зависимости от типа обнаруженной сети) перейдите в окно **Устройства в моей сети**.

3. В окне **Устройства в моей сети** напротив сети нажмите на кнопку и выберите пункт **Отключить уведомления**.

Программа больше не будет показывать вам уведомления, если к этой сети будут подключаться какие-либо устройства.

Также вы можете отключить уведомления для выбранной сети, когда программа показывает вам уведомление, что к этой сети подключается устройство. Для этого в окне уведомления нажмите на ссылку **Отключить уведомления для этой сети**.

Как отправить отзыв о компоненте Устройства в моей сети

Чтобы отправить в "Лабораторию Касперского" отзыв о работе компонента Устройства в моей сети, выполните следующие действия:

1. Откройте главное окно программы.

2. По значку сети в нижней части окна (или или , в зависимости от типа обнаруженной сети) перейдите в окно **Устройства в моей сети**.

3. В окне **Устройства в моей сети** нажмите на кнопку и выберите пункт **Оставить отзыв**.

   Откроется окно **Помогите нам стать лучше! Оставьте свой отзыв**.

4. Оцените работу компонента по 5-балльной шкале, выбрав от 1 до 5 звезд.

5. Если вы поставили компоненту от 3 до 5 звезд, выполните следующие действия:

   a. Если вы хотите добавить к вашему отзыву комментарий, введите его в поле **Подробнее**.

b. Установите флажок **Я согласен предоставить свои персональные данные, а именно уникальный идентификатор своего компьютера, для повышения качества программного обеспечения и принимаю условия Политики конфиденциальности**.

6. Если вы поставили компоненту от 1 до 2 звезд, выполните следующие действия:

a. Если вы хотите сообщить в "Лабораторию Касперского" о проблеме с компонентом Устройства в моей сети, выберите наиболее близкую по смыслу тему из раскрывающегося списка **Тема**.

Вы можете выбрать один из следующих элементов списка:

- **Неудобно пользоваться**. Выберите этот элемент, если вы испытываете неудобства при использовании компонента Устройства в моей сети.
- **Программа долго ищет устройства в сети**. Выберите этот элемент, если компонент Устройства в моей сети работает слишком медленно.
- **Программа неправильно определяет устройства в сети**. Выберите этот элемент, если программа неправильно определяет названия и / или типы устройств, подключенных к сети Wi-Fi или проводной сети Ethernet.
- **Много сообщений о новых устройствах в сети**. Выберите этот элемент, если программа показывает вам слишком много уведомлений о новых устройствах в сети Wi-Fi или проводной сети Ethernet.
- **Снижается производительность компьютера**. Выберите этот элемент, если использование компонента Устройства в моей сети замедляет работу вашего компьютера.
- **Нельзя настроить компонент**. Выберите этот элемент, если у вас возникли трудности с настройкой компонента Устройства в моей сети.
- **Другое**. Выберите этот элемент, если ваша проблема не относится к указанным в других пунктах.

b. Если вы хотите добавить к вашему отзыву комментарий, введите его в поле **Подробнее**.

c. Установите флажок **Я согласен предоставить свои персональные данные, а именно уникальный идентификатор своего компьютера, для повышения качества программного обеспечения и принимаю условия Политики конфиденциальности**.

7. Нажмите на кнопку **Отправить**.

При отправке "Лаборатория Касперского" получает и обрабатывает следующую информацию:

- Ваш отзыв, который содержит оценку работы компонента, тему проблемы и комментарий.
- Информацию об операционной системе и ее версии.
- Информацию об установленной программе и ее версии.

"Лаборатория Касперского" получает и обрабатывает эту информацию в зашифрованном виде с целью анализа ошибок и улучшения работы компонента Устройства в моей сети. "Лаборатория Касперского" не требует указывать персональные данные при отправке отзыва и не собирает их. Подробная информация об обработке персональных данных представлена в Политике конфиденциальности "Лаборатории Касперского" .

Работа с неизвестными программами

С помощью Kaspersky Security Cloud вы сможете снизить риски, связанные с использованием неизвестных программ (например, риски заражения компьютера вирусами и другими программами, представляющими угрозу).

В состав Kaspersky Security Cloud входят компоненты и инструменты, позволяющие проверить репутацию программы и контролировать активность программы на вашем компьютере.

Проверка репутации программы

Kaspersky Security Cloud позволяет проверять репутацию программ у пользователей во всем мире. В состав репутации программы входят следующие показатели:

- название производителя;
- информация о цифровой подписи (доступно при наличии цифровой подписи);
- информация о группе, в которую программа помещена Контролем программ или большинством пользователей Kaspersky Security Network;
- количество пользователей Kaspersky Security Network, использующих программу (доступно, если программа отнесена к группе Доверенные в базе Kaspersky Security Network);
- время, когда программа стала известна в Kaspersky Security Network;
- страны, в которых программа наиболее распространена.

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

Чтобы узнать репутацию программы,

откройте контекстное меню исполняемого файла программы и выберите пункт **Посмотреть репутацию в KSN**.

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

Контроль действий программы на компьютере и в сети

Компонент Контроль программ предотвращает выполнение программами 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.

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

При работе на 64-разрядных операционных системах недоступны для настройки права программ 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 программ;
- изменение системных модулей (KnownDlls);
- запуск драйвера.

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

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

Сетевую активность программ контролирует компонент Сетевой экран.

При первом запуске программы на компьютере Контроль программ проверяет ее безопасность и помещает в одну из групп ("Доверенные", "Недоверенные", "Сильные ограничения" или "Слабые ограничения"). Группа определяет правила, которые Kaspersky Security Cloud применяет для контроля активности этой программы.

Kaspersky Security Cloud помещает программы в группы доверия ("Доверенные", "Недоверенные", "Сильные ограничения" или "Слабые ограничения"), только если включен компонент Контроль программ или Сетевой экран, а также когда включены оба эти компонента. Если оба эти компонента выключены, функциональность распределения программ по группам доверия не работает.

Вы можете изменить правила контроля действий программы вручную.

Правила, которые вы создаете для программ, наследуются дочерними программами. Например, если вы запретили любую сетевую активность программе cmd.exe, этот запрет будет распространятся на программу notepad.exe, если она была запущена с помощью cmd.exe. При опосредованном запуске программы (если программа не является дочерней по отношению к программе, из которой она запускается), правила унаследованы не будут.

Начиная с версии Kaspersky Security Cloud 4, из программы был исключен компонент Режим Безопасных программ. Если вы хотите продолжать использовать этот компонент, вы можете вернуться на предыдущую версию программы.

Как изменить настройки Контроля программ

Чтобы изменить настройки Контроля программ, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Защита**.
4. Выберите компонент **Контроль программ**.
5. В окне **Контроль программ** по ссылке **Управление программами** откройте окно **Управление программами**.

6. Выберите нужную программу в списке и двойным щелчком мыши по названию программы откройте окно **Правила программы**.

7. Чтобы настроить правила доступа программы 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**, **Выбирать действие автоматически** или **Запретить**).

8. Чтобы настроить права программы 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**, **Выбирать действие автоматически** или **Запретить**).

9. Чтобы настроить права программы 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 программы из проверки Контролем программ, на закладке **Исключения** установите флажки для действий, которые не нужно контролировать.

11. Нажмите на кнопку **Сохранить**.

    Все исключения, созданные в правилах контроля программ, доступны в окне настройки Kaspersky Security Cloud в разделе **Угрозы и исключения**.

Компонент Контроль программ будет отслеживать и ограничивать действия программы в соответствии с настройками.

О защите аудиосигнала, поступающего с устройств записи звука

Злоумышленники могут пытаться получить аудиосигнал с устройств записи звука с помощью специальных программ. *Устройства записи звука* – это микрофоны, подключаемые к компьютеру или встроенные в компьютер, способные передавать аудиопоток через интерфейс звуковой карты ("на вход"). Kaspersky Security Cloud контролирует получение программами аудиосигнала с устройств записи звука и защищает аудиосигнал от несанкционированного перехвата.

По умолчанию Kaspersky Security Cloud запрещает программам из групп доверия "Недоверенные" и "Сильные ограничения" получать аудиосигнал, поступающий с подключенных к компьютеру устройств записи звука. Вы можете вручную разрешать программам получать аудиосигнал с устройств записи звука.

Если к устройству записи звука обращается программа из группы доверия "Слабые ограничения", Kaspersky Security Cloud показывает уведомление и предлагает вам самостоятельно решить, разрешать такой программе получать аудиосигнал с устройства записи звука или запрещать. Если Kaspersky Security Cloud не может показать такое уведомление (например, еще не загрузился графический интерфейс Kaspersky Security Cloud), программе из группы доверия "Слабые ограничения" разрешается получение аудиосигнала с устройства записи звука.

Для всех программ, входящих в группу "Доверенные", получение аудиосигнала с устройств записи звука разрешено по умолчанию.

Функциональность защиты аудиосигнала имеет следующие особенности:

- Для работы функциональности необходимо, чтобы был включен компонент Контроль программ.
- При изменении настроек доступа программы к устройствам записи звука (например, программе было запрещено получение аудиосигнала в окне настроек Контроля программ), чтобы программа перестала получать аудиосигнал, требуется перезапуск этой программы.
- Контроль получения аудиосигнала с устройств записи звука не зависит от настроек доступа программ к веб-камере.

- Kaspersky Security Cloud защищает доступ только к встроенным микрофонам и внешним микрофонам. Другие устройства передачи звука не поддерживаются.

- Kaspersky Security Cloud разрешает программе получение аудиосигнала и не показывает никаких уведомлений, если программа начала получать аудиосигнал до запуска Kaspersky Security Cloud, или если вы поместили программу в группу "Недоверенные" или "Сильные ограничения" после того, как программа начала получать аудиосигнал.

Программа Kaspersky Security Cloud не гарантирует защиту аудиосигнала, передаваемого с таких устройств, как DSLR-камеры, портативные видеокамеры, экшн-камеры.

Как изменить настройки защиты аудиосигнала

Чтобы изменить настройки защиты аудиосигнала, выполните следующие действия:

1. Откройте главное окно программы.

2. Нажмите на кнопку **Больше функций**, расположенную в нижней части главного окна.

   Откроется окно **Инструменты**.

3. Перейдите в раздел **Управление программами**.

4. По ссылке **Контроль программ** откройте окно **Контроль программ**.

5. По ссылке **Управление программами** откройте окно **Управление программами**.

6. Выберите программу в списке, которой вы хотите разрешить доступ к устройствам записи звука, и откройте окно **Правила программы** двойным щелчком мыши.

7. В окне **Правила программы** перейдите на закладку **Права**.

8. В списке категорий прав выберите пункт **Изменение операционной системы → Подозрительные изменения в операционной системе → Доступ к устройствам записи звука**.

9. В графе **Действие** нажмите на значок и выберите один из пунктов меню:

   - Чтобы разрешить программе получение аудиосигнала, выберите пункт **Разрешить**.

   - Чтобы запретить программе доступ к аудиосигналу, выберите пункт **Запретить**.

10. Если вы хотите получать уведомления о том, что программе был запрещен или разрешен доступ к аудиосигналу, в графе **Действие** нажмите на значок и выберите пункт **Записывать в отчет**.

11. Нажмите на кнопку **Сохранить**.

Как изменить настройки Менеджера программ

Чтобы изменить настройки Менеджера программ, выполните следующие действия:

1. Откройте главное окно программы.

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

   Откроется окно **Настройка**.

3. Выберите раздел **Защита**.

4. По ссылке **Менеджер программ** перейдите в окно **Настройки Менеджера программ**.

5. Включите переключатель **Менеджер программ**, чтобы изменения вступили в силу и компонент защиты Менеджер программ начал работать.

6. В блоке настроек **Помощник по установке** установите флажок **Во время установки программ автоматически снимать флажки установки дополнительных программ. Предупреждать при попытке установить дополнительные программы**, чтобы запретить установку дополнительного программного обеспечения при установке новых программ. Если при установке новой программы будут предотвращены нежелательные действия, Kaspersky Security Cloud уведомит вас об этом.

   Если флажок **Во время установки программ автоматически снимать флажки установки дополнительных программ** снят после того, как вы уже запустили установку какой-либо программы, помощник по установке продолжит свою работу в рамках текущей установки. Флажки напротив программ, предлагаемых к дополнительной установке, будут сняты, а сами дополнительные программы не будут устанавливаться. При последующей установке программ эта функциональность работать не будет. Дополнительные программы будут устанавливаться совместно с основной.

7. Установите флажок **Не отображать шаги установки, которые могут содержать рекламу или предложения об установке дополнительных программ**, чтобы запретить показ шагов установки, содержащих рекламу, во время установки на компьютер новых программ. Если такие шаги установки будут удалены, Kaspersky Security Cloud уведомит вас об этом.

Обновление программ, установленных на компьютере

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

Об обновлении программ

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

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

Kaspersky Security Cloud подразделяет обновления программ на два типа:

- *Важные* – это обновления, которые устраняют уязвимости установленных программ и повышают безопасность вашего компьютера.

- *Рекомендуемые* – это обновления, которые улучшают функциональность и / или вносят изменения в установленные программы.

Kaspersky Security Cloud регулярно выполняет поиск обновлений. Когда Kaspersky Security Cloud находит новое обновление для установленной на компьютере программы, Kaspersky Security Cloud 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 программ вручную.

По умолчанию Kaspersky Security Cloud автоматически скачивает и устанавливает все обновления для известных программ, если для этого от вас не требуется принимать новое лицензионное соглашение.

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

Для обновления некоторых программ вам могут потребоваться права администратора на компьютере.

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

Перед первым поиском обновлений для программ Kaspersky Security Cloud может потребоваться обновление баз и программных модулей.

Как изменить настройки обновления программ

Чтобы изменить настройки обновления программ, выполните следующие действия:

1. Откройте главное окно программы.

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

Откроется окно **Настройка**.

3. В разделе **Защита** выберите компонент Обновление программ.

   Откроется окно **Настройки обновления программ**.

4. Если вы не хотите, чтобы программа Kaspersky Security Cloud автоматически скачивала и устанавливала обновления программ, 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.

5. В блоке **Искать обновления для программ** выберите, какие обновления программ будет скачивать и устанавливать Kaspersky Security Cloud:

   - Выберите вариант **Важные обновления, которые повышают безопасность компьютера**, чтобы программа Kaspersky Security Cloud устанавливала только важные обновления, которые устраняют уязвимости программ и повышают безопасность вашего компьютера.

   - Выберите вариант **Все обновления для известных программ**, чтобы программа Kaspersky Security Cloud устанавливала все обновления программ.

Поиск обновлений для программ

Чтобы запустить поиск обновлений для программ, выполните следующие действия:

1. Откройте главное окно программы.

2. Нажмите на кнопку **Больше функций**.

   Откроется окно **Инструменты**.

3. Перейдите в раздел **Управление программами**.

4. По ссылке **Обновление программ** перейдите в окно **Обновление программ**.

5. Нажмите на кнопку **Начать поиск**.

Запустится поиск обновлений для программ. Информация о результатах поиска отобразится в окне.

Как настроить режим поиска обновлений

Чтобы настроить режим поиска обновлений для установленных программ, выполните следующие действия:

1. Откройте главное окно программы.

2. Нажмите на кнопку ⚙.

3. Выберите раздел **Защита**.

4. Выберите компонент **Обновление программ**.

   Откроется окно **Настройки обновления программ**.

5. В блоке **Обновление** установите флажок **Включить поиск обновлений для программ**.

6. По ссылке **Задать режим поиска обновлений** перейдите в окно **Режим поиска обновлений**.

7. В раскрывающемся списке **Искать обновления** выберите один из следующих пунктов:

   - **Автоматически**. Если вы выберете этот пункт, Kaspersky Security Cloud будет выполнять поиск обновлений для программ минимум раз в сутки согласно внутренним настройкам программы.

   - **По минутам** / **По часам** / **По дням** / **Еженедельно** / **Каждый месяц** / **В указанное время**. Если вы выберете один из этих пунктов, Kaspersky Security Cloud будет запускать поиск обновлений по заданному вами расписанию, с точностью до минуты. При выборе

одного из этих вариантов доступен флажок **Отложить запуск после старта программы на** N **минут**.

- **После запуска программы**. Kaspersky Security Cloud будет выполнять поиск обновлений для программ после своего запуска, спустя столько минут, сколько указано в поле **Запускать через** N **минут**.

- **После каждого обновления**. Kaspersky Security Cloud будет выполнять поиск обновлений для программ после загрузки и установки нового пакета обновлений Kaspersky Security Cloud.

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, программа будет запускать поиск обновлений только в заданное по расписанию время, когда компьютер включен.

9. Установите флажок **Искать обновления для программ только в случае, когда компьютер заблокирован или включена экранная заставка**, чтобы запускать поиск обновлений, только если вы не работаете с компьютером, и не занимать дополнительные ресурсы компьютера во время вашей работы. Если флажок не установлен, программа будет запускать поиск в заданное по расписанию время вне зависимости от того, работаете вы с компьютером или нет.

10. Нажмите на кнопку **Сохранить**, чтобы сохранить настройки.

Просмотр списка обновлений для программ

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

Чтобы просмотреть список, сформированный в результате поиска обновлений программ, выполните следующие действия:

1. Откройте главное окно программы.

2. Нажмите на кнопку **Подробнее** в верхней части окна.

   Откроется окно **Центр уведомлений**.

3. В разделе **Защита** в строке с сообщением о найденных обновлениях для программ нажмите на кнопку **Показать**.

   Откроется окно **Обновление программ**, которое содержит список найденных обновлений для программ.

4. Если вы хотите обновить все программы, которые отображаются в списке, нажмите на кнопку **Обновить все** (доступно не во всех регионах).

5. Если вы хотите принять решение по каждой программе, которую предлагается обновить, выполните одно из следующих действий:

   - Нажмите на кнопку **Обновить** в строке с программой, если хотите обновить эту программу.

     > Перед обновлением программы рекомендуется ознакомиться с ее лицензионными соглашениями. Лицензионные соглашения доступны в раскрывающемся списке **Лицензионные соглашения**. По умолчанию язык лицензионного соглашения соответствует языку, заданному в интерфейсе программы. Если лицензионное соглашение на языке интерфейса программы недоступно, его текст будет представлен на языке интерфейса Kaspersky Security Cloud. 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 эту программу**, если хотите, чтобы программа Kaspersky Security Cloud не уведомляла вас о появлении обновлений для выбранной программы.

     Выбранная программа будет перемещена в список исключений. Kaspersky Security Cloud не будет уведомлять о появлении новых обновлений для этой программы.

   - По кнопке  откройте меню и выберите элемент **Пропустить это обновление**, если хотите, чтобы программа Kaspersky Security Cloud не уведомляла вас о выбранном обновлении.

     Выбранное обновление программы будет перемещено в список исключений. Kaspersky Security Cloud уведомит вас о появлении нового обновления для этой программы.

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

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

Интерфейс окна, обновление программ и просмотр Лицензионных соглашений могут отличаться в зависимости от языка локализации Kaspersky Security Cloud.

Удаление обновления или программы из списка исключений

Просматривая список обновлений для программ, вы можете пропускать как уведомления об отдельных обновлениях, так и уведомления обо всех обновлениях для определенных программ. Kaspersky Security Cloud помещает такие обновления и программы в список исключений.

Чтобы удалить обновление или программу из списка исключений, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. В разделе **Защита** выберите компонент Обновление программ.

   Откроется окно **Настройки обновления программ**.
4. По ссылке **Исключения** откройте окно **Исключения**.

   В списке **Исключения** содержатся программы и обновления, для которых вы указали, что их не надо обновлять, и отдельные обновления программ, которые вы не установили.

5. Выберите в списке обновление или программу и нажмите на кнопку **Удалить из списка**.

При следующем поиске обновлений Kaspersky Security Cloud уведомит вас о наличии обновлений для программ, которые вы удалили из списка исключений.

Удаление несовместимых программ

Этот раздел содержит информацию о том, как Kaspersky Security Cloud помогает удалить с компьютера программы, несовместимые с Kaspersky Security Cloud.

Об удалении несовместимых программ

Kaspersky Security Cloud регулярно проверяет ваш компьютер на наличие несовместимых программ. Обнаружив такую программу, Kaspersky Security Cloud вносит ее в список несовместимых программ. Вы можете просмотреть этот список и принять решение, как поступить с несовместимыми программами.

Рекомендуется удалять с компьютера несовместимые программы, иначе Kaspersky Security Cloud не сможет защитить ваш компьютер в полной мере.

Причины несовместимости сторонней программы с Kaspersky Security Cloud могут быть следующие:

- Программа конфликтует с Файловым Антивирусом.
- Программа конфликтует с Сетевым экраном.
- Программа конфликтует с Анти-Спамом.
- Программа препятствует защите сетевого трафика.
- Программа конфликтует с Виртуальными сейфами.

- Программа конфликтует с Kaspersky Password Manager.

Как удалить несовместимые программы

Чтобы удалить несовместимые программы, выполните следующие действия:

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

   Откроется окно **Центр уведомлений**.
3. В разделе **Рекомендации** в строке с сообщением о найденных несовместимых программах нажмите на кнопку **Показать**.

   Откроется окно **Несовместимое программное обеспечение** со списком найденных несовместимых программ, которые Kaspersky Security Cloud может удалить.
4. Оставьте флажки напротив названий несовместимых программ, которые нужно удалить, и нажмите **Удалить**. Kaspersky Security Cloud удалит указанные программы с вашего компьютера. Kaspersky Security Cloud удаляет программы с помощью средств удаления, предоставляемых этими программами. В процессе удаления от вас может потребоваться согласие на удаление или изменение настроек, связанных с удалением программ.
5. Если на компьютере остались несовместимые программы, которые Kaspersky Security Cloud не удаляет, откроется окно со списком таких программ. Чтобы удалить несовместимые программы вручную, нажмите **Удалить вручную**. Откроется стандартное окно операционной системы со списком установленных программ. Удалите несовместимые программы в соответствии с инструкциями для вашей операционной системы.
6. После удаления несовместимых программ перезагрузите компьютер.

Очистка компьютера

Этот раздел содержит информацию о том, как с помощью Kaspersky Security Cloud обнаружить на компьютере программы и расширения браузеров, которые, возможно, вы захотите удалить.

Об очистке компьютера

С помощью Kaspersky Security Cloud вы можете найти на компьютере программы и расширения браузеров, которые, возможно, вы захотите удалить. Например, это могут быть программы и расширения браузеров, которые установлены без вашего согласия или редко используются вами.

Kaspersky Security Cloud регулярно анализирует установленные программы и расширения браузеров с точки зрения возможных причин для их удаления, а также распределяет обнаруженные программы и расширения браузеров по категориям.

Вы можете запустить анализ установленных программ и расширений браузеров вручную или настроить запуск анализа по расписанию.

Информация об обнаруженных программах и расширениях браузеров отображается в окне **Центр уведомлений**, из которого вы можете перейти к просмотру списка обнаруженных объектов.

Программы и расширения, которые вы не хотите удалять, можно поместить в список исключений. Вы можете просматривать и изменять список исключений.

Вы можете передать в "Лабораторию Касперского" данные о программах, которые мешают вам или создают проблемы, воспользовавшись ссылкой **Пожаловаться на программу**.

Как запустить анализ объектов вручную

Чтобы запустить анализ объектов вручную, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Больше функций**.

Откроется окно **Инструменты**.

3. В окне **Инструменты** перейдите в раздел **Очистка и оптимизация**.

4. По ссылке **Очистка компьютера** перейдите в окно **Очистка компьютера**.

5. В открывшемся окне нажмите на кнопку **Запустить**.

Запустится анализ объектов. Информация о результатах анализа отобразится в окне в виде ссылки на списки обнаруженных программ и расширений браузеров. Перейдите к списку обнаруженных объектов по ссылке.

Как настроить запуск анализа по расписанию

Чтобы настроить запуск анализа установленных программ и расширений браузеров по расписанию, выполните следующие действия:

1. Откройте главное окно программы.

2. Нажмите на кнопку ⚙.

Откроется окно **Настройка**.

3. Выберите раздел **Защита**.

4. Выберите компонент Менеджер программ.

Откроется окно **Настройки Менеджера программ**.

5. В блоке **Очистка компьютера** поставьте флажок **Выполнять анализ установленных программ и расширений браузеров**.

6. По ссылке **Настроить расписание** перейдите в окно **Расписание**.

7. В раскрывающемся списке **Выполнять анализ** выберите один из следующих пунктов:

- **Автоматически**. Если вы выберете этот пункт, Kaspersky Security Cloud будет выполнять анализ раз в сутки в заданное по умолчанию время.

- **По минутам** / **По часам** / **По дням** / **Еженедельно** / **Каждый месяц** / **В указанное время**. Если вы выберете один из этих пунктов, Kaspersky Security Cloud будет выполнять анализ по заданному вами расписанию, с точностью до минуты. При выборе одного из этих вариантов доступен флажок **Отложить запуск после старта программы на** N **минут**.

- **После запуска программы**. Kaspersky Security Cloud будет выполнять анализ после своего запуска, спустя столько минут, сколько указано в поле **Запускать через** N **минут**.

- **После каждого обновления**. Kaspersky Security Cloud будет выполнять анализ после загрузки и установки нового пакета обновлений.

8. Установите флажок **Выполнять анализ объектов на следующий день, если компьютер был выключен**, чтобы выполнять анализ после включения компьютера в случае пропуска запланированного времени анализа. Если флажок не установлен, программа будет выполнять анализ только в заданное по расписанию время, когда компьютер включен.

9. Установите флажок **Выполнять анализ объектов только в случае, когда компьютер заблокирован или включена экранная заставка**, чтобы выполнять анализ объектов, только если вы не работаете с компьютером, и не создавать дополнительную загрузку ресурсов компьютера во время вашей работы. Если флажок не установлен, программа будет выполнять анализ в заданное по расписанию время вне зависимости от того, работаете вы с компьютером или нет.

10. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения настроек.

Как выбрать категории объектов для анализа

Чтобы выбрать категории объектов, обнаруживаемых при анализе, выполните следующие действия:

1. Откройте главное окно программы.

2. Нажмите на кнопку ⚙.

Откроется окно **Настройка**.

3. Выберите раздел **Защита**.

4. Выберите **Менеджер программ**.

   Откроется окно **Настройки Менеджера программ**.

5. По ссылке **Выбрать категории объектов** перейдите в окно **Категории объектов**.

6. Выполните следующие действия:

   - Чтобы провести анализ установленных программ, установите флажок **Программы**.
   - Чтобы провести анализ установленных расширений браузеров, установите флажок **Расширения браузеров**.

7. Выберите категории программ и расширений браузеров, которые вы хотите найти и, возможно, удалить. Для этого установите флажки напротив выбранных категорий.

8. Нажмите на кнопку **Сохранить**.

Категории обнаруживаемых объектов

Категории описаны в таблице ниже.

Категории программ

Категория программ и расширений браузеров	Описание
Предоставляют ложную информацию	По данным "Лаборатории Касперского"*, программа или расширение браузера сообщают вам ложные сведения о состоянии операционной системы или установленных программ, чтобы предложить покупку и установку программ в интересах своего производителя.

Установлены без вашего согласия	По данным "Лаборатории Касперского"*, программа или расширение браузера устанавливаются на компьютер без вашего явного согласия в электронном виде.
Выводят анонимные сообщения / баннеры	По данным "Лаборатории Касперского"*, программа или расширение браузера анонимно выводят на экран компьютера сообщения и уведомления.
Замедляют загрузку компьютера	По данным "Лаборатории Касперского"*, программа или расширение браузера запускаются вместе с операционной системой, тогда как вы не давали на это явного согласия.
Установлены принудительно	По данным "Лаборатории Касперского"*, установка программы или расширения браузера была вам навязана, например, посредством блокировки браузера или операционной системы.
Скрывают свою работу	По данным "Лаборатории Касперского"*, программа или расширение браузера скрывают от вас свою работу: не имеют видимых окон, не отображают значок в области уведомлений панели задач.
Не поддерживаются производителем и содержат уязвимости	Производитель не поддерживает эту программу или расширение браузера, не выпускает для них обновления и не исправляет уязвимости.
Скрывают механизм закрытия	По данным "Лаборатории Касперского"*, программа или расширение браузера скрывают и / или ограничивают механизмы, с помощью которых вы можете закрыть, отключить или удалить эту программу или расширение браузера.
Установлены совместно с другой программой	По данным "Лаборатории Касперского", программа или расширение браузера устанавливаются на компьютер совместно с другой программой. Возможно, программа или расширение браузера установлены по ошибке, или вы не давали разрешение на его установку.
Редко используется	По данным "Лаборатории Касперского", программа не запускалась более <N> дней.
Собирают и передают ваши данные	По данным "Лаборатории Касперского", программа или расширение браузера могут собирать и передавать ваши данные без вашего явного согласия.
Перенаправляют трафик	По данным "Лаборатории Касперского", программа или расширение браузера могут перенаправлять или блокировать сетевой трафик (например, ваши поисковые запросы в интернете), могут получать доступ к

	сайтам и менять страницы, не уведомляя вас об этом.
Изменяют настройки операционной системы или браузера	По данным "Лаборатории Касперского", программа или расширение браузера могут изменять настройки браузера или операционной системы (например, выбранную вами поисковую систему или домашнюю страницу браузера) без вашего явного согласия.
Ограничивают возможность изменения настроек	По данным "Лаборатории Касперского", программа или расширение браузера могут ограничивать возможность просмотра и изменения настроек браузера и операционной системы.
Изменяют поведение браузера	По данным "Лаборатории Касперского", программа или расширение браузера могут изменять поведение браузера при его установке, удалении, работе или отключении расширений.

* "Лаборатории Касперского" известно, что для программы или расширения браузера характерны описанные в таблице действия. Kaspersky Security Cloud не проверяет, выполнялись ли эти действия на вашем компьютере.

Просмотр списка обнаруженных объектов

Чтобы просмотреть список, сформированный в результате анализа объектов, выполните следующие действия:

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

   Откроется окно **Центр уведомлений**.
3. В разделе **Рекомендации** в строке с сообщением об обнаруженных объектах нажмите на кнопку **Показать**.

   Откроется окно со списком обнаруженных программ и расширений браузеров. Для каждого объекта в списке указаны предположительные причины для его возможного удаления или исправления.

   - Если вы хотите удалить программу или расширение браузера с вашего компьютера, в строке с описанием программы или расширения браузера нажмите на кнопку **Удалить**. Kaspersky Security Cloud запустит процесс удаления.

- Если вы хотите, чтобы программа или расширение браузера остались на компьютере и больше не попадали в список с результатами анализа обнаруженных объектов, в строке с описанием объекта нажмите на кнопку **Игнорировать**. Объект будет добавлен в список исключений, Kaspersky Security Cloud больше не будет показывать его в списке обнаруженных объектов.

Просмотр списка исключений

Программы и расширения, которые вы не хотите удалять, можно поместить в список исключений.

Чтобы просмотреть список исключений, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Защита**.
4. Выберите компонент Менеджер программ.

   Откроется окно **Настройки Менеджера программ**.
5. По ссылке **Исключения** откройте окно **Исключения**.

   В окне **Исключения** представлены программы и расширения браузеров, которые вы добавили в список исключений, нажав на кнопку **Игнорировать** в списке обнаруженных объектов.
6. Если вы хотите удалить объект из списка исключений, нажмите на кнопку **Удалить из списка**.

Как отправить в "Лабораторию Касперского" данные об окне программы или браузера

Если у вас возникла проблема с окном программы или браузера, открытым на вашем компьютере, вы можете пожаловаться на это окно в "Лабораторию Касперского" с помощью Kaspersky Security Cloud.

Чтобы отправить в "Лабораторию Касперского" данные об окне программы или браузера, выполните следующие действия:

1. Откройте главное окно Kaspersky Security Cloud.
2. Нажмите на кнопку **Больше функций**.
3. Выберите раздел **Очистка и оптимизация**.
4. По ссылке **Очистка компьютера** откройте окно **Очистка компьютера**.
5. Нажмите на ссылку **Пожаловаться на программу**.

   Курсор мыши превратится в значок мишени.
6. Наведите курсор на окно программы или браузера, данные о котором вы хотите отправить в "Лабораторию Касперского".
7. Нажмите на левую клавишу мыши, чтобы собрать данные о программе или сайте, открывших это окно.

   Откроется окно **Сбор данных о программе**.
8. В окне **Сбор данных о программе** выполните следующие действия:

   a. Если вы хотите просмотреть данные о выбранном вами окне, нажмите на ссылку **Просмотреть собранные данные**.

      Откроется окно **Просмотр данных о программе**, в котором вы можете просмотреть всю собранную информацию о выбранном вами окне.

   b. Чтобы просмотреть скопированное вами изображение, наведите на него курсор и нажмите на левую клавишу мыши.

      Откроется папка, в которой было сохранено изображение.

c. По ссылке **Положение об обработке данных** ознакомьтесь с Положением об обработке данных.

d. Установите флажок **Я прочитал и согласен с Положением о технической поддержке**.

e. Нажмите на кнопку **Отправить**.

Данные об окне программы или браузера будут отправлены в "Лабораторию Касперского".

Удаление данных без возможности восстановления

Дополнительная безопасность персональных данных обеспечивается защитой от несанкционированного восстановления удаленной информации злоумышленниками.

В состав Kaspersky Security Cloud входит инструмент для удаления данных без возможности восстановления обычными программными средствами.

Kaspersky Security Cloud позволяет удалять данные без возможности восстановления со следующих носителей информации:

- Локальные диски. Удаление возможно, если у вас есть права на запись и удаление информации.
- Съемные диски или другие устройства, которые распознаются как съемные 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 программами.

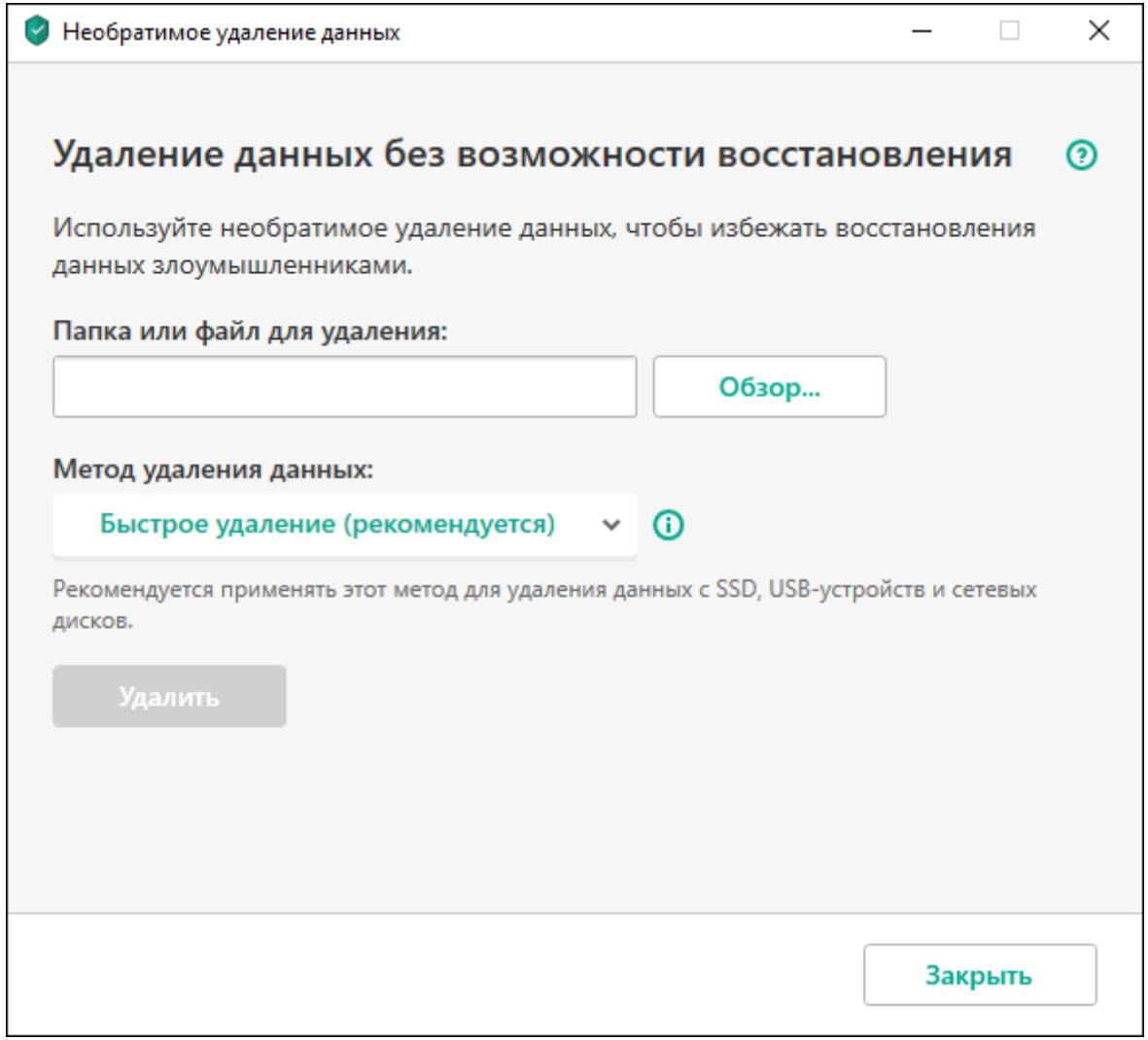
Чтобы удалить данные без возможности восстановления, выполните следующие действия:

1. Откройте главное окно программы.

2. Нажав на кнопку **Больше функций**, расположенную в нижней части главного окна, откройте окно **Инструменты**.

3. Перейдите в раздел **Безопасность данных**.

4. По ссылке **Необратимое удаление данных** перейдите в окно **Необратимое удаление данных** (см. рис. ниже).



Окно **Необратимое удаление данных**

5. Нажмите на кнопку **Обзор** и в открывшемся окне **Выбор папки** выберите папку или файл для удаления без возможности восстановления.

> Удаление системных файлов может вызвать сбои в работе операционной системы.

6. В раскрывающемся списке **Метод удаления данных** выберите нужный метод удаления данных.

> Для удаления данных с SSD- и USB-устройств рекомендуется применять методы **Быстрое удаление** 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.

7. Нажмите на кнопку **Удалить**.

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

Файлы, используемые сторонним приложением, не могут быть удалены.

Удаление неиспользуемых данных

Этот раздел содержит информацию об удалении временных и неиспользуемых файлов.

Об удалении неиспользуемых данных

Со временем в операционной системе накапливаются временные и неиспользуемые файлы. Эти файлы могут занимать большой объем памяти, что снижает эффективность работы системы, а также могут использоваться вредоносными программами.

Временные файлы создаются при запуске любых программ или операционных систем. По завершении работы не все временные файлы автоматически удаляются. В состав Kaspersky Security Cloud входит мастер удаления неиспользуемых данных.

Мастер удаления неиспользуемых данных позволяет найти и удалить следующие файлы:

- журналы событий системы, куда записываются названия всех открытых программ;
- журналы событий разных программ или утилит обновления (например, Windows Updater);
- журналы системных соединений;

- временные файлы браузеров (cookies);
- временные файлы, которые остаются после установки / удаления программ;
- содержимое корзины;
- файлы папки TEMP, объем которой иногда достигает нескольких гигабайт.

Помимо удаления из системы ненужных файлов, мастер удаляет те файлы, в которых могли сохраниться конфиденциальные данные (пароли, имена пользователей и информация с регистрационных форм). Тем не менее, для полного удаления таких данных рекомендуется использовать мастер устранения следов активности.

Процедура удаления неиспользуемых данных

Чтобы запустить мастер удаления неиспользуемых данных, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажав на кнопку **Больше функций**, расположенную в нижней части главного окна, откройте окно **Инструменты**.
3. В окне **Инструменты** перейдите в раздел **Очистка и оптимизация**.
4. По ссылке **Удаление неиспользуемых данных** запустите мастер удаления неиспользуемых данных.

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 шаге следует нажать на кнопку **Отмена**.

Рассмотрим подробнее шаги мастера.

Начало работы мастера

В первом окне мастера представлена информация об удалении неиспользуемых данных.

Нажмите на кнопку **Далее**, чтобы начать работу мастера.

Поиск неиспользуемых данных

Мастер осуществляет поиск неиспользуемых данных на вашем компьютере. Поиск может занять некоторое время. По завершении поиска мастер автоматически перейдет к следующему шагу.

Выбор действий для удаления неиспользуемых данных

По завершении поиска неиспользуемых данных открывается окно, в котором отображается список действий.

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.

Не рекомендуется снимать флажки, установленные по умолчанию. В результате этого действия безопасность вашего компьютера может оказаться под угрозой.

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

Удаление неиспользуемой информации

Мастер выполняет действия, выбранные на предыдущем шаге. Удаление неиспользуемой информации может занять некоторое время.

После удаления неиспользуемой информации мастер автоматически перейдет к следующему шагу.

> Во время работы мастера некоторые файлы (например, файл журнала Microsoft Windows, журнал событий Microsoft Office) могут использоваться операционной системой. Чтобы удалить эти файлы, мастер предложит перезагрузить операционную систему.

Завершение работы мастера

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

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 программы вы можете просматривать информацию о выполнении этих задач.

Сохранять резервные копии данных рекомендуется на съемных дисках или в Онлайн-хранилище.

> Kaspersky Security Cloud не может создавать полную копию диска с активной операционной системой Microsoft Windows.

Для создания резервных копий Kaspersky Security Cloud позволяет использовать следующие типы хранилищ:

- локальный диск;
- съемный диск (например, внешний жесткий диск);
- сетевой диск;
- Онлайн-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 Kaspersky Security Cloud 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, Kaspersky Security Cloud делает резервную копию этого файла.
- Если файла нет в облаке, но есть в папке OneDrive на вашем компьютере, Kaspersky Security Cloud делает резервную копию этого файла.

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

Как создать задачу резервного копирования

Чтобы создать задачу резервного копирования, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Больше функций**.

   Откроется окно **Инструменты**.
3. В окне **Инструменты** перейдите в раздел **Безопасность данных**.
4. По ссылке **Резервное копирование** перейдите в окно **Резервное копирование**.
5. В окне **Резервное копирование** выполните одно из следующих действий:

   - Если задача резервного копирования еще не создавалась, нажмите на кнопку **Выбрать файлы для резервного копирования**.
   - Если у вас есть задача резервного копирования и вы хотите создать новую, нажмите на кнопку **Создать резервные копии других файлов**.

   Будет запущен мастер создания задачи резервного копирования.

   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 шаге следует нажать на кнопку **Отмена**.

   Рассмотрим подробнее шаги мастера.

Шаг 1. Выбор файлов

На этом шаге мастера выберите тип файлов или укажите папки, для которых вы хотите создать резервные копии:

- Для быстрой настройки выберите один из предустановленных типов файлов (файлы из папок "Мои документы" и "Рабочий стол", фотографии и изображения, фильмы и видео, музыкальные файлы). При подтверждении этого варианта мастер сразу перейдет к шагу 4 "Выбор хранилища резервных копий".

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

- Выберите вариант **Создать резервные копии файлов из указанных папок**, чтобы вручную указать папки, для которых вы хотите создать резервные копии.

Шаг 2. Выбор папок для резервного копирования

Если на предыдущем шаге мастера вы выбрали вариант **Создать резервные копии файлов из указанных папок**, нажмите на кнопку **Добавить папку** и выберите папку в открывшемся окне **Выбор папки для резервного копирования** или перетащите папку в окно программы.

Установите флажок **Дополнительно указать типы файлов**, если вы хотите в указанных папках уточнить типы файлов, для которых требуется создать резервные копии.

Шаг 3. Выбор типов файлов для резервного копирования

Если на предыдущем шаге мастера вы установили флажок **Дополнительно указать типы файлов**, на этом шаге мастера установите флажки напротив типов файлов, для которых вы хотите создать резервные копии.

Шаг 4. Выбор хранилища резервных копий

На этом шаге выберите хранилище резервных копий:

- **Онлайн-хранилище**. Выберите этот вариант, если вы хотите хранить резервные копии в Онлайн-хранилище Dropbox. Перед использованием требуется активировать Онлайн-хранилище. При создании резервной копии с использованием Онлайн-хранилища Kaspersky Security Cloud не создает резервные копии тех типов данных, на которые наложены ограничения правилами использования Dropbox.
- **Локальный диск**. Если вы хотите хранить резервные копии на локальном диске, выберите нужный локальный диск в списке.
- **Сетевой диск**. Если вы хотите хранить резервные копии на сетевом диске, выберите нужный сетевой диск в списке.
- **Съемный диск**. Если вы хотите хранить резервные копии на съемном диске, выберите нужный съемный диск в списке.

Для безопасности данных рекомендуется использовать Онлайн-хранилище или создавать хранилища резервных копий на съемных дисках.

Как добавить сетевое хранилище

Чтобы добавить сетевое хранилище, выполните следующие действия:

1. По ссылке **Добавить сетевое хранилище** откройте окно **Добавление сетевого хранилища** и выберите сетевое хранилище.
2. Укажите данные, необходимые для подключения к сетевому хранилищу.
3. Нажмите на кнопку **OK**.

Как добавить съемный диск в качестве хранилища

Чтобы добавить съемный диск в качестве хранилища резервных копий, выполните следующие действия:

1. По ссылке **Подключить имеющееся хранилище** откройте окно **Подключение хранилища**.
2. Выберите раздел **Съемный диск**.
3. Нажмите на кнопку **Обзор** и в открывшемся окне укажите съемный диск, на который вы хотите сохранять резервные копии файлов.

Установите флажок **Использовать расширенную настройку хранилища**, если вы хотите изменить настройки хранения файлов, такие как количество хранимых версий резервных копий и время хранения версий резервных копий.

Шаг 5. Создание расписания резервного копирования

На этом шаге мастера выполните одно из следующих действий:

- Задайте расписание запуска задачи резервного копирования, если хотите, чтобы задача запускалась автоматически.

  a. В раскрывающемся списке **Запускать резервное копирование** выберите интервал, через который будет запускаться задача (например, **ежедневно**) и укажите время запуска задачи в поле **Время**.

  b. В блоке **Учетная запись** укажите имя пользователя и пароль своей учетной записи на этом компьютере. Данные учётной записи требуются для получения прав доступа к файлам во время резервного копирования.

  c. Установите флажок **Запускать при включении компьютера, если в указанное время он был выключен**, если вы хотите, чтобы программа запускала резервное копирование при первой возможности после перезапуска программы. Например, согласно расписанию резервное копирование нужно выполнять по выходным дням. Если в выходные дни компьютер был выключен, резервное копирование выполняется после включения компьютера в будний день. Если флажок снят, резервное копирование выполняется согласно расписанию, без повторных попыток в случае неудачного запуска резервного копирования.

- В раскрывающемся списке **Запускать резервное копирование** выберите вариант **по требованию**, если хотите запускать задачу самостоятельно.

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 6. Ввод пароля для защиты резервных копий

Установите флажок **Включить защиту паролем** и заполните поля **Пароль для доступа к резервным копиям** и **Подтверждение пароля**, если вы хотите защитить паролем доступ к резервным копиям.

Пароль необходим для защиты хранилища резервных копий от несанкционированного доступа.

Программа запрашивает у вас ввод пароля в следующих случаях:

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

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

- Когда вы подключаете съемный диск к компьютеру. Программа проверяет съемный диск и просит вас ввести пароль в случае обнаружения хранилища резервных копий на этом съемном диске.

Шаг 7. Настройки хранения резервных копий файлов

Этот шаг доступен, если на шаге 4 "Выбор хранилища резервных копий" вы установили флажок **Использовать расширенную настройку хранилища**.

Укажите настройки хранения файлов:

- Установите флажок **Ограничить количество версий резервных копий** и в поле **Количество хранимых версий резервных копий** укажите количество версий резервных копий одного файла, которые необходимо сохранять.

- Установите флажок **Ограничить время хранения версий резервных копий** и в поле **Период хранения версии резервной копии** укажите количество дней, которые должна храниться каждая версия резервной копии.

Шаг 8. Ввод имени задачи резервного копирования

На этом шаге выполните следующие действия:

- Введите имя задачи резервного копирования.

- Установите флажок **Запустить резервное копирование по завершении работы мастера**, если вы хотите, чтобы резервное копирование началось автоматически после завершения работы мастера.

Шаг 9. Завершение работы мастера

В этом окне отображается процесс настройки хранилища резервных копий. Настройка может занять некоторое время.

По окончании настройки нажмите на кнопку **Готово**.

Будет создана задача резервного копирования. Созданная задача отображается в окне **Резервное копирование**.

Как запустить задачу резервного копирования

Чтобы запустить задачу резервного копирования, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Больше функций**.

   Откроется окно **Инструменты**.
3. В окне **Инструменты** перейдите в раздел **Безопасность данных**.
4. По ссылке **Резервное копирование** перейдите в окно **Резервное копирование**.
5. В открывшемся окне **Резервное копирование** выберите задачу резервного копирования и нажмите на кнопку **Запустить**.

Запустится задача резервного копирования.

Восстановление данных из резервной копии

Чтобы восстановить данные из резервной копии, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Больше функций**.

   Откроется окно **Инструменты**.
3. В окне **Инструменты** перейдите в раздел **Безопасность данных**.
4. По ссылке **Резервное копирование** перейдите в окно **Резервное копирование**.

5. Выполните одно из следующих действий:

   - Нажмите на кнопку **Восстановить файлы** напротив нужной задачи резервного копирования.
   - По ссылке **Управление хранилищами** откройте окно, где напротив нужного хранилища резервных копий нажмите на кнопку **Восстановить файлы**.

6. Если при создании резервной копии был задан пароль, укажите этот пароль в окне **Введите пароль для доступа к хранилищу**.

7. В раскрывающем списке **Дата / время копирования** выберите дату и время создания резервной копии.

8. 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**.

9. Если вы хотите восстановить только определенные типы файлов, в раскрывающемся списке **Тип файлов** выберите эти типы файлов.

10. Нажмите на кнопку **Восстановить выбранные файлы**.

    Откроется окно **Восстановление файлов из резервных копий**.

11. Выберите один из двух вариантов:

    - **В исходную папку**. Если выбран этот вариант, программа восстанавливает данные в исходную папку.
    - **В указанную папку**. Если выбран этот вариант, программа восстанавливает данные в указанную папку. Нажмите на кнопку **Обзор**, чтобы выбрать папку, в которую вы хотите восстановить данные.

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

    - **спрашивать пользователя** – программа 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** – Kaspersky Security Cloud удаляет существующий файл и помещает на его место файл, восстановленный из резервной копии.
    - **сохранить оба файла** – Kaspersky Security Cloud оставляет существующий файл без изменений и сохраняет файл, восстановленный из резервной копии, под новым именем в этой же папке.
    - **не восстанавливать этот файл** – Kaspersky Security Cloud оставляет существующий файл без изменений, не восстанавливая одноименный файл из резервной копии.

13. Нажмите на кнопку **Восстановить**.

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

Восстановление данных из FTP-хранилища

Текущая версия программы не поддерживает резервное копирование по FTP. Для восстановления резервных копий из FTP-хранилища, созданных в более ранних версиях программы, воспользуйтесь следующей инструкцией.

Чтобы восстановить резервные копии из FTP-хранилища, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Больше функций**.

   Откроется окно **Инструменты**.

3. В окне **Инструменты** перейдите в раздел **Безопасность данных**.
4. По ссылке **Резервное копирование** перейдите в окно **Резервное копирование**.
5. По ссылке **Управление хранилищами** откройте окно **Хранилища**.
6. По ссылке **Перейти на FTP-сервер** откройте в проводнике папку FTP-хранилища.
7. Скопируйте данные, включая файл `storage.xml`, на локальный диск (например, C:\<название папки>).
8. В окне **Управление хранилищами** напротив FTP-хранилища нажмите на кнопку **Удалить хранилище**.
9. В окне подтверждения удаления нажмите на кнопку **Удалить**.

   Хранилище будет удалено.
10. В окне **Управление хранилищами** нажмите на кнопку **Подключить имеющееся хранилище**.
11. В окне **Подключение хранилища** выберите раздел **Локальный диск** и с помощью кнопки **Обзор** укажите путь к папке с резервными копиями, которые вы скопировали на локальный диск из FTP-хранилища.
12. В окне **Хранилища** напротив подключенного хранилища нажмите на кнопку **Восстановить**.
13. 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 на компьютере, на котором удалена или повреждена программа "Лаборатории Касперского". По умолчанию после установки программы утилита находится в папке Kaspersky Restore Utility, расположенной в папке установки программы. Чтобы использовать утилиту на компьютере, на котором не установлена или повреждена программа "Лаборатории Касперского", утилиту требуется скопировать на съемный диск.

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

Как запустить утилиту восстановления

Чтобы запустить утилиту восстановления, выполните следующие действия:

1. Откройте съемный диск, на который была скопирована утилита.
2. В папке Kaspersky Restore Utility запустите файл kasperskylab.pure.restoretool.

   Откроется главное окно утилиты восстановления. В окне отобразится хранилище, заданное по умолчанию в программе. Вы можете указать путь к другому хранилищу.

Как открыть хранилище с помощью утилиты восстановления

Чтобы открыть хранилище с помощью утилиты восстановления, выполните следующие действия:

1. Запустите утилиту восстановления.

   Утилита автоматически определяет путь к хранилищу резервных копий, если оно создано на локальном диске C.
2. Если хранилище резервных копий находится не на диске C, в главном окне утилиты восстановления нажмите на кнопку **Указать хранилище**.
3. В открывшемся окне нажмите на кнопку **Обзор** и укажите путь к хранилищу резервных копий.
4. Нажмите на кнопку **Выбрать хранилище**.

Как восстановить данные из резервной копии

Чтобы восстановить данные из резервной копии, выполните следующие действия:

1. Запустите утилиту восстановления.
2. В главном окне утилиты восстановления выполните следующие действия:
   a. В раскрывающемся списке **Задача резервного копирования** выберите задачу, в процессе выполнения которой были созданы нужные резервные копии.
   b. В раскрывающемся списке **Дата / время копирования** выберите дату и время создания нужных резервных копий.
3. Выберите файлы, 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.
4. Нажмите на кнопку **Восстановить выбранные данные**.

   Откроется окно **Выбор папки для восстановленных файлов**.
5. В открывшемся окне выберите место сохранения восстановленных файлов.
   - **В исходную папку**. Выберите этот вариант, если вы хотите восстановить данные в исходную папку.
   - **В указанную папку**. Выберите этот вариант, если вы хотите выбрать папку для восстановления данных. Чтобы выбрать папку для восстановления данных, нажмите на кнопку **Обзор**.
6. В раскрывающемся списке **При совпадении имен файлов** выберите действие, которое должна выполнять программа, если в папке, куда требуется поместить восстановленный файл, уже находится файл с таким же именем:

- **спрашивать пользователя** – программа 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** – Kaspersky Security Cloud удаляет существующий файл и помещает на его место файл, восстановленный из резервной копии.
- **сохранить оба файла** – Kaspersky Security Cloud оставляет существующий файл без изменений и сохраняет файл, восстановленный из резервной копии, под новым именем в этой же папке.
- **не восстанавливать этот файл** – Kaspersky Security Cloud оставляет существующий файл без изменений, не восстанавливая одноименный файл из резервной копии.

7. Нажмите на кнопку **Восстановить**.

   Откроется окно **Восстановление файлов**. 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 Онлайн-хранилище

Программа Kaspersky Security Cloud позволяет сохранять резервные копии ваших данных в Онлайн-хранилище на удаленном сервере, используя веб-сервис Dropbox.

Для использования Онлайн-хранилища требуется:

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

Вы можете использовать одну и ту же учетную запись Dropbox для сохранения в единое Онлайн-хранилище резервных копий данных с разных устройств, на которых установлена программа Kaspersky Security Cloud.

Объем Онлайн-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 Kaspersky Security Cloud 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, Kaspersky Security Cloud создает только одну резервную копию, так как в Dropbox возникает конфликт регистров.

Как активировать Онлайн-хранилище

Чтобы активировать Онлайн-хранилище, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Больше функций**.

   Откроется окно **Инструменты**.
3. В окне **Инструменты** перейдите в раздел **Безопасность данных**.
4. По ссылке **Резервное копирование** перейдите в окно **Резервное копирование**.
5. Выполните одно из следующих действий:

   - Если задача резервного копирования не создавалась, нажмите на кнопку **Выбрать файлы для резервного копирования**.
   - Если у вас уже есть задача резервного копирования,нажмите на кнопку **Создать резервные копии других файлов**.

Будет запущен мастер создания задачи резервного копирования.

6. В окне выбора типа данных выберите категорию данных или вручную укажите файлы, для которых нужно создавать резервные копии.

7. В окне выбора хранилища выберите **Онлайн-хранилище** и нажмите на кнопку **Активировать**.

   Для создания Онлайн-хранилища требуется подключение к интернету.

   Откроется окно входа в учетную запись Dropbox.

8. 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.

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

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

При копировании файлов в хранилище Dropbox Kaspersky Security Cloud 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, Kaspersky Security Cloud создает только одну резервную копию, так как в Dropbox возникает конфликт регистров.

Хранение данных в сейфах

Этот раздел содержит информацию о том, как вы можете защитить данные с помощью сейфов.

О сейфе

Для защиты ваших конфиденциальных данных от несанкционированного доступа предназначены сейфы. *Сейф* – это хранилище данных на вашем компьютере, которое вы можете открывать или закрывать с помощью известного только вам пароля. Для изменения файлов, хранящихся в закрытом сейфе, требуется ввести пароль. Если вы ввели неверный пароль 10 раз подряд, доступ к сейфу блокируется на один час.

Если вы потеряете или забудете пароль, восстановить данные будет невозможно.

Для создания сейфов в Kaspersky Security Cloud используется алгоритм шифрования данных AES XTS с эффективной длиной ключа 56 бит.

> Если на вашем компьютере используется файловая система FAT32, вы можете создавать виртуальные сейфы объемом не более 4 ГБ.

Как поместить файлы в сейф

Чтобы поместить файлы в сейф, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Больше функций**, расположенную в нижней части главного окна.

   Откроется окно **Инструменты**.
3. Перейдите в раздел **Безопасность данных**.

4. По ссылке **Виртуальные сейфы** перейдите в окно **Виртуальные сейфы**.

5. В окне **Виртуальные сейфы** выполните одно из следующих действий:

   - Если у вас еще нет сейфа, нажмите на кнопку **Создать новый сейф**.
   - Если ранее вы создавали сейфы, нажмите на кнопку **Создать сейф**.

6. По ссылке **Добавить** откройте Проводник и укажите файлы, которые вы хотите поместить в сейф.

   Выбранные файлы отобразятся в окне **Виртуальные сейфы**.

7. Нажмите на кнопку **Продолжить**.

8. Введите название сейфа и укажите его расположение или используйте значения этих настроек по умолчанию.

9. Для получения быстрого доступа к сейфу установите флажок **Создать ярлык сейфа на рабочем столе**.

10. Нажмите на кнопку **Продолжить**.

11. Заполните поля **Пароль для доступа к сейфу** и **Подтверждение пароля** и нажмите на кнопку **Продолжить**.

12. Выберите действие с исходными копиями файлов вне сейфа:

    - Чтобы удалить исходные копии файлов вне сейфа, нажмите на кнопку **Удалить**.
    - Чтобы сохранить исходные копии файлов вне сейфа, нажмите на кнопку **Пропустить**.

13. Нажмите на кнопку **Готово**.

    В списке сейфов отобразится созданный вами сейф.

14. Чтобы закрыть сейф, нажмите на кнопку **Закрыть**.

Данные в закрытом сейфе будут доступны только после ввода пароля.

При добавлении в сейф файлов с одинаковыми названиями, написанными в разных регистрах, один из таких файлов может быть недоступен при попытке открытия сейфа. Чтобы избежать потери данных, мы рекомендуем добавлять такие файлы в разные сейфы или поменять названия файлов на полностью уникальные.

Как получить доступ к файлам, хранящимся в сейфе

Чтобы получить доступ к файлам, хранящимся в сейфе, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Больше функций**, расположенную в нижней части главного окна.

   Откроется окно **Инструменты**.
3. По ссылке **Виртуальные сейфы** перейдите в окно **Виртуальные сейфы**.
4. Нажмите на кнопку **Открыть** рядом с нужным сейфом.
5. Введите пароль и нажмите на кнопку **Открыть в Проводнике**.

Файлы, сохраненные в сейфе, отобразятся в окне Проводника. Вы можете внести необходимые изменения в файлы и снова закрыть сейф.

Начиная с версии Kaspersky Security Cloud 4, при переименовании сейфа появляется ошибка при попытке открытия такого сейфа. Чтобы этого избежать, мы рекомендуем открыть сейф, который вы хотите переименовать, извлечь ваши данные и создать новый сейф с этими данными, назвав его другим именем.

Диагностика жесткого диска

Этот раздел содержит информацию о том, как проверить состояние жесткого диска вашего компьютера или подключенного внешнего жесткого диска с помощью Kaspersky Security Cloud.

О диагностике жесткого диска

Неожиданный выход из строя жесткого диска может привести к потере данных, хранящихся на этом жестком диске. С помощью Kaspersky Security Cloud вы можете следить за состоянием ваших жестких дисков с использованием технологии самодиагностики S.M.A.R.T. (Self-Monitoring Analysis and Reporting Technology). В основе этой технологии лежит постоянное наблюдение за основными характеристиками жесткого диска. С помощью Kaspersky Security Cloud вы можете своевременно узнавать об ухудшении состояния ваших жестких дисков и копировать данные с поврежденных дисков на другие носители информации.

Если компонент Диагностика жесткого диска включен, Kaspersky Security Cloud постоянно следит за состоянием жестких дисков и уведомляет вас, если их состояние ухудшается. Вы можете просмотреть информацию о состоянии как внутренних, так и внешних жестких дисков. Уведомления об ухудшении состояния жестких дисков появляются в области уведомлений панели задач. Подробные отчеты о результатах диагностики жестких дисков выводятся в разделе **Отчеты**.

Если состояние жесткого диска ухудшилось и хранение данных на этом диске стало ненадежным, Kaspersky Security Cloud предлагает вам скопировать данные с этого диска на другой носитель во избежание их потери. Вы можете скопировать данные с поврежденного диска на любой из доступных исправных носителей информации.

Вы можете выключить диагностику жесткого диска. После выключения диагностики Kaspersky Security Cloud больше не уведомляет вас об изменениях состояния ваших жестких дисков и не предлагает вам скопировать данные с поврежденных дисков на другие носители.

> Диагностика жесткого диска доступна в тарифных планах Personal и Family.

Как включить и выключить диагностику жесткого диска

Чтобы включить или выключить диагностику жесткого диска, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Производительность**.
4. Выполните одно из следующих действий:

   - Чтобы включить диагностику жесткого диска, установите флажок **Выполнять диагностику жесткого диска**.
   - Чтобы выключить диагностику жесткого диска, снимите флажок **Выполнять диагностику жесткого диска**.

Как проверить состояние жесткого диска

Kaspersky Security Cloud постоянно наблюдает за состоянием как внутренних, так и внешних жестких дисков вашего компьютера. Наблюдение осуществляется в фоновом режиме. Если состояние жесткого диска ухудшается и хранение данных на этом диске становится ненадежным, программа уведомляет вас об этом и предлагает скопировать данные на другой носитель.

Окно **Диагностика жесткого диска** отображает следующую информацию о состоянии жесткого диска:

- Состояние диска.
- Температура диска.

Возможны следующие состояния жесткого диска:

- *Хорошо* – состояние нового жесткого диска.

- *Нормально* – состояние жесткого диска с незначительными ухудшениями.
- *Плохо* – критическое состояние жесткого диска с возможностью потери данных.

Возможны следующие диапазоны температуры жесткого диска:

- *Хорошо* – жесткий диск не перегревается.
- *Нормально* – температура жесткого диска незначительно повышена.
- *Плохо* – жесткий диск перегревается.

График **История состояния диска** отображает информацию об изменениях состояния диска за определенный период времени. Максимальный отображаемый период – 1 год.

Также Kaspersky Security Cloud показывает следующие статистические данные о ваших жестких дисках:

- *Всего отработано часов* – общее время работы жесткого диска в часах.
- *Всего включений* – общее количество включений жесткого диска.

Отчет **S.M.A.R.T. параметры <название диска>** отображает информацию о значениях S.M.A.R.T.-параметров жесткого диска, отсортированных по критичности. Набор параметров может отличаться в зависимости от модели и производителя жесткого диска.

Чтобы узнать, каково текущее состояние жестких дисков вашего компьютера, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Больше функций**, расположенную в нижней части главного окна программы.

   Откроется окно **Инструменты**.

3. В окне **Инструменты** перейдите в раздел **Безопасность данных**.

4. По ссылке **Диагностика жесткого диска** откройте окно **Диагностика жесткого диска**.

5. Выберите жесткий диск, о состоянии которого вы хотите узнать.

6. Выполните одно из следующих действий:

   - Если вы хотите просмотреть график, нажмите на кнопку **История**.
   - Если вы хотите просмотреть отчет, нажмите на кнопку **Подробнее**.

Как скопировать данные с поврежденного жесткого диска

Если состояние одного или нескольких жестких дисков вашего компьютера ухудшилось и хранение данных на этих дисках стало ненадежным, Kaspersky Security Cloud уведомляет вас об этом и предлагает скопировать данные с этих жестких дисков на другие носители информации.

Чтобы скопировать данные с поврежденного жесткого диска на исправный жесткий диск, выполните следующие действия:

1. Выполните одно из следующих действий:

   - Если вы получили уведомление об ухудшении состояния жесткого диска, нажмите на кнопку **Подробнее** в окне уведомления.

     Откроется окно **Диагностика жесткого диска**.

   - Нажмите на кнопку **Скопировать данные** в окне **Диагностика жесткого диска**.

2. В открывшемся окне **Копирование важных данных** нажмите на кнопку **Начать копирование**.

   Откроется окно **Выбор хранилища**.

3. В окне **Выбор хранилища** выберите исправный жесткий диск, на который будут скопированы данные с поврежденного диска.

4. Нажмите на кнопку **Далее**.

   Откроется окно **Выбор файлов и папок для копирования**.

5. Выполните одно из следующих действий:

   - Перетащите файлы из Проводника Windows в выделенную область окна **Выбор файлов и папок для копирования**.
   - Нажмите на ссылку **выберите их из списка**.

     Откроется окно Проводника, в котором вы сможете выбрать файлы и папки для копирования на исправный жесткий диск.

6. После того, как вы добавили в список все файлы и папки, которые вы хотите скопировать, нажмите на кнопку **Далее**.

   Откроется окно **Создание папки для копирования данных**.

7. Выполните одно из следующих действий:

   - Чтобы создать на выбранном исправном диске новую папку и скопировать в нее файлы и папки с поврежденного диска, нажмите на кнопку **Далее**.
   - Чтобы выбрать существующую папку на исправном диске и скопировать в нее файлы и папки с поврежденного диска, нажмите на кнопку **Изменить**.

8. Выполните одно из следующих действий:

   - Если на выбранном исправном диске достаточно места для копирования выбранных файлов и папок, нажмите на кнопку **Далее**, чтобы начать копирование.
   - Если на выбранном исправном диске недостаточно места для копирования выбранных файлов и папок, нажмите на кнопку **Назад**, чтобы выбрать другой исправный диск и повторить попытку.

9. После завершения копирования выполните одно из следующих действий:

- Чтобы открыть папку, в которую были скопированы данные с поврежденного жесткого диска, нажмите на кнопку **Открыть папку**.
- Чтобы закрыть окно, нажмите на кнопку **Готово**.

Чтобы скопировать данные с поврежденного жесткого диска в онлайн-хранилище Dropbox, выполните следующие действия:

1. Выполните одно из следующих действий:
   - Если вы получили уведомление об ухудшении состояния жесткого диска, нажмите на кнопку **Подробнее** в окне уведомления.

     Откроется окно **Диагностика жесткого диска**.
   - Нажмите на кнопку **Скопировать данные** в окне **Диагностика жесткого диска**.
2. В открывшемся окне **Копирование важных данных** нажмите на кнопку **Начать копирование**.

   Откроется окно **Выбор хранилища**.
3. В окне **Выбор хранилища** выберите онлайн-хранилище Dropbox.

   Также вы можете выполнить одно из следующих действий:
   - Если хранилище неактивно, нажмите на кнопку **Активировать**.
   - Если вы хотите отключить хранилище, нажмите на ссылку **Отключить хранилище**.
4. Нажмите на кнопку **Далее**.

   Откроется окно **Копирование данных**.
5. Выполните одно из следующих действий:
   - Перетащите файлы из Проводника Windows в выделенную область окна **Копирование данных**.

- Нажмите на ссылку **выберите их из списка**.

  Откроется окно Проводника, в котором вы сможете выбрать файлы и папки для копирования в онлайн-хранилище Dropbox.

6. После того, как вы добавили в список все файлы и папки, которые вы хотите скопировать, нажмите на кнопку **Начать копирование**.

   Начнется копирование данных.

7. После завершения копирования выполните одно из следующих действий:

   - Если копирование данных завершено успешно, нажмите на кнопку **Готово**, чтобы закрыть окно.
   - Если программа уведомила вас о невозможности скопировать данные, освободите место в онлайн-хранилище и повторите попытку.

Есть ограничения на копирование данных, хранящихся в облачном хранилище OneDrive.

Ограничения диагностики жесткого диска

В некоторых случаях Kaspersky Security Cloud не может определить состояние жесткого диска из-за следующих ограничений:

- Жесткий диск не поддерживает технологию S.M.A.R.T.
- Функция S.M.A.R.T. отключена на жестком диске.
- Kaspersky Security Cloud не поддерживает:
  - тип подключенного жесткого диска;
  - тип USB-контроллера жесткого диска.

- Жесткий диск отключен.

Как сохранить ресурсы операционной системы для компьютерных игр

При одновременной работе Kaspersky Security Cloud и некоторых программ (в особенности компьютерных игр) в полноэкранном режиме иногда могут возникать следующие неудобства:

- работа программы или игры замедляется из-за недостатка системных ресурсов;
- окна уведомлений Kaspersky Security Cloud отвлекают от игры.

Чтобы не изменять настройки Kaspersky Security Cloud вручную перед каждым переходом в полноэкранный режим, вы можете использовать Игровой режим. Если Игровой режим используется и вы играете или работаете с программами в полноэкранном режиме, Kaspersky Security Cloud не запускает задачи проверки и обновления, не отображает уведомления.

Чтобы включить использование Игрового режима, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Общие**.
4. В блоке параметров **Производительность** установите флажок **Использовать Игровой режим**.

Дополнительно установите флажок **Использовать режим Не беспокоить**. В этом режиме не показываются уведомления, если вы активно работаете с некоторыми программами, а также не запускаются задачи проверки и обновления.

Как оптимизировать нагрузку на операционную систему для задач Kaspersky Security Cloud

Проверка компьютера с помощью Kaspersky Security Cloud может потребовать значительных системных ресурсов. Чтобы оптимизировать нагрузку на систему, в Kaspersky Security Cloud 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, Kaspersky Security Cloud не будет выполнять задачи во время простоя компьютера, чтобы продлить время его работы.

Чтобы оптимизировать нагрузку на операционную систему, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Общие** и в блоке **Производительность** установите флажок **Откладывать выполнение задач проверки компьютера при высокой нагрузке на центральный процессор и дисковые системы**.

Как устранить следы работы на компьютере

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 программ, 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 Kaspersky Security Cloud входит мастер устранения следов активности пользователя в операционной системе.

Чтобы запустить мастер устранения следов активности, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Больше функций**, расположенную в нижней части главного окна.

   Откроется окно **Инструменты**.
3. Перейдите в раздел **Очистка и оптимизация**.
4. По ссылке **Устранение следов активности** запустите мастер устранения следов активности.

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.

Начало работы мастера

a. Выберите один из двух вариантов работы мастера:

- **Выполнить поиск следов активности пользователя**. Мастер выполнит поиск следов вашей работы на компьютере.
- **Отменить внесенные ранее изменения**. Мастер 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.

b. Нажмите на кнопку **Далее**, чтобы начать работу мастера.

Поиск следов активности

Если вы выбрали вариант **Выполнить поиск следов активности пользователя**, мастер осуществляет поиск следов активности на вашем компьютере. Поиск может занять некоторое время. По завершении поиска мастер автоматически переходит к следующему шагу.

Выбор действий для устранения следов активности

По завершении поиска мастер сообщает об обнаруженных следах активности и предлагаемых действиях для их устранения.

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.

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

Устранение следов активности

Мастер выполняет действия, выбранные на предыдущем шаге. Устранение следов активности может занять некоторое время. Для устранения некоторых следов активности может потребоваться перезагрузка компьютера, о чем мастер вас уведомит.

После устранения следов активности мастер автоматически перейдет к следующему шагу.

Завершение работы мастера

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

Как приостановить и возобновить защиту компьютера

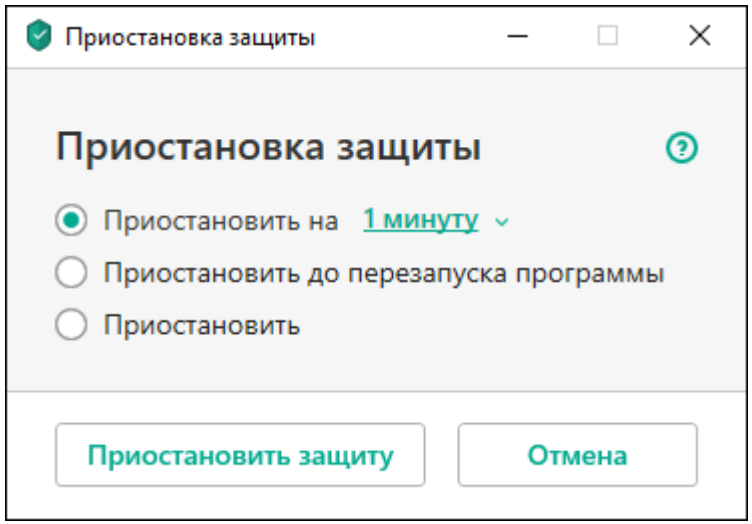
Приостановка защиты означает выключение на некоторое время всех ее компонентов.

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

Чтобы приостановить защиту компьютера, выполните следующие действия:

1. В контекстном меню значка программы в области уведомлений панели задач выберите пункт **Приостановить защиту**.

   Откроется окно **Приостановка защиты** (см. рис. ниже).



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 программы** – защита будет включена после перезапуска программы или перезагрузки операционной системы (при условии, что включен автоматический запуск программы).

- **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 программы в области уведомлений панели задач.

Как восстановить стандартные настройки работы программы

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

Чтобы восстановить стандартные настройки работы программы, выполните следующие действия:

1. Откройте главное окно программы.

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

   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 программы до тех, которые заданы специалистами "Лаборатории Касперского" по умолчанию.

6. После того как процесс восстановления стандартных настроек работы программы будет завершен, нажмите на кнопку **Готово**.

Как просмотреть отчет о работе программы

Kaspersky Security Cloud ведет отчеты о работе каждого компонента защиты. С помощью отчета вы можете получить статистическую информацию о работе программы (например, узнать, сколько обнаружено и обезврежено вредоносных объектов за определенный период, сколько раз за это время обновлялись базы и программные модули, сколько обнаружено спам-сообщений и многое другое).

Чтобы просмотреть отчет о работе программы, выполните следующие действия:

1. Откройте главное окно программы.

2. Нажмите на кнопку **Больше функций**, расположенную в нижней части главного окна.

   Откроется окно **Инструменты**.

3. В окне **Инструменты** по ссылке **Отчеты** перейдите в окно **Отчеты**.

   В окне **Отчеты** данные представлены в табличном виде. Для удобства просмотра отчетов вы можете выбирать различные варианты фильтрации записей.

Как применить настройки программы на другом компьютере

Настроив программу, вы можете применить настройки ее работы к программе Kaspersky Security Cloud, установленной на другом компьютере. В результате программа на обоих компьютерах будет настроена одинаково.

Настройки работы программы сохраняются в конфигурационном файле, который вы можете перенести с одного компьютера на другой.

Перенос настроек Kaspersky Security Cloud с одного компьютера на другой производится в три этапа:

1. Сохранение настроек программы в конфигурационном файле.
2. Перенос конфигурационного файла на другой компьютер (например, по электронной почте или на съемном диске).
3. Импорт настроек из конфигурационного файла в программу, установленную на другом компьютере.

Как экспортировать настройки программы

Чтобы экспортировать настройки программы, выполните следующие действия:

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

   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 программы будут сохранены в конфигурационный файл.

Вы также можете экспортировать настройки работы программы при помощи командной строки, используя команду: `avp.com EXPORT <имя_файла>`.

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

Как импортировать настройки программы

Чтобы импортировать настройки в программу, установленную на другом компьютере, выполните следующие действия:

1. Откройте главное окно программы Kaspersky Security Cloud, установленной 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 программу, установленную на другом компьютере.

Участие в Kaspersky Security Network

Чтобы повысить эффективность защиты вашего компьютера, Kaspersky Security Cloud 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 программ и сайтов. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Security Cloud 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 программ 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 Kaspersky Security Cloud.

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 Kaspersky Security Cloud и / или в любой момент после установки программы.

Чтобы включить или выключить участие в Kaspersky Security Network, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. В разделе **Защита** выберите блок **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 программы вместо информации о Kaspersky Security Network в окне **Kaspersky Security Network** отображается **Положение о Kaspersky Security Network**.

Чтобы принять Положение о Kaspersky Security Network, выполните следующие действия:

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 программах и о скачиваемых подписанных программах, 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:
  - Программа не активирована.
  - Срок действия лицензии или подписки истек.
  - Выявлены проблемы, связанные с лицензионным ключом (например, ключ попал в список запрещенных ключей).

> Текущий статус ключа отображается на My Kaspersky.

Чтобы проверить подключение к Kaspersky Security Network, выполните следующие действия:

1. Откройте главное окно программы.
2. Нажмите на кнопку **Больше функций**, расположенную в нижней части главного окна.

   Откроется окно **Инструменты**.
3. В окне **Инструменты** перейдите в раздел **Защита**.
4. В разделе **Защита** по ссылке **Облачная защита** откройте окно **Облачная защита**.

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

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

Программа Kaspersky Security Cloud, установленная 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 программ, 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 программы.

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

- Функциональность недоступна при запуске гипервизора сторонней программы, например, программы для виртуализации компании VMware. После завершения работы гипервизора сторонней программы 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 браузера обнаружен работающий гипервизор сторонней программы, например, программы 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, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Дополнительно**.
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.

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 программы, например Microsoft Office, могут отправлять в Kaspersky Security Cloud скрипты для проверки через интерфейс Antimalware Scan Interface (AMSI), а также о том, как выключить защиту с помощью AMSI в программе Kaspersky Security Cloud.

О защите с помощью Antimalware Scan Interface

Antimalware Scan Interface (AMSI) позволяет сторонней программе с поддержкой AMSI отправлять объекты в Kaspersky Security Cloud для дополнительной проверки (например, скрипты PowerShell) и получать результаты проверки этих объектов. Сторонними программами могут быть, например, программы Microsoft Office. Подробнее об интерфейсе AMSI см. в *документации Microsoft*.

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

Kaspersky Security Cloud может отклонить запрос от сторонней программы, например, если эта программа превысила максимальное количество запросов за промежуток времени. В этом случае Kaspersky Security Cloud 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.

Как включить защиту с помощью Antimalware Scan Interface

Чтобы включить защиту с помощью Antimalware Scan Interface, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. В разделе **Защита** выберите компонент **AMSI-защита**.
4. Переведите переключатель в верхней части окна в положение **Вкл**.

Как исключить скрипт из проверки с помощью Antimalware Scan Interface

Чтобы исключить скрипт из проверки с помощью Antimalware Scan Interface, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Защита**.
4. Выберите компонент Файловый Антивирус.

   Откроется окно **Настройки Файлового Антивируса**.
5. По ссылке **Расширенная настройка** перейдите в окно **Дополнительные настройки Файлового Антивируса**.
6. В блоке **Проверка скриптов** установите флажок **Проверять скрипты с помощью Antimalware Scan Interface (AMSI)**.
7. По ссылке **Настроить исключения** перейдите в окно **Исключения**.
8. В окне **Исключения** нажмите на кнопку **Добавить**.

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

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

12. Выберите статус **Активно**.

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

Работа с программой из командной строки

Вы можете работать с Kaspersky Security Cloud 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 Kaspersky Security Cloud 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 программе через командную строку следует из папки установки программы либо с указанием полного пути к avp.com.

Вы можете включать и выключать запись событий программы (создание файлов трассировки) через командную строку, если ранее вы установили пароль на защиту доступа к управлению Kaspersky Security Cloud в окне настройки программы.

Если вы не установили пароль в окне настройки программы, вы не сможете создать пароль и включить запись событий из командной строки.

Некоторые команды можно выполнить только под учетной записью администратора.

Оценка работы Kaspersky Security Cloud

Вы можете отправить в "Лабораторию Касперского" вашу оценку работы Kaspersky Security Cloud.

По истечении некоторого времени с момента установки программа предлагает вам оценить ее работу.

Чтобы оценить работу Kaspersky Security Cloud, выполните следующие действия:

1. В окне **Нам важно ваше мнение** выполните одно из следующих действий:
   - Если вы готовы оценить работу Kaspersky Security Cloud, поставьте программе оценку по 10-балльной шкале.
   - Если вы не хотите оценивать работу Kaspersky Security Cloud, нажмите на кнопку ✕, чтобы закрыть окно оценки.
2. Нажмите на кнопку **Отправить**.
3. Нажмите на кнопку **Закрыть**, чтобы закрыть окно.

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 справке программы или в одном из источников информации о программе, рекомендуем обратиться в Службу технической поддержки "Лаборатории Касперского". Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- Позвонить по телефону. Этот способ позволяет проконсультироваться по телефону со специалистами русскоязычной или интернациональной Службы технической поддержки.
- Отправить запрос с My Kaspersky. Этот способ позволяет вам связаться со специалистами Службы технической поддержки через форму запроса.

Техническая поддержка предоставляется только пользователям, которые приобрели подписку на программу. Техническая поддержка для пользователей пробных версий не осуществляется.

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского".

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

Техническая поддержка через My Kaspersky

Сайт My Kaspersky – это единый онлайн-ресурс для управления защитой ваших устройств и кодами активации программ "Лаборатории Касперского", а также для получения технической поддержки.

Для доступа к сайту My Kaspersky вам нужно зарегистрироваться. Для этого вам нужно указать адрес электронной почты и задать пароль.

Для получения технической поддержки вы можете выполнять следующие действия на сайте My Kaspersky:

- отправлять запросы в Службу технической поддержки;
- обмениваться сообщениями со Службой технической поддержки без использования электронной почты;
- отслеживать состояние ваших запросов в реальном времени.

Вы также можете просматривать полную историю ваших запросов в Службу технической поддержки.

Электронный запрос в Службу технической поддержки

В электронном запросе в Службу технической поддержки вам нужно указать следующую информацию:

- тему вашего запроса;
- название и номер версии программы;
- название и номер версии операционной системы;
- описание проблемы.

Специалист Службы технической поддержки направляет ответ на ваш вопрос на сайт My Kaspersky и на адрес электронной почты, который вы указали при регистрации.

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 программы и обнаружить, на каком этапе работы программы возникает ошибка.

Для более эффективного оказания поддержки в случае возникновения вопросов по работе программы специалисты Службы технической поддержки могут попросить вас в отладочных целях на время проведения работ по диагностике изменить настройки программы. Для этого может потребоваться выполнение следующих действий:

- Собрать расширенную диагностическую информацию.
- Выполнить более тонкую настройку работы отдельных компонентов программы, 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. 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 программы 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_dateXX.XX_timeXX.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 трассировки

Включайте и настраивайте трассировки только под руководством специалиста Службы технической поддержки "Лаборатории Касперского".

Чтобы включить трассировку программы и трассировку производительности, выполните следующие действия:

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

   Откроется окно **Поддержка**.
3. По ссылке **Мониторинг проблем** откройте окно **Мониторинг проблем**.
4. Включите и настройте трассировку программы и трассировку производительности в соответствии с инструкциями специалиста Службы технической поддержки "Лаборатории Касперского".

Ограничения и предупреждения

Kaspersky Security Cloud имеет ряд некритичных для работы программы ограничений.

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 программных модулей. Также в автоматическом режиме обновляются правила Сетевого экрана, Защиты веб-камеры, Менеджера программ, Удаления программ, Контроля программ.

Если проверка устройства запускается с My Kaspersky, файлы будут обработаны в автоматическом режиме по правилам, заданным в программе. Обнаруженные на устройстве файлы могут быть обработаны в автоматическом режиме по запросу с My Kaspersky без вашего подтверждения.

Ограничения подключения к Kaspersky Security Network

Во время работы программа может обращаться за информацией в Kaspersky Security Network. Если данные из Kaspersky Security Network получить не удалось, программа принимает решения на основании локальных антивирусных баз.

Ограничения функциональности Мониторинга активности

Функциональность противодействия программам-шифровальщикам (шифрование файлов пользователя вредоносной программой) 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 программ-шифровальщиков не предоставляется. При этом уведомление о невыполнении копирования (непредоставлении защиты) не выводится.

- Временные файлы удаляются автоматически при завершении работы Kaspersky Security Cloud или отключении компонента Мониторинг активности.

- В случае нештатного завершения работы Kaspersky Security Cloud 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 программ-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 программ-шифровальщиков после установки Kaspersky Security Cloud 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, программа не будет контролировать установленное соединение.

Программа Kaspersky Security Cloud не поддерживает обработку трафика, передаваемого через HTTPS/2 Proxy. Также программа не обрабатывает трафик, передаваемый через расширения протокола HTTP/2.

Программа Kaspersky Security Cloud 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.

Программа Kaspersky Security Cloud контролирует только те защищенные соединения, которые она может расшифровать. Программа не контролирует соединения, добавленные в список исключений (ссылка **Сайты** в окне **Настройки сети**).

Проверка и расшифровка зашифрованного трафика по умолчанию выполняется следующими компонентами:

- Веб-Антивирус;
- Безопасные платежи;
- Проверка ссылок.

Kaspersky Security Cloud расшифровывает зашифрованный трафик при работе пользователя в браузере Google Chrome, если в этом браузере отсутствует или выключено расширение Kaspersky Protection.

Kaspersky Security Cloud 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 Security Cloud 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, могут продолжать проверять защищенные соединения. Компоненты Безопасные платежи и Веб-Антивирус 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 "Лаборатории Касперского".

- 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 программа 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 Виртуальные сейфы

При создании сейфа в файловой системе FAT32 размер файла сейфа на диске не должен превышать 4 ГБ.

Особенности проверки памяти ядра на наличие руткитов во время работы в Защищенном браузере

В случае обнаружения недоверенного модуля во время работы Защищенного браузера открывается новая вкладка браузера с уведомлением о том, что была обнаружена вредоносная программа. В этом случае рекомендуется закрыть браузер и выполнить полную проверку компьютера.

Особенности защиты данных буфера обмена

Kaspersky Security Cloud разрешает программе обращаться к буферу обмена в следующих случаях:

- Программа с активным окном пытается поместить данные в буфер обмена. Активным считается окно, с которым вы работаете в настоящий момент.
- Защищенный процесс программы пытается поместить данные в буфер обмена.
- Защищенный процесс программы или процесс с активным окном пытается получить данные из буфера обмена.
- Данные из буфера обмена пытается получить процесс программы, который ранее сам поместил эти данные в буфер обмена.

Особенности обработки зараженных файлов компонентами программы

Программа по умолчанию может удалять зараженные файлы, если их лечение невозможно. Удаление по умолчанию может выполняться при обработке файлов такими компонентами, как Контроль программ, Почтовый Антивирус, Файловый Антивирус, при выполнении задач проверки, а также при обнаружении опасной активности программ компонентом Мониторинг активности.

Ограничения работы некоторых компонентов при совместной установке программы с Kaspersky Fraud Prevention for Endpoints

Работа следующих компонентов Kaspersky Security Cloud ограничивается в Защищенном браузере, если программа установлена совместно с Kaspersky Fraud Prevention for Endpoints:

- Веб-Антивирус, кроме Анти-Фишинга;
- 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 Security Cloud при включенном режиме Device Guard на Microsoft Windows 10 RS4

Частично ограничена работа следующей функциональности:

- защита буфера обмена;
- защита браузера от программ эмуляции ввода с клавиатуры и мыши (подмен вводимых данных);
- защита от программ 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 программ).

Если в операционной системе Windows включен режим работы UMCI, Kaspersky Security Cloud не обнаруживает программы 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 программах сбора информации

Если у вас на компьютере установлена программа, выполняющая сбор и отправку информации на обработку, Kaspersky Security Cloud может классифицировать такую программу как вредоносную. Чтобы избежать этого, вы можете исключить программу из проверки, настроив Kaspersky Security Cloud способом, описанным в этом документе.

Предупреждение о создании отчета об установке программы

При установке программы на компьютер создается файл отчета об установке. Если установка программы 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 программы. В случае успешной установки программы 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 программы 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 Security Cloud 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 программы.

Ограничения работы компонента Контроль программ

Если на вашем компьютере установлена программа VeraCrypt, Kaspersky Security Cloud может завершить работу при работе с компонентом Контроль программ. Для решение этой проблемы требуется обновить программу VeraCrypt до версии 1.19 или выше.

Ограничение первого запуска программы 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 Security Cloud работает со следующими ограничениями:

- Работает только Файловый Антивирус (постоянная защита). Остальные компоненты программы не работают.
- Работает самозащита файлов и системного реестра. Самозащита процессов не работает.
- Интерфейс программы недоступен до перезагрузки компьютера. Программа показывает уведомление о том, что некоторые компоненты программы 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**.
- Программа не показывает уведомления и автоматически выбирает рекомендованное действие.

Предупреждение об ошибке адаптации драйверов программы 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 Security Cloud. 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 программы:

- Сетевым экраном;
- функцией обнаружения угроз во время загрузки операционной системы;

- функцией защиты процессов программы с помощью технологии Protected Process Light (PPL) от Microsoft.

Вы можете воспользоваться следующими способами исправления ошибки:

- перезагрузить компьютер и повторить адаптацию программы из оповещения в Центре уведомлений;
- удалить и заново установить программу.

Ограничения использования функциональности Устройства в моей сети

Изменение параметров Ethernet-сети в системном реестре может привести к тому, что компонент Устройства в моей сети будет отображать Ethernet-сеть в списке обнаруженных сетей Wi-Fi и показывать устройства, подключенные к этой сети.

Ограничения проверки трафика, передаваемого по протоколу HTTPS, в браузере Mozilla Firefox

В версиях Mozilla Firefox 58.x и выше программа не проверяет трафик, передаваемый по протоколу HTTPS, если изменение настроек браузера защищено Основным паролем. При обнаружении Основного пароля в браузере, программа 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:

- Веб-Антивирус;
- Анти-Фишинг;
- Kaspersky Safe Kids;
- 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 установлена программа Malwarebytes for Windows.

Особенности установки программы на операционной системе Microsoft Windows 7 Service Pack 0 и Service Pack 1

При установке программы на операционные системы, которые не поддерживают сертификаты с цифровой подписью SHA256, программа устанавливает свой доверенный сертификат.

Другие источники информации о программе

Страница Kaspersky Security Cloud в Базе знаний

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

На странице Kaspersky Security Cloud в Базе знаний вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Security Cloud, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Обсуждение программ "Лаборатории Касперского" в нашем сообществе

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями в нашем сообществе.

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

Глоссарий

Kaspersky Security Network (KSN)

Облачная база знаний "Лаборатории Касперского", которая содержит информацию о репутации программ и сайтов. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Активация программы

Перевод программы в полнофункциональный режим. Активация выполняется пользователем во время или после установки программы. Для активации программы пользователю необходим код активации.

Антивирусные базы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных "Лаборатории Касперского" на момент выпуска антивирусных баз. Записи в антивирусных базах позволяют обнаруживать в проверяемых объектах вредоносный код. Антивирусные базы формируются специалистами "Лаборатории Касперского" и обновляются каждый час.

База вредоносных веб-адресов

Список адресов веб-ресурсов, содержимое которых может быть расценено как опасное. Список сформирован специалистами "Лаборатории Касперского", регулярно обновляется и входит в поставку программы "Лаборатории Касперского".

База фишинговых веб-адресов

Список адресов веб-ресурсов, которые определены специалистами "Лаборатории Касперского" как фишинговые. База регулярно обновляется и входит в поставку программы "Лаборатории Касперского".

Блокирование объекта

Запрет доступа к объекту со стороны внешних программ. Заблокированный объект не может быть прочитан, выполнен, изменен или удален.

Виртуальный сейф

Специальное хранилище данных, в котором файлы хранятся в зашифрованном виде. Для получения доступа к таким файлам требуется ввод пароля. Виртуальные сейфы служат для предотвращения несанкционированного доступа к данным пользователей.

Вирус

Программа, которая заражает другие программы – добавляет в них свой код, чтобы получить управление при запуске зараженных файлов. Это простое определение дает возможность выявить основное действие, выполняемое вирусом – заражение.

Возможно зараженный объект

Объект, код которого содержит модифицированный участок кода известной программы, представляющей угрозу, или объект, напоминающий такую программу по своему поведению.

Возможный спам

Сообщение, которое нельзя однозначно классифицировать как спам, но которое обладает некоторыми признаками спама (например, некоторые виды рассылок и рекламных сообщений).

Гипервизор

Программа, обеспечивающая параллельную работу нескольких операционных систем на одном компьютере.

Группа доверия

Группа, в которую Kaspersky Security Cloud помещает программу или процесс в зависимости от наличия электронной цифровой подписи программы, репутации программы в Kaspersky Security Network, доверия к источнику программы и потенциальной опасности действий, которые выполняет программа или процесс. На основании принадлежности программы к группе доверия Kaspersky Security Cloud может накладывать ограничения на действия этой программы в операционной системе.

В Kaspersky Security Cloud используются следующие группы доверия: "Доверенные", "Слабые ограничения", "Сильные ограничения", "Недоверенные".

Доверенный процесс

Программный процесс, файловые операции которого не контролируются программой "Лаборатории Касперского" в режиме постоянной защиты. При обнаружении подозрительной активности доверенного процесса Kaspersky Security Cloud исключает этот процесс из списка доверенных и блокирует его действия.

Загрузочный сектор диска

Загрузочный сектор – это особый сектор на жестком диске компьютера, дискете или другом устройстве хранения информации. Содержит сведения о файловой системе диска и программу-загрузчик, отвечающую за запуск операционной системы.

Существует ряд вирусов, поражающих загрузочные секторы дисков, которые так и называются – загрузочные вирусы (boot-вирусы). Программа "Лаборатории Касперского" позволяет проверять загрузочные секторы на присутствие вирусов и лечить их в случае заражения.

Задача

Функции, выполняемые программой "Лаборатории Касперского", реализованы в виде задач, например: задача полной проверки, задача обновления.

Зараженный объект

Объект, участок кода которого полностью совпадает с участком кода известной программы, представляющей угрозу. Специалисты "Лаборатории Касперского" не рекомендуют вам работать с такими объектами.

Защищенный браузер

Специальный режим работы обычного браузера, предназначенный для финансовых операций и покупок в интернете. С помощью Защищенного браузера программа защищает конфиденциальные данные, которые вы вводите на сайтах банков и платежных систем (например, номера банковской карты, пароли для доступа к интернет-банкам), а также предотвращает кражу платежных средств при проведении платежей онлайн.

Карантин

Специальное хранилище, в которое программа помещает резервные копии файлов, измененных или удаленных во время лечения. Копии файлов хранятся в специальном формате и не представляют опасности для компьютера.

Клавиатурный шпион

Программа, предназначенная для скрытой записи информации о клавишах, нажимаемых пользователем во время работы на компьютере. Клавиатурные шпионы также называют кейлоггерами.

Компоненты защиты

Части Kaspersky Security Cloud, предназначенные для защиты компьютера от отдельных типов угроз (например, Анти-Спам, Анти-Фишинг). Каждый компонент защиты относительно независим от других компонентов и может быть отключен или настроен отдельно.

Ложное срабатывание

Ситуация, когда незараженный объект определяется программой "Лаборатории Касперского" как зараженный из-за того, что его код напоминает код вируса.

Маска файла

Представление имени файла общими символами. Основными символами, используемыми в масках файлов, являются * и ? (где * – любое число любых символов, а ? – любой один символ).

Настройки задачи

Настройки работы программы, специфичные для каждого типа задач.

Неизвестный вирус

Новый вирус, информации о котором нет в базах. Как правило, неизвестные вирусы обнаруживаются программой в объектах при помощи эвристического анализатора. Таким объектам присваивается статус возможно зараженных.

Несовместимая программа

Антивирусная программа стороннего производителя или программа "Лаборатории Касперского", не поддерживающая управление через Kaspersky Security Cloud.

Обновление

Процедура замены / добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений "Лаборатории Касперского".

Объекты автозапуска

Набор программ, необходимых для запуска и правильной работы операционной системы и программного обеспечения вашего компьютера. Каждый раз при старте операционная система запускает эти объекты. Существуют вирусы, способные поражать именно объекты автозапуска, что может привести, например, к блокированию запуска операционной системы.

Пакет обновлений

Пакет файлов для обновления баз и программных модулей. Программа "Лаборатории Касперского" копирует пакеты обновлений с серверов обновлений "Лаборатории Касперского", затем автоматически устанавливает и применяет их.

Проверка трафика

Проверка в режиме реального времени с использованием информации текущей (последней) версии баз объектов, передаваемых по всем протоколам (например, HTTP, FTP и прочим).

Программные модули

Файлы, входящие в состав установочного пакета программы "Лаборатории Касперского" и отвечающие за реализацию его основных задач. Каждому типу задач, реализуемых программой (защита, проверка, обновление баз и программных модулей), соответствует свой программный модуль.

Протокол

Четко определенный и стандартизованный набор правил, регулирующих взаимодействие между клиентом и сервером. К ряду хорошо известных протоколов и связанных с ними служб относятся: HTTP, FTP и NNTP.

Резервное копирование данных

Создание резервных копий данных, хранящихся на компьютере. Резервные копии создаются с целью предотвращения потери данных в результате кражи, поломки оборудования или действий злоумышленников.

Руткит

Программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в операционной системе.

В операционных системах Windows под руткитом принято подразумевать программу, которая внедряется в операционную систему и перехватывает системные функции (Windows API). Перехват и модификация низкоуровневых API-функций, в первую очередь, позволяет такой программе достаточно качественно маскировать свое присутствие в операционной системе. Кроме того, как правило, руткит может маскировать присутствие в операционной системе любых описанных в его конфигурации процессов, каталогов и файлов на диске, ключей в реестре. Многие руткиты устанавливают в операционную систему свои драйверы и службы (они также являются "невидимыми").

Серверы обновлений "Лаборатории Касперского"

HTTP-серверы "Лаборатории Касперского", с которых программа "Лаборатории Касперского" получает обновления баз и программных модулей.

Скрипт

Небольшая компьютерная программа или независимая часть программы (функция), как правило, написанная для выполнения конкретной задачи. Наиболее часто применяется при использовании программ, встраиваемых в гипертекст. Скрипты запускаются, например, когда вы открываете некоторые сайты.

Если включена постоянная защита, программа отслеживает запуск скриптов, перехватывает их и проверяет на присутствие вирусов. В зависимости от результатов проверки вы можете запретить или разрешить выполнение скрипта.

Спам

Несанкционированная массовая рассылка сообщений электронной почты, чаще всего рекламного характера.

Степень угрозы

Показатель вероятности, с которой компьютерная программа может представлять угрозу для операционной системы. Степень угрозы вычисляется с помощью эвристического анализа на основании критериев двух типов:

- статических (например, информация об исполняемом файле программы: размер файла, дата создания и тому подобное);
- динамических, которые применяются во время моделирования работы программы в виртуальном окружении (анализ вызовов программой системных функций).

Степень угрозы позволяет выявить поведение, типичное для вредоносных программ. Чем ниже степень угрозы, тем больше действий в операционной системе разрешено программе.

Технология iChecker

Технология, позволяющая увеличить скорость антивирусной проверки за счет исключения тех объектов, которые не были изменены с момента предыдущей проверки, при условии, что настройки проверки (базы программы и настройки) не были изменены. Информация об этом хранится в специальной базе. Технология применяется как в режиме постоянной защиты, так и в режиме проверки по требованию.

Например, у вас есть файл архива, который был проверен программой "Лаборатории Касперского" и которому был присвоен статус *не заражен*. В следующий раз этот архив будет исключен из проверки, если он не был изменен и не менялись настройки проверки. Если вы изменили состав архива, добавив в него новый объект, изменили настройки проверки, обновили базы программы, архив будет проверен повторно.

Ограничения технологии iChecker:

- технология не работает с файлами больших размеров, так как в этом случае проверить весь файл быстрее, чем вычислять, был ли он изменен с момента последней проверки;
- технология поддерживает ограниченное число форматов.

Трассировка

Отладочное выполнение программы, при котором после выполнения каждой команды происходит остановка и отображается результат этого шага.

Упакованный файл

Исполняемый файл в сжатом виде, который содержит в себе программу-распаковщик и инструкции операционной системе для ее выполнения.

Уровень безопасности

Под уровнем безопасности понимается предустановленный набор настроек работы компонента программы.

Уязвимость

Недостаток в операционной системе или программе, который может быть использован производителями вредоносного программного обеспечения для проникновения в операционную систему или программу и нарушения ее целостности. Большое количество уязвимостей в операционной системе делает ее работу ненадежной, так как внедрившиеся в операционную систему вирусы могут вызывать сбои в работе как самой операционной системы, так и установленных программ.

Фишинг

Вид интернет-мошенничества, целью которого является получение неправомерного доступа к конфиденциальным данным пользователей.

Цифровая подпись

Зашифрованный блок данных, который входит в состав документа или программы. Цифровая подпись используется для идентификации автора документа или программы. Для создания цифровой подписи автор документа или программы должен иметь цифровой сертификат, который подтверждает личность автора.

Цифровая подпись позволяет проверить источник и целостность данных, и защититься от подделки.

Эвристический анализатор

Технология обнаружения угроз, информация о которых еще не занесена в базы "Лаборатории Касперского". Эвристический анализатор позволяет обнаруживать объекты, поведение которых в операционной системе может представлять угрозу безопасности. Объекты, обнаруженные с помощью эвристического анализатора, признаются возможно зараженными. Например, возможно зараженным может быть признан объект, который содержит последовательности команд, свойственные вредоносным объектам (открытие файла, запись в файл).

Эксплойт

Программный код, который использует какую-либо уязвимость в системе или программном обеспечении. Эксплойты часто используются для установки вредоносного программного обеспечения на компьютере без ведома пользователя.

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Adobe, Reader – товарные знаки или зарегистрированные в Соединенных Штатах Америки и / или в других странах товарные знаки Adobe Systems Incorporated.

Apple, App Store, macOS и Safari – товарные знаки Apple Inc., зарегистрированные в США и других странах.

Dropbox – товарный знак Dropbox, Inc.

Google Chrome, Google Play, Chromium, SPDY, App Store, Android – товарные знаки Google, Inc.

Intel, Celeron, Atom – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

IOS – зарегистрированный в Соединенных Штатах Америки и в других странах товарный знак Cisco Systems, Inc. и / или ее аффилированных компаний.

LogMeIn Pro и Remotely Anywhere – товарные знаки компании LogMeIn, Inc.

Mail.ru – зарегистрированный товарный знак, правообладателем которого является ООО "Мэйл.Ру".

Microsoft, Windows, Internet Explorer, Outlook, PowerShell, Skype – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Mozilla, Thunderbird и Firefox – товарные знаки Mozilla Foundation.

VMware – товарный знак VMware, Inc. или зарегистрированный в США или других юрисдикциях товарный знак VMware, Inc.

Java и JavaScript – зарегистрированные товарные знаки компании Oracle и/или ее аффилированных компаний.

Окно Расширение защиты

Развернуть всё | Свернуть всё

Пробная версия

Кнопка, при нажатии на которую запускается переход с Kaspersky Security Cloud на пробную версию Kaspersky Internet Security.

Купить код активации

По ссылке открывается окно браузера на странице интернет-магазина, в котором вы можете приобрести лицензию Kaspersky Internet Security.

Ввести код активации

По ссылке запускается мастер активации Kaspersky Internet Security.

Окно Расширение защиты

Развернуть всё | Свернуть всё

Купить код активации

По ссылке открывается окно браузера на странице интернет-магазина, в котором вы можете приобрести код активации Kaspersky Total Security.

Ввести код активации

По ссылке запускается мастер активации Kaspersky Total Security.

Пробная версия

Кнопка, при нажатии на которую запускается переход с Kaspersky Security Cloud на пробную версию Kaspersky Total Security.

Активация с помощью резервного кода активации

Развернуть всё | Свернуть всё

После нажатия на кнопку **Далее** будет применен резервный код активации.

Если срок действия лицензии еще не истек, вы можете применить код активации, с помощью которого программа была активирована ранее, на другом компьютере.

Если вы указываете резервный код активации, который был выписан на несколько устройств, то вы должны повторить процедуру добавления резервного кода на всех устройствах, на которых вы хотите автоматически продлить срок действия лицензии.

По ссылке **Отмена** вы можете отменить активацию программы.

Отмена

По ссылке вы можете отменить применение резервного кода активации и вернуться к окну **Лицензирование**.

Окно Ввод кода активации

Развернуть всё | Свернуть всё

Код активации

Поля для ввода кода активации программы. Код активации состоит из четырех групп символов (например, **ABA9C-CDEFG-ABCBC-ABC2D**). Первую группу символов нужно ввести в первое поле ввода, вторую группу – во второе и так далее.

По ссылке **Где найти код активации?** открывается окно браузера на сайте Службы технической поддержки с подробной информацией о коде активации.

Если в поле ввода вы укажете код активации Kaspersky Internet Security, по завершении активации запустится процедура перехода на Kaspersky Internet Security. Если в поле ввода вы укажете код активации Kaspersky Total Security, по завершении активации запустится процедура перехода на Kaspersky Total Security.

Активировать пробную версию программы

По ссылке выполняется активация пробной версии программы. Вы сможете использовать пробную версию программы в течение короткого ознакомительного периода в режиме полной функциональности. По истечении срока действия лицензии повторная активация пробной версии программы невозможна.

Этот вариант доступен, если пробная версия программы еще не использовалась.

Купить лицензию

По ссылке открывается окно браузера на странице интернет-магазина, в котором вы можете приобрести лицензию.

Код активации соответствует другой программе

Развернуть всё | Свернуть всё

Это окно отображается, если введенный код активации соответствует другой программе. Название программы указано в строке **Соответствующая программа**. Вы можете перейти к использованию этой программы сейчас или после истечения срока действия лицензии на Kaspersky Security Cloud.

Отмена

По ссылке вы можете отменить активацию программы.

Продолжить

При нажатии на кнопку запускается установка и активация той программы, которой соответствует введенный вами код активации.

Как настроить защиту DNS по HTTPS

Развернуть всё | Свернуть всё

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.

Kaspersky Security Cloud автоматически получает данные о том, какой DoH-сервер используется в браузере Mozilla Firefox. Если вы добавили DoH-сервер в программе Kaspersky Security Cloud 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, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. В разделе **Дополнительно** выберите подраздел **Сеть**.

   Откроется окно **Настройки сети**.
4. В блоке **Обработка трафика** по ссылке **Управлять DoH-серверами** откройте 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

Развернуть всё | Свернуть всё

Да, использовать <программа>

При выборе этого варианта работа мастера активации завершается. Программа будет работать по обнаруженной действующей лицензии. Если обнаружена лицензия на Kaspersky Internet Security или Kaspersky Total Security, будет запущен мастер миграции.

Нет, продолжить работу мастера и ввести новый код активации

При выборе этого варианта мастер активации продолжает работу и активирует Kaspersky Security Cloud. Вам потребуется ввести новый код активации, соответствующий Kaspersky Security Cloud.

Окно Регистрация

В этом окне нужно указать регистрационные данные, которые понадобятся в случае обращения в Службу технической поддержки.

Отсутствует соединение с интернетом

Развернуть всё | Свернуть всё

Это окно отображается, если попытка активировать программу не удалась из-за проблем с подключением к интернету.

Повторить попытку

По ссылке мастер активации пытается активировать программу повторно. Если проблемы с интернетом краткосрочные, то повторная попытка может оказаться успешной.

Окно Выбор папки для восстановленных файлов

Развернуть всё | Свернуть всё

В исходную папку

При выборе этого варианта Kaspersky Security Cloud помещает восстановленные файлы в папку, в которой находились исходные файлы в момент создания резервной копии.

В указанную папку

При выборе этого варианта Kaspersky Security Cloud помещает восстановленные файлы в папку, указанную в поле **Выберите папку**.

Выберите папку

Поле содержит путь к папке, в которую нужно поместить восстановленные файлы.

Поле доступно, если выбран вариант **В указанную папку**.

Обзор

При нажатии на кнопку открывается окно **Выбор папки для восстановленных файлов**. В этом окне можно выбрать папку, в которую нужно поместить восстановленные файлы.

Кнопка доступна, если выбран вариант **В указанную папку**.

При совпадении имен файлов

В раскрывающемся списке можно выбрать действие, которое должна выполнять программа, если в папке, куда требуется поместить восстановленный файл, уже находится файл с таким же именем:

- **спрашивать пользователя** – программа 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** – Kaspersky Security Cloud удаляет существующий файл и помещает на его место файл, восстановленный из резервной копии.
- **сохранить оба файла** – Kaspersky Security Cloud оставляет существующий файл без изменений и сохраняет файл, восстановленный из резервной копии, под новым именем в этой же папке.
- **не восстанавливать этот файл** – Kaspersky Security Cloud оставляет существующий файл без изменений, не восстанавливая одноименный файл из резервной копии.

Восстановить

При нажатии на кнопку запускается восстановление файлов из резервных копий.

Ошибка активации

Развернуть всё | Свернуть всё

Не удалось активировать программу. 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 программы.

Переход к использованию другой программы

Развернуть всё | Свернуть всё

После нажатия на кнопку **Далее** будет запущен мастер миграции. В результате работы мастера миграции будет установлена программа, соответствующая введенному коду активации (Kaspersky Internet Security или Kaspersky Total Security).

Если срок действия подписки на Kaspersky Security Cloud еще не истек, вы можете применить код активации Kaspersky Security Cloud на другом компьютере.

По ссылке **Отмена** вы можете отменить переход на Kaspersky Internet Security или Kaspersky Total Security.

Отмена

По ссылке можно отменить запуск мастера миграции и вернуться к предыдущему шагу.

Убедитесь, что введенный код активации не является кодом активации для подписки

Развернуть всё | Свернуть всё

Убедитесь, что код активации, который вы указываете в качестве резервного, не предназначен для использования программы по подписке. Оплата за использование программы по подписке взимается с момента оформления подписки. Если вы оформили подписку на Kaspersky Security Cloud, откажитесь от использования программы по действующей лицензии и активируйте программу с помощью кода активации для подписки.

Вы можете применить код активации, с помощью которого программа была активирована ранее, на другом компьютере до истечения срока действия лицензии.

Окно Последовательность запуска

Развернуть всё | Свернуть всё

Последовательность запуска программ

В списке содержится информация о программах, запущенных выбранной программой (дочерних программах). По умолчанию дочерние программы отсортированы по времени запуска, начиная с самого раннего.

Запуск

В графе отображается время запуска дочерней программы.

ID процесса

В графе отображается идентификатор процесса дочерней программы.

Программа

В графе отображается название дочерней программы.

Группа доверия

В графе отображается группа доверия, в которую входит программа:

- **Доверенные**. Программа работает без ограничений, но контролируется компонентом Файловый Антивирус.
- **Слабые ограничения**. Программе 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 такой программы ограничена.

- **Сильные ограничения**. Программе запрещено обращаться к конфиденциальным данным и настройкам пользователя, публичным и системным данным. При попытке выполнения привилегированных операций запрашивается разрешение пользователя. Сетевая активность такой программы заблокирована.

- **Недоверенные**. Работа такой программы полностью блокируется.

Закладка Работающие

Развернуть всё | Свернуть всё

Список работающих программ

В списке отображаются программы 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 программах и процессах:

- название исполняемого файла программы или процесса;
- сведения о производителе программы;
- идентификатор процесса;
- расположение исполняемого файла программы;
- имя пользователя, запустившего программу или процесс;
- время создания и запуска программы или процесса;
- настройки автозапуска программы.

С помощью пункта **Упорядочить столбцы по умолчанию** можно восстановить исходный вид таблицы.

По правой клавише мыши на строке программы или процесса открывается контекстное меню. Из контекстного меню можно выполнить следующие действия:

- открыть окно **Правила программы**, в котором можно настроить правила для контроля действий программы;
- отобразить последовательность запуска процессов в окне **Последовательность запуска**;
- переместить программу в другую группу доверия;
- установить для программы настройки контроля активности, предусмотренные по умолчанию;
- завершить процесс;
- открыть папку, в которой расположен исполняемый файл программы.

Вид

В раскрывающемся списке можно включить отображение системных процессов и процессов Kaspersky Security Cloud:

- **Показывать системные процессы**. При выборе этого элемента в общем списке программ и процессов отображаются процессы, необходимые для работы операционной системы.
- **Показывать процессы Kaspersky Security Cloud**. При выборе этого элемента в общем списке программ и процессов отображаются процессы, запущенные Kaspersky Security Cloud.

В раскрывающемся списке также можно выбрать способ отображения программ и процессов:

- **Показывать как список**. При выборе этого варианта программы / процессы отображаются в виде списка.
- **Показывать как дерево**. При выборе этого варианта программы / процессы отображаются в виде иерархической структуры в соответствии с последовательностью вызова процессов.

Программа

В графе отображается название программы или процесса.

Цифровая подпись

В графе отображается информация о наличии цифровой подписи у программы и владельце цифровой подписи.

Группа доверия

В графе отображается группа доверия, в которую помещена программа. В зависимости от группы доверия программы в графе отображаются следующие значки:

- Красный значок означает, что программа находится в группе "Недоверенные".
- Розовый значок означает, что программа находится в группе "Сильные ограничения".
- Желтый значок означает, что программа находится в группе "Слабые ограничения".
- Зеленый значок означает, что программа находится в группе "Доверенные".

Популярность

В графе отображается уровень популярности программы среди участников Kaspersky Security Network (KSN). Уровень популярности соответствует числу участников KSN, использующих программу.

Процессор

В графе отображается текущее потребление ресурсов центрального процессора программой / процессом.

Память

В графе отображается текущее потребление оперативной памяти программой / процессом.

Диск

В графе отображается суммарная скорость чтения и записи данных на диск программой или процессом.

Сеть

В графе отображается суммарная скорость приема и передачи данных программой через сетевой интерфейс.

Завершить процесс

При нажатии на кнопку завершается работа программы, выбранной в списке.

Закладка Запускаемые при старте

Развернуть всё | Свернуть всё

Список программ, запускаемых при старте

Список содержит программы, 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 программы или процесса открывается контекстное меню. Из контекстного меню можно выполнить следующие действия:

- открыть окно **Правила программы**, в котором можно настроить правила для контроля действий программы;
- переместить программу в другую группу доверия;
- установить для программы настройки контроля активности, предусмотренные по умолчанию;
- открыть папку, в которой расположен исполняемый файл программы.

Программа

В графе отображается название программы, запускаемой при старте операционной системы.

Статус

В графе отображается состояние программы: *Выполняется* или *Остановлено*.

Цифровая подпись

В графе отображается информация о наличии цифровой подписи у программы и владельце цифровой подписи.

Группа доверия

В графе отображается группа доверия, в которую помещена программа. В зависимости от группы доверия программы в графе отображаются следующие значки:

- Красный значок означает, что программа находится в группе "Недоверенные".
- Розовый значок означает, что программа находится в группе "Сильные ограничения".
- Желтый значок означает, что программа находится в группе "Слабые ограничения".
- Зеленый значок означает, что программа находится в группе "Доверенные".

Популярность

В графе отображается уровень популярности программы среди участников Kaspersky Security Network (KSN). Уровень популярности соответствует числу участников KSN, использующих программу.

Последний запуск

В графе отображается время последнего запуска программы.

Закладка Все программы

Развернуть всё | Свернуть всё

Список программ

В списке содержатся программы, установленные на вашем компьютере. Для каждой программы в списке отображается информация о статусе, цифровой подписи, группе доверия, популярности программы среди пользователей KSN и времени последнего запуска.

По двойному щелчку мышью на строке программы или процесса открывается окно **Правила программы**. В окне можно настроить правила для контроля действий программы.

По правой клавише мыши на строке программы открывается контекстное меню. В контекстном меню можно выполнить следующие действия:

- открыть окно **Правила программы**, в котором можно настроить разрешения для действий программы;
- разрешить или запретить запуск программы;
- переместить программу в другую группу доверия;
- установить для программы настройки контроля активности, предусмотренные по умолчанию (сбросить настройки программы);
- удалить программу из списка;
- открыть папку, содержащую исполняемый файл программы.

Программы в списке объединены в группы и подгруппы. По правой клавише мыши на строке группы открывается контекстное меню. В контекстном меню можно выполнить следующие действия:

- открыть окно **Правила группы**, в котором можно настроить разрешения для действий программ из этой группы, используемые по умолчанию;
- создать подгруппу внутри группы; по умолчанию к подгруппе применяются правила, указанные для группы, в которую она входит;
- добавить программу в группу; по умолчанию к программе применяются правила, указанные для группы, в которую она входит;

- установить для группы и всех входящих в нее подгрупп и программ настройки контроля активности, предусмотренные по умолчанию (сбросить настройки группы);
- установить для подгрупп и программ, входящих в группу, настройки контроля активности, предусмотренные по умолчанию, оставив настройки группы без изменений (сбросить настройки подгрупп и программ);
- удалить входящие в группу подгруппы и программы.

Программа

В графе отображается название программы.

Статус

В графе отображается состояние программы: *Выполняется* или *Остановлено*.

Цифровая подпись

В графе отображается информация о наличии цифровой подписи у программы и владельце цифровой подписи.

Группа доверия

В графе отображается группа доверия, в которую помещена программа. Группа доверия определяет правила использования программы на компьютере: запрет или разрешение запуска, доступ программы к файлам и системному реестру, ограничения сетевой активности программы.

Популярность

В графе отображается уровень популярности программы среди участников Kaspersky Security Network (KSN). Уровень популярности соответствует числу участников KSN, использующих программу.

Последний запуск

В графе отображается время последнего запуска программы.

Окно Нецензурные слова

Развернуть всё | Свернуть всё

Соглашение

Содержит условие, в соответствии с которым вы можете внести изменения в список нецензурных фраз.

Я достиг совершеннолетия и согласен с этими условиями

Установка флажка означает согласие с условиями, изложенными в соглашении. Если флажок установлен, список нецензурных фраз доступен для редактирования.

Если флажок снят, список нецензурных фраз недоступен для редактирования.

Окно Отправить отзыв

Развернуть всё | Свернуть всё

Проблема

Раскрывающийся список, где вы можете выбрать категорию, к которой относится ваш отзыв. Категория отзыва может затрагивать проблему с сайтом, открытым в Защищенном браузере:

- **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 браузер запускается не тогда, когда нужно**. Выберите этот элемент, если в Защищенном браузере открываются сайты, не требующие использования Безопасных платежей.
- **Не получается авторизоваться на сайте**. Выберите этот элемент, если при попытках авторизоваться на сайте, открытом в Защищенном браузере, возникают ошибки.
- **Не открывается или неправильно отображается сайт**. Выберите этот элемент, если сайты не открываются в Защищенном браузере 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 запущен Защищенный браузер**. Выберите этот элемент, если в Защищенном браузере не создаются скриншоты.
- **Ошибки во время ввода данных с клавиатуры или из буфера обмена**. Выберите этот элемент, если во время ввода данных в Защищенном браузере возникают ошибки.
- **Не печатается страница, открытая в Защищенном браузере**. 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 браузера появляется сообщение "Не установлены важные обновления операционной системы".
- **В качестве Защищенного запускается другой браузер**. Выберите этот элемент, если Защищенный браузер открывается не в том браузере, в котором вы его запустили.
- **Работает с ошибками**. Выберите этот элемент, если в работе Защищенного браузера возникают ошибки, не указанные в списке.
- **Другое**. 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 программе не удается отправить отзыв (например, отсутствует соединение с интернетом), программа 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 программы. Если флажок установлен напротив какого-либо действия, это означает, что выбранное действие разрешено пользователю или группе пользователей.

Настройка программы	Изменение настроек программы в главном окне, окне **Настройка**, в Центре уведомлений и в самих уведомлениях. Включение и выключение трассировки программы.
Управление резервным копированием	Создание, изменение, удаление задач резервного копирования, а также задач восстановления данных из резервных копий.
Управление защитой детей	Возможность запретить запуск программы Kaspersky Safe Kids с помощью компонента Контроль программ, возможность завершить работу Kaspersky Security Cloud или настроить Kaspersky Security Cloud таким образом, чтобы защита не работала. При попытке загрузить, установить или запустить Kaspersky Safe Kids пароль не запрашивается.
Завершение работы программы	Выход из программы.
Удаление / изменение / восстановление программы	Удаление, изменение или восстановление программы.
Удаление ключа	Удаление или изменение кода активации и резервного кода активации.
Просмотр отчетов	Переход в окно **Отчеты**.
Выключение компонентов защиты	Выключение и включение компонентов защиты, представленных в окне **Настройка** в разделе **Защита**.

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.

Информация о подписке

В окне содержится информация о подписке на программу:

- Статус подписки.
- Количество дней, оставшихся до окончания срока действия подписки.
- Количество компьютеров, на которые распространяется подписка.
- Дата активации.
- Дата окончания срока действия подписки.

Как настроить безопасное VPN-соединение для выбранного сайта

Чтобы настроить безопасное VPN-соединение для выбранного сайта, выполните следующие действия:

1. Откройте главное окно программы.
2. В главном окне программы нажмите на кнопку ☰.
3. Выберите пункт **Настройки** → 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 должна выполнять программа, когда вы заходите на этот сайт:

   - **Включать безопасное VPN-соединение**. Программа Kaspersky Security Cloud включает безопасное VPN-соединение, когда вы посещаете указанный сайт. Например, вы можете указать, что программа должна 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 сервер** выберите регион, через который вы хотите устанавливать безопасное VPN-соединение, когда посещаете этот сайт. Если для сайта и категории, в которую входит этот сайт, заданы разные регионы для включения безопасного VPN-соединения, подключение к сайту происходит через тот регион, который указан 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**. Программа Kaspersky Security Cloud не включает безопасное VPN-соединение, когда вы посещаете указанный сайт.

9. Нажмите на кнопку **Добавить**.

Kaspersky Secure Connection не включает безопасное VPN-соединение, если подключение к сайту выполняется по протоколу HTTPS.

Вернуться в справку Kaspersky Secure Connection.

Как настроить безопасное VPN-соединение для категорий сайтов

По умолчанию программа 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 установлена и активирована программа Kaspersky Internet Security, Kaspersky Total Security или Kaspersky Security Cloud. 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, выполните следующие действия:

1. Откройте главное окно программы.
2. В главном окне программы нажмите на кнопку ☰.
3. Выберите пункт **Настройки** → 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**. Программа будет включать безопасное VPN-соединение при посещении сайтов выбранной категории.

   - **Спрашивать**. При посещении какого-либо сайта из выбранной категории программа 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**. Программа будет выполнять выбранное вами действие каждый раз при посещении этого сайта. Если флажок не установлен, программа запоминает ваш выбор на один час.

   - **Не реагировать**. Программа не будет включать безопасное VPN-соединение при посещении сайтов выбранной категории.

7. Если выбран вариант **Включать безопасное VPN-соединение**, в раскрывающемся списке **Выбирать сервер** укажите регион, 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.

Вернуться в справку Kaspersky Secure Connection .

Контроль программ

В блоке **Программы** отображается информация о количестве программ, которые контролирует Kaspersky Security Cloud.

Управление программами

По ссылке открывается окно **Управление программами**. В этом окне можно указать группы доверия программ, разрешить или запретить запуск программ, а также перейти к настройке разрешений для отдельной программы.

В блоке **Текущая активность** отображается информация о количестве программ и процессов, выполняемых в данный момент. В графическом виде представлена информация о загрузке центрального процессора, объеме оперативной памяти и дискового пространства, а также о сетевой активности.

Показать всю активность

По ссылке открывается окно **Активность программ** на закладке **Работающие**. В этом окне можно просмотреть информацию о потреблении ресурсов компьютера каждой из программ, выполняемых в текущий момент, а также перейти к настройке разрешений для отдельной программы.

Контроль программ. Исключения

Исключения

Содержит ресурсы с персональными данными, исключаемые из области защиты Контроля программ. 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, программа контролирует действия с этим ресурсом.
- **Выключить контроль**. Если выбран этот вариант, программа 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

Развернуть всё | Свернуть всё

Закладка Общие

Описание выбранной группы программ.

Закладка Ресурсы

Развернуть всё | Свернуть всё

На этой закладке можно выбрать системные ресурсы или ресурсы пользователя и изменить права доступа программ 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 программы**. Если выбран этот вариант, в списке ресурсов не отображаются ресурсы системных программ.
- **Скрывать Kaspersky Security Cloud**. Если выбран этот вариант, в списке не отображаются ресурсы Kaspersky Security Cloud.

Операционная система

Содержит настройки и ресурсы операционной системы выбранной категории. Ресурсом может быть файл или папка, ключ реестра, сетевой сервис или IP-адрес. Контроль программ контролирует доступ других программ 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. Контроль программ анализирует действия других программ 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 программ: браузеров, файловых менеджеров, почтовых клиентов, IM-клиентов и электронных кошельков.

Ресурс

Графа, в которой содержится название ресурса операционной системы, защищаемого Контролем программ.

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, программа контролирует действия с этим ресурсом.
- **Выключить контроль**. Если выбран этот вариант, программа 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. Контроль программ не будет контролировать доступ других программ 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 программ

В списке отображаются группы доверия и программы, входящие в эти группы доверия. В графах **Чтение**, **Запись**, **Создание**, **Удаление** указаны права доступа программы или группы программ к выбранному ресурсу.

В таблице ниже приведено описание действий Kaspersky Security Cloud, если программа или группа программ пытается получить доступ к ресурсу.

Описание действий Kaspersky Security Cloud

Действие	Описание

Наследовать	Программа или группа программ наследует реакцию из вышестоящей группы.
Разрешить	Kaspersky Security Cloud разрешает программам, входящим в выбранную группу, доступ к ресурсу.
Запретить	Kaspersky Security Cloud запрещает программам, входящим в выбранную группу, доступ к ресурсу.
Спрашивать пользователя	Если в разделе **Настройки** → **Общие** установлен флажок **Автоматически выполнять рекомендуемые действия**, Kaspersky Security Cloud 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, программа спрашивает пользователя, разрешать этой программе доступ к ресурсу или нет.
Записывать в отчет	Помимо заданной реакции Kaspersky Security Cloud записывает в отчет информацию о попытке доступа программы к ресурсу.

Окно Лицензионное соглашение

Развернуть всё | Свернуть всё

Окно содержит текст Лицензионного соглашения. Для просмотра Лицензионного соглашения вы можете воспользоваться полосой прокрутки.

Как вернуться на предыдущую версию программы

Чтобы вернуться на предыдущую версию программы, выполните следующие действия:

1. Нажмите `Win+E` на клавиатуре.
2. Перейдите в папку:

- `C:\Program Files\Kaspersky Lab\Kaspersky Security Cloud <версия программы>` — для пользователей 64-битных операционных систем.
- `C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Cloud <версия программы>` — для пользователей 32-битных операционных систем.

3. Скопируйте файл `install.cfg.imported` на Рабочий стол.
4. Переименуйте скопированный файл в `settings.cfg`.
5. Удалите Kaspersky Security Cloud.
6. При удалении убедитесь, что в окне **Сохранение объектов** установлен флажок **Информация о лицензии**.
7. Перезагрузите компьютер и скачайте установочный файл предыдущей версии программы с сервера "Лаборатории Касперского".
8. Запустите установочный файл.
9. Откажитесь от поиска и скачивания новой версии, нажав **Пропустить**. Продолжите установку.
10. После окончания установки в главном окне Kaspersky Security Cloud нажмите на кнопку ⚙.
11. Выберите **Управление настройками** → **Импортировать**.
12. Выберите файл `settings.cfg` и нажмите **Открыть**.
13. Если программа запросит ваше подтверждение, нажмите **Продолжить**.

    Дождитесь завершения импорта настроек.
14. Перейдите в раздел **Дополнительно** и выберите **Обновление**.

15. Выберите вариант **Не скачивать новую версию и не уведомлять о выходе новой версии**.

    Предыдущая версия программы будет установлена с сохранением настроек и больше не будет обновляться.

Окно Лицензирование

Развернуть всё | Свернуть всё

В блоке, расположенном в верхней части окна, представлена информация о подписке:

- Статус подписки.
- Количество дней, оставшихся до окончания срока действия подписки.

О лицензии / О подписке

По ссылке открывается окно со сведениями о действующей подписке.

Перейти на My Kaspersky

По кнопке в браузере по умолчанию открывается страница My Kaspersky.

Лицензионное соглашение

При нажатии на кнопку открывается окно с текстом Лицензионного соглашения.

В зависимости от наличия подписки и от особенностей вашей версии программы в окне могут отображаться различные кнопки для запуска действий, связанных с подпиской. Ниже приведены описания кнопок, предусмотренных по умолчанию.

Продлить подписку

При нажатии на кнопку открывается окно браузера на странице интернет-магазина, в котором вы можете приобрести подписку.

Кнопка отображается, если срок действия подписки истек или истекает.

Купить подписку

При нажатии на кнопку открывается окно браузера на странице интернет-магазина, в котором вы можете приобрести подписку.

Кнопка отображается, если подписка была заблокирована или истек срок действия пробной версии.

Обновить базы

Кнопка, при нажатии на которую запускается обновление баз программы.

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 подпиской.

Обновить статус

Кнопка, при нажатии на которую с сервера поставщика услуг скачивается актуальная информация о статусе подписки.

Кнопка отображается, если программа используется по подписке.

Найдены другие несовместимые программы

Развернуть всё | Свернуть всё

Список несовместимых программ

В списке перечислены программы, несовместимые с устанавливаемой программой. Для корректной работы устанавливаемой программы нужно удалить несовместимые с ней программы.

Удалить вручную

Кнопка, при нажатии на которую открывается окно со списком программ, установленных на компьютере. В этом списке можно выбрать программы, несовместимые с устанавливаемой программой, чтобы удалить их с компьютера.

Продолжить

Кнопка, при нажатии на которую несовместимые программы, представленные в списке, остаются на компьютере, а мастер продолжает работу.

Одновременное использование программ, несовместимых с устанавливаемой программой, может привести к некорректной работе устанавливаемой программы и существенному ослаблению защиты вашего компьютера.

Найдены несовместимые программы

Развернуть всё | Свернуть всё

Список несовместимых программ

В списке перечислены программы, несовместимые с устанавливаемой программой. Для корректной работы устанавливаемой программы нужно удалить несовместимые с ней программы.

Удалить

Кнопка, при нажатии на которую несовместимые программы, представленные в списке, удаляются с компьютера, а мастер продолжает работу.

Оставить

Кнопка, при нажатии на которую несовместимые программы, представленные в списке, остаются на компьютере, а мастер продолжает работу.

Одновременное использование программ, несовместимых с устанавливаемой программой, может привести к некорректной работе устанавливаемой программы и существенному ослаблению защиты вашего компьютера.

Необходимо перезагрузить компьютер

Развернуть всё | Свернуть всё

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

Развернуть всё | Свернуть всё

Показать информацию о сертификате

Ссылка, по которой 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.

Kaspersky Security Cloud 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

Развернуть всё | Свернуть всё

Готово

Кнопка, при нажатии на которую Kaspersky Security Cloud завершает работу мастера установки сертификата.

Раздел Заблокированные компьютеры

Развернуть всё | Свернуть всё

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

Развернуть всё | Свернуть всё

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 (программы, 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 программы** на закладке **Сетевые правила**. В этом окне вы можете настроить сетевые правила для программы, которая 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 программы**. При выборе этого пункта меню открывается окно **Правила программы** на закладке **Сетевые правила**. В окне вы можете настроить сетевое правило для программы, которая 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 программы, которая использует порт, выбранный в списке.

Раздел Сетевая активность

Развернуть всё | Свернуть всё

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 Security Cloud** – в списке отображается информация о соединениях, установленных Kaspersky Security Cloud.

Сетевая активность

Содержит активные сетевые соединения, установленные на вашем компьютере в данный момент.

Для каждого соединения указана следующая информация:

- название процесса (программы, 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 программы**. При выборе этого пункта меню открывается окно **Правила программы** на закладке **Сетевые правила**. В этом окне вы можете настроить сетевое правило для программы, выбранной в списке.

- **Все сетевые правила**. При выборе этого пункта меню открывается окно **Пакетные правила**. В этом окне вы можете настроить пакетные правила для программы, выбранной 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 программ. Например, если программа 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 программ, 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

Развернуть всё | Свернуть всё

Период

Список содержит интервалы времени для просмотра распределения сетевого трафика.

Возможные значения:

- **За сегодня**. 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 каждой программы (компьютера, службы, сервера, процесса) указан объем входящего и исходящего трафика.

По двойному щелчку на программе в списке открывается окно **Правила программы** на закладке **Сетевые правила**. В этом окне вы можете настроить сетевые правила для выбранной программы.

По правой клавише мыши на элементе списка открывается контекстное меню, из которого можно перейти к настройке сетевых правил.

Меню содержит следующие пункты:

- **Сетевые правила программы**. При выборе этого пункта открывается окно **Правила программы** на закладке **Сетевые правила**, на которой вы можете настроить сетевое правило для выбранной программы.
- **Все сетевые правила**. При выборе этого пункта открывается окно **Пакетные правила**, в котором вы можете настроить пакетные правила для выбранной программы.

В нижней части окна отображается диаграмма распределения трафика выбранной программы по времени за выбранный период.

Разрыв сетевых соединений

Если в момент завершения работы на компьютере или приостановки защиты были установлены сетевые соединения, контролируемые программой, на экран будет выведено уведомление о разрыве этих соединений. Это необходимо для корректного завершения работы программы. 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 программа продолжит свою работу.

Поиск проблем / Поиск изменений

В этом окне отображается процесс анализа настроек браузера Microsoft Internet Explorer или поиск изменений, сделанных мастером настройки браузера ранее.

Процесс может занять некоторое время. Процесс можно прервать, нажав на кнопку **Отмена**.

Поиск проблем завершен / Поиск изменений завершен

Развернуть всё | Свернуть всё

Список проблем

Содержит перечисление проблем, которые обнаружила программа Kaspersky Security Cloud на предыдущем шаге. Найденные проблемы Kaspersky Security Cloud группирует в зависимости от опасности, которую они представляю:

- *Проблемы, которые настоятельно рекомендуется устранить*. Уязвимости браузера, представляющие серьезную угрозу безопасности компьютера.
- *Проблемы, которые рекомендуется устранить*. Уязвимости браузера, которые могут представлять опасность для компьютера.
- *Проблемы, которые можно устранить*. Неопасные в данный момент уязвимости браузера, которые в дальнейшем могут поставить безопасность компьютера под угрозу.

Если флажок в строке проблемы установлен, Kaspersky Security Cloud пытается устранить проблему.

Если флажок в строке проблемы снят, Kaspersky Security Cloud не устраняет проблему.

Если на первом шаге работы мастера настройки браузера был выбран вариант **Отменить изменения**, в списке содержатся устраненные ранее проблемы. Вы можете отменить действия, выполненные для устранения этих проблем.

Настройка браузера

Развернуть всё | Свернуть всё

Выполнить диагностику Microsoft Internet Explorer

Kaspersky Security Cloud запускает анализ настроек браузера Microsoft Internet Explorer.

Отменить изменения

Kaspersky Security Cloud отменяет изменения, которые были сделаны в результате предыдущей работы мастера настройки браузера.

Этот вариант доступен, если в результате предыдущей работы мастер настройки браузера внес изменения в настройки браузера.

Устранение проблем / Отмена изменений

В этом окне отображается процесс устранения проблем, обнаруженных в ходе анализа настроек браузера. Устранение проблем может занять некоторое время.

Если на первом шаге был выбран вариант **Отменить изменения**, мастер настройки браузера выполняет откат действий, выбранных на предыдущем шаге.

Завершение работы

Развернуть всё | Свернуть всё

Готово

Кнопка, при нажатии на которую мастер настройки браузера завершает работу.

Перезагрузить компьютер

Если флажок установлен, компьютер перезагружается после завершения работы мастера.

О дополнительных возможностях безопасного VPN-соединения

Дополнительные возможности безопасного VPN-соединения доступны вам, если на вашем компьютере установлена и запущена программа Kaspersky Internet Security, Kaspersky Total Security или Kaspersky Security Cloud.

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 региона. Если вы указали в настройках безопасного VPN-соединения разные регионы при подключении к сайтам разных категорий, вы можете указать, надо ли менять регион, когда вы перемещаетесь между сайтами разных категорий.
- Настройка безопасного VPN-соединения для отдельных сайтов, например, для сайтов, которые вы часто посещаете.

Вернуться в справку Kaspersky Secure Connection .

Обнаруженные объекты

Устранить

При нажатии на кнопку Kaspersky Security Cloud 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 Security Cloud

Уведомления программы, появляющиеся в области уведомлений панели задач, информируют о событиях, происходящих в процессе работы программы и требующих вашего внимания.

При появлении на экране уведомления следует выбрать один из предложенных в уведомлении вариантов действия. Оптимальный вариант – тот, который рекомендован экспертами "Лаборатории Касперского" по умолчанию.

Об облачной защите

В этом окне вы можете ознакомиться с информацией о Kaspersky Security Network.

Окно Активация

В этом окне отображается процесс активации программы.

Отмена

При нажатии на кнопку можно отменить активацию программы.

Регистрация

Адрес электронной почты

Поле для ввода адреса электронной почты для входа на сайт My Kaspersky.

Пароль

Поле для ввода пароля для входа на сайт My Kaspersky.

Войти

При нажатии на кнопку выполняется вход на сайт My Kaspersky.

Забыли пароль?

Переход к окну восстановления пароля от учетной записи на сайте My Kaspersky, если вы его забыли.

У меня нет учетной записи

При нажатии на кнопку выполняется переход к форме регистрации на сайте My Kaspersky.

Подтвердить вход

Если на сайте My Kaspersky вы настроили двухэтапную проверку, на ваш телефон будет отправлено сообщение с проверочным кодом. Введите проверочным код в поле ввода и нажмите на кнопку **Подтвердить вход**.

Двухэтапная проверка доступна не во всех регионах. Подробнее смотрите в справке My Kaspersky.

При переходе к регистрации на My Kaspersky в окне отображаются следующие поля:

Адрес электронной почты

Поле для ввода адреса электронной почты для регистрации на My Kaspersky.

Пароль

Поле для ввода пароля для регистрации на My Kaspersky.

Регион

По ссылке открывается окно выбора региона. От выбранного региона зависит, какие программы и какие способы оплаты вы сможете использовать.

Я соглашаюсь предоставить "Лаборатории Касперского" адрес своей электронной почты для получения персональных маркетинговых предложений

Если флажок установлен, вы будете получать новости от "Лаборатории Касперского" на указанный адрес электронной почты.

Я подтверждаю, что разрешаю АО "Лаборатория Касперского" использовать мой адрес электронной почты, имя и фамилию, чтобы оповещать меня по электронной почте о персонализированных специальных предложениях, обзорах, опросах, напоминать о незавершенных заказах, отправлять актуальные новости и события.

Если флажок установлен, вы будете получать на указанный адрес электронной почты специальные предложения и новости от "Лаборатории Касперского". Этот флажок доступен в следующих регионах.

В некоторых регионах флажок называется **Я подтверждаю, что разрешаю АО "Лаборатория Касперского" использовать мой адрес электронной почты, чтобы оповещать меня по электронной почте о персонализированных специальных предложениях, обзорах, опросах, напоминать о незавершенных заказах, отправлять актуальные новости и события**.

Создать

При нажатии на кнопку выполняется регистрация учетной записи My Kaspersky. На указанный вами при регистрации адрес электронной почты придет письмо, содержащее ссылку для активации учетной записи My Kaspersky.

Состав полей при создании учетной записи формируется специалистами "Лаборатории Касперского" и может меняться.

Подробнее о подключении к Kaspersky Security Cloud

Окно Выбор ключа в реестре

Развернуть всё | Свернуть всё

Выбрать

При нажатии на кнопку поля в окне **Добавление ключа реестра** заполняются значениями выбранного ключа.

Окно Выбор папки хранения сейфа

Развернуть всё | Свернуть всё

В этом окне можно выбрать папку, в которой будет храниться создаваемый сейф.

Выбрать

При нажатии на кнопку можно подтвердить, что указанный путь верный.

Окно Выбор файла или папки

Развернуть всё | Свернуть всё

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 программ

Развернуть всё | Свернуть всё

В этом окне отображаются программы, которые не удалось распределить по другим группам. Вы можете выбрать группу доверия из списка и нажать на кнопку **Сохранить**. Программы, которые не удалось распределить по другим группам, будут попадать в указанную вами группу доверия.

По умолчанию такие программы помещаются в группу **Слабые ограничения**.

Окно Группа доверия для программ, запущенных до начала работы Kaspersky Security Cloud

Развернуть всё | Свернуть всё

В этом окне можно выбрать группу доверия для неизвестных программ, запущенных до начала работы Kaspersky Security Cloud.

Список групп доверия

В списке можно указать группу доверия, в которую нужно помещать программы, запущенные до начала работы Kaspersky Security Cloud. Сетевая активность таких программ будет ограничиваться в соответствии с правилами выбранной группы доверия. По умолчанию сетевая активность программ, запущенных до начала работы Kaspersky Security Cloud, ограничивается в соответствии с правилами, заданными специалистами "Лаборатории Касперского".

Выбрать группу доверия автоматически

Если выбран этот вариант, компонент Контроль программ помещает программы, запущенные до начала работы Kaspersky Security Cloud, 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 программы, запущенные до начала работы Kaspersky Security Cloud.

Окно Добавление / изменение исключения Защиты от сбора данных

Развернуть всё | Свернуть всё

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.

Окно Добавление / Изменение категории

Развернуть всё | Свернуть всё

Название категории

В этом поле можно указать название категории ресурсов, доступ к которым со стороны программ должен анализировать и контролировать Контроль программ.

Окно Добавление / Изменение ключа реестра

Развернуть всё | Свернуть всё

Выбрать

При нажатии на кнопку открывается окно **Выбор ключа в реестре**, где вы можете выбрать ключ реестра, доступ к которому должен контролировать Контроль программ.

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 Контроль программ 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 нецензурного слова

Развернуть всё | Свернуть всё

Маска нецензурного слова

Слово или маска слова, наличие которого в сообщении является признаком спама.

Весовой коэффициент нецензурного слова

Числовое значение, выражающее вероятность того, что письмо, содержащее нецензурное слово, является спамом. Чем выше весовой коэффициент, тем выше вероятность того, что письмо, в котором содержится нецензурное слово, является спамом.

Анти-Спам определяет письмо как спам, если сумма весовых коэффициентов нецензурных слов и запрещенных фраз в письме превышает установленное значение.

Статус

В блоке **Статус** вы можете указать, должен ли Анти-Спам проверять сообщения на наличие нецензурного слова:

- **Активно**. Анти-Спам проверяет сообщения на наличие нецензурного слова.
- **Неактивно**. Анти-Спам не проверяет сообщения на наличие нецензурного слова.

Окно Добавление / Изменение файла или папки

Название

В поле можно указать название ресурса с файлом или папкой, доступ к которым должен контролировать Контроль программ.

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 программ 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\*`

  Программа 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

Развернуть всё | Свернуть всё

Это окно открывается, если программа активирована успешно.

Готово

При нажатии на кнопку завершается процедура активации программы. Выполняется переход в окно лицензирования.

Окно Запрещенные и разрешенные программы

Развернуть всё | Свернуть всё

В этом окне отображается список программ, которым разрешено или запрещено изменять настройки операционной системы. Пустой список означает, что вы еще не разрешали и не запрещали программам изменять настройки операционной системы.

Список программ

Список программ содержит следующую информацию:

- **Программа**. В графе отображается название программы.
- **Имя файла**. В графе отображается название исполняемого файла программы.
- **Путь**. В графе отображается путь к исполняемому файлу программы на жестком диске вашего компьютера.
- **Издатель**. В графе отображается цифровая подпись издателя программы.
- **Изменения**. В графе отображается, запрещено или разрешено программе изменять настройки операционной системы, браузеров, а также настройки сети.

Окно Защита приватности

В этом окне вы можете включать и выключать следующие компоненты:

Защита веб-камеры

Проверка учетных записей

Защита от сбора данных

Обновление программ. Исключения

Развернуть всё | Свернуть всё

Исключения

В список **Исключения** попадают пропущенные вами обновления установленных программ. Вы можете пропустить как отдельное обновление, так и все обновления для программы, установленной на компьютере.

Список **Исключения** состоит из следующих граф:

- **Программа** – в графе отображается название программы.
- **Пропускать** – графа может содержать следующие значения:
  - **Версия обновления** – отображается, если вы пропустили отдельное обновление для установленной программы.
  - **Все обновления** – отображается, если вы решили не обновлять программу.

Удалить из списка

При нажатии на кнопку выбранные программы удаляются из списка исключений. Кнопка доступна, если программа выбрана в списке.

Kaspersky Security Cloud будет сообщать о наличии обновлений для программ, удаленных из списка.

Окно Исключения Защиты от сбора данных

Развернуть всё | Свернуть всё

Список исключений

Список включает в себя адреса сайтов, на которых разрешен сбор данных о ваших действиях. На указанных сайтах компонент Защита от сбора данных 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 программ

Развернуть всё | Свернуть всё

Программа

В графе отображаются программы и группы программ, использование которых вы можете ограничить.

Использование

В графе указано, разрешено или запрещено пользователю работать с программой или группой программ:

- **Разрешено** – пользователь может работать с этой программой или группой программ.
- **Заблокировано** – пользователю запрещено работать с этой программой или группой программ.
- **Ограничено** – пользователь может работать с этой программой или группой программ ограниченное количество времени.

Вы можете разрешить, запретить или ограничить использование программы или группы программ для выбранного пользователя, выбрав нужный пункт раскрывающегося списка.

Путь

В графе отображается путь к исполняемому файлу программы.

Правила

По кнопке открывается окно, где вы можете ограничить использование выбранной программы по времени.

Удалить

Нажатие на кнопку удаляет выбранную программу из списка. После удаления программы из списка Kaspersky Security Cloud перестает контролировать использование программы, пользователь может работать с этой программой без ограничений.

Добавить программу

По кнопке открывается окно, в котором вы можете выбрать исполняемый файл программы для добавления в список. Kaspersky Safe Kids помещает программу в подходящую категорию в списке.

Окно Карантин

Развернуть всё | Свернуть всё

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 Kaspersky Security Cloud возвращает файл, выбранный в списке, в папку, в которой он находился до помещения на карантин.

Удалить

Кнопка, при нажатии на которую Kaspersky Security Cloud удаляет файл, выбранный в списке.

Удалить все

При нажатии на кнопку Kaspersky Security Cloud удаляет все резервные копии файлов, помещенные на карантин.

Kaspersky Security Cloud 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 Kaspersky Security Cloud 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 Нецензурные слова

В этом окне представлен список нецензурных слов. По наличию этих слов Kaspersky Security Cloud определяет, что сообщение является спамом.

Кнопка

При нажатии на кнопку открывается меню, в котором можно выбрать действие:

- Импортировать и добавить к существующему. При выборе этого действия можно загрузить список нецензурных слов из файла формата CSV. Текущие фразы не удаляются.
- Импортировать и заменить существующий. При выборе этого действия можно загрузить список нецензурных слов из файла формата CSV. Текущие фразы удаляются.
- Экспортировать. При выборе этого действия можно сохранить список нецензурных слов в файле формата CSV.

Нецензурное слово

Графа, в которой отображается слово или словосочетание. Наличие этого слова или словосочетания может означать, что сообщение является спамом.

Вес

В графе отображается весовой коэффициент, присвоенный нецензурному слову. Если в сообщении несколько нецензурных слов, суммарный коэффициент которых превышает 100, такое сообщение считается спамом.

Статус

Графа, в которой указано, использует ли Анти-Спам это слово при проверке сообщений на наличие нецензурных слов.

- **Активно**. Программа проверяет наличие этого слова в сообщениях.
- **Неактивно**. Программа не проверяет наличие этого слова в сообщениях.

Изменить

При нажатии на кнопку открывается окно, в котором можно изменить выбранное в списке нецензурное слово или маску слова.

Удалить

При нажатии на кнопку можно удалить нецензурное слово.

Добавить

При нажатии на кнопку открывается окно, в котором можно добавить в список нецензурное слово или маску слова.

Окно Новости

Развернуть всё | Свернуть всё

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 Новость

Развернуть всё | Свернуть всё

Ссылки на Twitter и социальные сети

По ссылкам можно перейти на ваши страницы в социальных сетях или в Twitter для публикации новости. Текст публикации можно дополнить.

Если вход на страницу не был выполнен, сайт социальной сети откроется на странице авторизации.

Ссылки на социальные сети отображаются, если их посещение разрешено.

Кнопки 

Кнопки, с помощью которых можно переходить к предыдущей или следующей новости.

Окно Настройки Менеджера программ

Развернуть всё | Свернуть всё

Включить / выключить Менеджер программ

Включение Менеджера программ. Если переключатель включен, программа Kaspersky Security Cloud контролирует установку и удаление дополнительных программ, а также показ шагов установки, содержащих рекламу.

Во время установки программ автоматически снимать флажки установки дополнительных программ. Предупреждать при попытке установить дополнительные программы

Если флажок установлен, при установке программ на ваш компьютер Kaspersky Security Cloud блокирует установку дополнительных программ.

Если флажок снят после того, как вы уже запустили установку какой-либо программы, помощник по установке продолжит свою работу в рамках текущей установки. Флажки напротив программ, предлагаемых к дополнительной установке, будут сняты, а сами дополнительные программы не будут устанавливаться. При последующей установке программ эта функциональность работать не будет. Дополнительные программы будут устанавливаться совместно с основной.

Не отображать шаги установки, которые могут содержать рекламу или предложения об установке дополнительных программ

Если флажок установлен, при установке программ на ваш компьютер Kaspersky Security Cloud блокирует показ рекламы или предложений об установке дополнительных программ.

Выполнять анализ установленных программ и расширений браузеров

Если флажок установлен, Kaspersky Security Cloud будет регулярно анализировать установленные программы и расширения браузеров с точки зрения возможных причин для их удаления.

Выбрать категории объектов

По ссылке открывается окно, в котором вы можете выбрать категории установленных программ и расширений браузеров, которые Kaspersky Security Cloud будет анализировать с точки зрения возможных причин для их удаления.

Настроить расписание

По ссылке открывается окно, в котором вы можете указать, в какие дни и в какое время Kaspersky Security Cloud будет проводить анализ установленных программ и расширений браузеров.

Исключения

По ссылке открывается окно **Исключения**. В окне представлены программы, которые вы добавили в список исключений, нажав на кнопку **Игнорировать** в списке обнаруженных программ компонента Очистка компьютера.

Окно Настройки обновления программ

Развернуть всё | Свернуть всё

Включить поиск обновлений для программ

Если флажок установлен, Kaspersky Security Cloud ищет обновления для установленных программ и предлагает скачать и установить их.

Задать режим поиска обновлений

По ссылке открывается окно, в котором вы можете задать режим поиска обновлений для программ, установленных на вашем компьютере.

Автоматически скачивать и устанавливать обновления, если не требуется принимать новое лицензионное соглашение

Если флажок установлен, Kaspersky Security Cloud автоматически ищет обновления для установленных программ, а также скачивает и устанавливает найденные обновления, если для этого от вас не требуется принять новое лицензионное соглашение.

Искать обновления для программ

В настройке требуется выбрать, какие обновления программ будет скачивать и устанавливать Kaspersky Security Cloud:

- **Важные обновления, которые повышают безопасность компьютера** – Kaspersky Security Cloud устанавливает для программ только важные обновления, которые устраняют уязвимости и повышают безопасность вашего компьютера.
- **Все обновления для известных программ** – Kaspersky Security Cloud устанавливает для программ все обновления.

Исключения

По ссылке открывается окно **Исключения** со списком исключений. В список исключений попадают пропущенные вами обновления установленных программ. Вы можете пропустить как отдельное обновление, так и все обновления для программы, установленной на компьютере.

Режим поиска обновлений / Расписание

В таблице описаны настройки, применимые к расписанию работы следующих компонентов: Обновление программ, Менеджер программ.

Настройка	Описание
Режим поиска обновлений (Обновление программ) **Выполнять анализ**	**Автоматически**. Kaspersky Security Cloud выполняет задачу один раз в сутки согласно внутренним настройкам.

(Менеджер программ)	**По минутам** / **По часам** / **По дням** / **Еженедельно** / **Каждый месяц** / **В указанное время**. Kaspersky Security Cloud выполняет задачу по сформированному вами расписанию, которое можно уточнить до минут. При выборе одного из этих вариантов доступен флажок **Отложить запуск после старта программы на** N **минут**. **После запуска программы**. Kaspersky Security Cloud выполняет задачу после своего запуска, спустя столько минут, сколько указано в поле **Запускать через** N **минут**. **После каждого обновления**. Kaspersky Security Cloud выполняет задачу после загрузки и установки нового пакета обновлений.
Запускать поиск обновлений на следующий день, если компьютер был выключен (Обновление программ) **Выполнять анализ объектов на следующий день, если компьютер был выключен** (Менеджер программ)	Если запланированный по расписанию поиск обновлений для программ или анализ объектов пропущен из-за того, что компьютер был выключен, Kaspersky Security Cloud выполняет задачу после включения компьютера. Флажок отображается, если выбран один из следующих режимов запуска: **По дням** / **Еженедельно** / **Каждый месяц** / **В указанное время**.
Искать обновления для программ только в случае, когда компьютер заблокирован или включена экранная заставка (Обновление программ) **Выполнять анализ объектов только в случае, когда компьютер заблокирован или включена экранная заставка**	Kaspersky Security Cloud 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**.

(Менеджер программ)

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 Kaspersky Security Cloud 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, Kaspersky Security Cloud 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** / **Каждый месяц** / **В указанное время** / **После запуска программы**. Режим запуска задачи обновления, при котором Kaspersky Security Cloud выполняет задачу обновления по сформированному вами расписанию. Если выбран этот режим запуска задачи обновления, вы также можете запускать задачу обновления Kaspersky Security Cloud 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 программа 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, Kaspersky Security Cloud обращается к ним по очереди, пока не скачает пакет обновлений с первого доступного источника обновлений.
Запускать	По ссылке открывается окно, в котором вы можете выбрать, от имени какого пользователя запускать обновление баз.

обновление баз с правами	По умолчанию задача обновления Kaspersky Security Cloud запускается от имени пользователя, с правами которого вы зарегистрированы в операционной системе. Однако обновление Kaspersky Security Cloud 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 Kaspersky Security Cloud и запускать задачу обновления Kaspersky Security Cloud от имени этого пользователя.

Окно Поиск уязвимостей

Развернуть всё | Свернуть всё

Начать поиск

Кнопка, при нажатии на которую запускается поиск уязвимостей.

Остановить

Кнопка, при нажатии на которую поиск уязвимостей останавливается.

Кнопка отображается, если запущен поиск уязвимостей.

<N> уязвимых программ

По ссылке открывается окно **Уязвимые программы** со списком уязвимых программ, обнаруженных при проверке. Ссылка отображается, если был запущен поиск уязвимостей.

Окно Приостановка защиты

Развернуть всё | Свернуть всё

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 программы

Режим возобновления работы компонентов защиты, при котором защита включается после перезапуска программы или перезагрузки операционной системы (при условии, что включен автоматический запуск программы).

Приостановить

Режим возобновления работы компонентов защиты, при котором защита включится только тогда, когда вы сами решите возобновить ее.

Окно Проверка пароля

Развернуть всё | Свернуть всё

Пароль

Пароль, ограничивающий доступ к управлению Kaspersky Security Cloud.

Запомнить пароль на эту сессию

Если флажок установлен, Kaspersky Security Cloud запоминает введенный пароль и больше не запрашивает его во время текущего сеанса работы.

Окно Программы, которым запрещен доступ к веб-камере

Развернуть всё | Свернуть всё

В окне отображаются программы, которым вы запретили доступ к веб-камере.

Разрешить доступ к веб-камере

При нажатии на кнопку программе, выбранной в списке, разрешается доступ к веб-камере.

Окно Рекомендуемая настройка

Развернуть всё | Свернуть всё

Включить защиту от рекламных предложений, чтобы устанавливать только нужные программы и блокировать дополнительные установки

Если флажок установлен, Kaspersky Security Cloud блокирует показ рекламы во время установки на компьютер какого-либо программного обеспечения. При этом блокируется также установка предлагаемых в рекламе дополнительных программ.

Готово

При нажатии на кнопку вы переходите в главное окно программы.

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 Kaspersky Security Cloud.

❗ **Критические события**. События критической важности, указывающие на проблемы в работе Kaspersky Security Cloud или на уязвимости в защите компьютера пользователя.

По кнопке **Сохранить отчет** можно сохранить отчет в файл формата TXT или CSV.

Окно Настройки учетной записи

Развернуть всё | Свернуть всё

Запускать обновления баз с правами

Выбор учетной записи, с правами которой Kaspersky Security Cloud будет запускать задачи обновления. Функция доступна для запуска задачи обновления Kaspersky Security Cloud 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**.

Отправка отчета

Развернуть всё | Свернуть всё

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 программой всех команд, а также информация о состоянии программы.

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 на компьютере

По ссылке открывается окно для сохранения файла отчета.

Введите номер запроса

Номер, присвоенный вашему запросу при обращении в Службу технической поддержки через сайт My Kaspersky.

Отправить отчет

Кнопка, при нажатии на которую выбранные файлы загружаются на FTP-сервер Службы технической поддержки.

Окно Полученные для анализа данные

Развернуть всё | Свернуть всё

Список файлов данных

Список файлов, которые Kaspersky Security Cloud включает в отчет, отсылаемый на сервер Службы технической поддержки. В состав списка входят файлы трассировок и дампов. В этих файлах сохранена история выполнения программой всех команд, а также информация о состоянии программы.

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. Kaspersky Security Cloud помещает файл в отчет, если установлен флажок в строке этого файла.

Запуск скрипта

Развернуть всё | Свернуть всё

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

Развернуть всё | Свернуть всё

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

Развернуть всё | Свернуть всё

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 программы

Уязвимые программы

Содержит найденные в программах уязвимости.

Из-за особенностей работы службы обновлений уязвимости некоторых программ 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 программы и установить его.

- **Добавить в исключения**

Кнопка, при нажатии на которую Kaspersky Security Cloud добавляет программу в доверенную зону.

Выберите zip-файл или папку

Применение альтернативных тем оформления доступно не во всех регионах.

При выборе темы оформления учитывайте следующие ограничения:

- Kaspersky Security Cloud 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 программы.

- Темы оформления предназначены для определенной версии Kaspersky Security Cloud и не применимы к другим версиям и другим программам. При обновлении программы до новой версии или установки поверх нее другой программы 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 отображения Kaspersky Security Cloud** из-за того, что шрифт сливается с фоном и нужные элементы управления неразличимы), рекомендуется переустановить Kaspersky Security Cloud.

Более подробную информацию вы можете найти в статье о применении альтернативных тем оформления .

Окно Добавление / изменение исключения для аппаратной клавиатуры

Развернуть всё | Свернуть всё

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 Kaspersky Security Cloud защищать ввод данных с аппаратной клавиатуры для выбранного сайта или веб-страницы.

Защищать

Kaspersky Security Cloud защищает ввод данных с аппаратной клавиатуры для выбранного сайта или веб-страницы.

Не защищать

Kaspersky Security Cloud не защищает ввод данных с аппаратной клавиатуры для выбранного сайта или веб-страницы.

Окно Добавление / изменение исключения для Экранной клавиатуры

Развернуть всё | Свернуть всё

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, должна или не должна программа показывать значок Экранной клавиатуры на страницах, соответствующих заданной маске веб-адреса.

Показывать значок в окне браузера

Kaspersky Security Cloud отображает значок быстрого вызова Экранной клавиатуры в полях ввода.

Не показывать значок в окне браузера

Kaspersky Security Cloud не отображает значок быстрого вызова Экранной клавиатуры в полях ввода.

Настройки отчетов и карантина

Развернуть всё | Свернуть всё

В блоке **Отчеты** вы можете изменить настройки формирования и хранения отчетов.

Хранить отчеты не более чем

Флажок включает / выключает функцию ограничения срока хранения отчетов. Срок хранения может составлять один день, одну неделю, один или шесть месяцев или один год.

Если флажок установлен, отчеты хранятся в течение срока, выбранного в раскрывающемся списке рядом с флажком. По истечении этого срока Kaspersky Security Cloud удаляет отчет.

Если флажок снят, срок хранения отчетов не ограничен.

Ограничить размер файла отчетов до

Флажок включает / выключает функцию, которая ограничивает максимальный размер файла отчета. Максимальный размер файла указывается в мегабайтах.

Если флажок установлен, то по умолчанию максимальный размер файла отчета составляет 1024 МБ. Когда файл достигает максимального размера, самые старые записи удаляются из файла по мере добавления новых записей.

Если флажок снят, то размер файла отчета не ограничен.

Очистить

При нажатии на кнопку Kaspersky Security Cloud удаляет данные из папки отчетов.

По умолчанию Kaspersky Security Cloud удаляет отчеты задач проверки, отчеты задачи обновления, отчеты обработки правил Сетевого экрана.

В блоке **Карантин** вы можете изменить настройки карантина.

Хранить объекты не более чем

Флажок включает / выключает функцию ограничения срока хранения объектов на карантине. Срок хранения может составлять один день, одну неделю, один или шесть месяцев или один год.

Если флажок установлен, объекты хранятся в течение срока, выбранного в раскрывающемся списке рядом с флажком.

Если флажок снят, срок хранения объектов не ограничен.

Ограничить размер карантина до

Флажок включает / выключает функцию, которая ограничивает максимальный размер карантина. Размер карантина указывается в мегабайтах.

Если флажок установлен, по умолчанию максимальный размер хранилища составляет 100 МБ. При достижении максимального размера самые старые объекты удаляются из хранилища, а новые добавляются.

Если флажок снят, размер хранилища не ограничен.

Настройки самозащиты

Развернуть всё | Свернуть всё

Включить самозащиту

Флажок включает / выключает механизм защиты Kaspersky Security Cloud 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, Kaspersky Security Cloud блокирует любую попытку удаленного управления сервисами программ. При попытке удаленного управления появляется уведомление над значком Kaspersky Security Cloud в области уведомлений панели задач Microsoft Windows (если уведомления не отключены).

Разрешить управление настройками Kaspersky Security Cloud через программы удаленного управления

Если флажок установлен, доверенные программы удаленного администрирования (такие как TeamViewer, LogMeIn Pro и Remotely Anywhere) могут изменять настройки Kaspersky Security Cloud.

Недоверенным программам удаленного администрирования изменение настроек Kaspersky Security Cloud будет запрещено, даже если флажок установлен.

Настройки прокси-сервера

Развернуть всё | Свернуть всё

Не использовать прокси-сервер

Переключатель включает / выключает использование прокси-сервера для выхода в интернет. Kaspersky Security Cloud использует подключение к интернету в работе некоторых компонентов защиты, а также для обновления баз и программных модулей.

Автоматически определять настройки прокси-сервера

Kaspersky Security Cloud 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 Security Cloud использует настройки прокси-сервера, указанные в браузере Microsoft Edge на базе Chromium. Kaspersky Security Cloud не учитывает настройки прокси-серверов, указанные для других браузеров, установленных на компьютере пользователя.

Использовать указанные настройки прокси-сервера

Kaspersky Security Cloud 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 Kaspersky Security Cloud попытается выполнить NTLM-, а затем BASIC-аутентификацию.

Если флажок не установлен или настройки прокси-сервера не указаны, то Kaspersky Security Cloud 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, Kaspersky Security Cloud будет использовать в дальнейшем указанные имя пользователя и пароль. В противном случае Kaspersky Security Cloud 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, Kaspersky Security Cloud не использует прокси-сервер при обновлении баз и программных модулей из локальной или сетевой папки.

Если флажок снят, Kaspersky Security Cloud использует прокси-сервер при обновлении баз и программных модулей из локальной или сетевой папки.

Настройки уведомлений

Развернуть всё | Свернуть всё

Уведомлять о событиях

Флажок включает / выключает уведомление о событиях.

Если флажок снят, Kaspersky Security Cloud не уведомляет вас о событиях, возникающих в ходе работы, но записывает информацию о них в отчет.

Уведомления могут быть реализованы следующими способами:

- всплывающими сообщениями над значком Kaspersky Security Cloud в области уведомлений панели задач;
- звуковыми оповещениями.

Показывать уведомления в учетной записи ребенка

Если флажок установлен, когда вы входите в операционную систему под учетной записью, которая привязана к профилю ребенка в программе Kaspersky Safe Kids, Kaspersky Security Cloud продолжает показывать следующие уведомления:

- уведомления о новостях безопасности;
- уведомления о том, что в операционной системе обнаружены небезопасные настройки;
- уведомления о том, что текущее устройство подключилось к сети Wi-Fi;
- уведомления о том, что к домашней сети Wi-Fi подключилось какое-либо устройство;
- уведомления в браузере о том, что пароль, который вы вводите на сайте, недостаточно надежен;
- уведомления о том, что пароль, который вы вводите на сайте, вы уже использовали на другом сайте.

Если флажок снят, когда вы входите в операционную систему под учетной записью, которая привязана к профилю ребенка в программе Kaspersky Safe Kids, Kaspersky Security Cloud перестает показывать эти уведомления.

Восстановить все скрытые уведомления

По ссылке вы можете восстановить значения настроек отображения уведомлений. Если ранее вы заблокировали отображение уведомлений, эти уведомления снова будут отображаться.

Если скрытых уведомлений нет, ссылка недоступна.

Сопровождать уведомления звуковыми сигналами

Флажок включает / выключает звуковое сопровождение уведомлений.

По умолчанию уведомления о критических событиях (например, об обнаружении вредоносной программы) сопровождаются звуковым сигналом.

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

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

Получать информационные и рекламные сообщения "Лаборатории Касперского"

Флажок включает / выключает отображение уведомлений о непрочитанных новостях в области уведомлений панели задач.

Если флажок снят, Kaspersky Security Cloud продолжает получать информационные и рекламные сообщения "Лаборатории Касперского", но не отображает уведомления о них.

Если флажок установлен, вы соглашаетесь передавать в "Лабораторию Касперского" данные, которые используются для формирования наиболее подходящих предложений информационного и рекламного характера. Подробнее о том, какие именно данные передаются, вы можете прочитать в разделе Предоставление данных.

Отображать информацию о специальных предложениях

Флажок включает / выключает настройку отображения информации о программах и специальных предложениях на сайтах "Лаборатории Касперского" и сайтах компаний-партнеров.

Если флажок установлен, на сайтах отображаются специальные предложения о покупке программ, подобранные с учетом уже приобретенных вами лицензий на использование программ "Лаборатории Касперского".

Если флажок снят, на сайтах отображаются стандартные предложения о покупке программ.

Получать информацию о специальных предложениях для пользователей социальных сетей

Если флажок установлен, Kaspersky Security Cloud определяет, являетесь ли вы пользователем социальных сетей, и отображает в новостях информацию о действиях "Лаборатории Касперского" в социальных сетях.

Если флажок снят, Kaspersky Security Cloud отображает стандартные новости "Лаборатории Касперского".

Получать информационные и рекламные сообщения по истечении срока действия лицензии

Если флажок установлен, по истечении срока действия подписки программа продолжает загружать и показывать новые информационные и рекламные сообщения.

Если флажок снят, новые информационные и рекламные сообщения не загружаются. Программа показывает сообщения, полученные до истечения срока действия подписки.

Раздел Защита

Развернуть всё | Свернуть всё

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.

Настройки Защиты веб-камеры

Развернуть всё | Свернуть всё

Включить / выключить Защиту веб-камеры

Переключатель включает / выключает компонент Защита веб-камеры.

Запретить всем программам доступ к веб-камере

Если флажок установлен, то запрет на доступ к веб-камере распространяется на все установленные на вашем компьютере программы.

Если флажок снят, то Kaspersky Security Cloud контролирует доступ программ к веб-камере на основе принадлежности программы к группе доверия:

- **Доверенные** – доступ к веб-камере разрешен.
- **Слабые ограничения** – при попытке доступа к веб-камере Kaspersky Security Cloud выводит на экран окно с запросом разрешения на доступ этой программы к веб-камере.
- **Сильные ограничения** и **Недоверенные** – доступ к веб-камере запрещен.

Показывать уведомление, когда веб-камеру использует программа, которой это разрешено

Если флажок установлен, Kaspersky Security Cloud выводит на экран уведомление при доступе к веб-камере программы, которой доступ разрешен. С помощью уведомления вы можете изменить настройки доступа программы к веб-камере, а также отказаться от дальнейшего отображения уведомлений.

Если флажок снят, уведомление не выводится.

Флажок доступен, если снят флажок **Запретить всем программам доступ к веб-камере**.

Обнаружено подозрительное перенаправление

Развернуть всё | Свернуть всё

Удалить записи

Kaspersky Security Cloud удаляет все подозрительные записи из файла hosts.

Пропустить

Kaspersky Security Cloud 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 программы к серверам "Лаборатории Касперского".

Рекомендуется удалять подозрительные записи из файла hosts.

Окно Ввод пароля

Развернуть всё | Свернуть всё

Текущий пароль

Текущий пароль, который используется для доступа к управлению Kaspersky Security Cloud.

Запомнить пароль на эту сессию

Если флажок установлен, Kaspersky Security Cloud запоминает введенный пароль и больше не запрашивает его во время текущего сеанса работы.

Окно Защита паролем

Развернуть всё | Свернуть всё

Ссылка **Изменить или удалить пароль** отображается, если пароль для защиты доступа к функциям Kaspersky Security Cloud ранее был задан.

Изменить или удалить пароль

По ссылке отображаются поля ввода, в которых можно указать новый пароль и подтвердить его.

Новый пароль

Пароль для доступа к управлению Kaspersky Security Cloud.

Подтверждение пароля

Повторный ввод пароля, введенного в поле **Новый пароль**.

В блоке **Область действия пароля** вы можете указать, какие функции управления программой нужно защитить паролем.

Настройка программы

Флажок включает / выключает запрос пароля при попытке пользователя сохранить изменения настроек программы.

Управление Резервным копированием

Флажок включает / выключает запрос пароля при попытке пользователя открыть окно **Резервное копирование**.

Завершение работы программы

Флажок включает / выключает запрос пароля при попытке пользователя завершить работу программы.

Удаление программы

Флажок включает / выключает запрос пароля при попытке пользователя удалить программу.

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 Kaspersky Security Cloud применяет разные наборы настроек. Наборы настроек, сохраненные в программе, называются *уровнями безопасности*. • **Предельный**. Kaspersky Security Cloud проверяет файлы всех типов. Во время проверки составных файлов Kaspersky Security Cloud дополнительно проверяет файлы почтовых форматов. • **Оптимальный**. Kaspersky Security Cloud проверяет только файлы определенных форматов на всех жестких, сменных и сетевых дисках компьютера, а также вложенные OLE-объекты. Kaspersky Security Cloud не проверяет архивы и установочные пакеты.

- **Низкий**. Kaspersky Security Cloud проверяет только новые и измененные файлы с определенными расширениями на всех жестких, сменных и сетевых дисках компьютера. Kaspersky Security Cloud не проверяет составные файлы.

Действие при обнаружении угрозы

- **Спрашивать пользователя**. Если во время проверки программа Kaspersky Security Cloud обнаруживает зараженный или возможно зараженный объект, она сразу уведомляет вас об этом и запрашивает действие над обнаруженным объектом.

  Этот вариант доступен, если в разделе **Настройки** → **Общие** снят флажок **Автоматически выполнять рекомендуемые действия**.

- **Выбирать действие автоматически**. При обнаружении зараженных или возможно зараженных объектов Kaspersky Security Cloud выполняет действие, рекомендуемое специалистами "Лаборатории Касперского":

  - Зараженный объект Kaspersky Security Cloud сначала пытается вылечить и, если это не удается - удаляет.

  - Возможно зараженный объект Kaspersky Security Cloud удаляет, если установлен флажок **Удалять вредоносные утилиты, рекламные программы, программы автодозвона и подозрительные упаковщики**. Если флажок снят, Kaspersky Security Cloud не удаляет возможно зараженный объект; уведомление об обнаружении такого объекта отображается в центре уведомлений (открывается по кнопке **Подробнее** в главном окне программы).

  Этот вариант доступен, если в разделе **Настройки** → **Общие** установлен флажок **Автоматически выполнять рекомендуемые действия**.

- **Лечить; удалять, если лечение невозможно** Если выбран этот вариант действия, то Kaspersky Security Cloud автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Security Cloud их удаляет.

- **Лечить; блокировать, если лечение невозможно**. Если выбран этот вариант действия, то Kaspersky Security Cloud автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то

Kaspersky Security Cloud добавляет информацию об обнаруженных зараженных файлах в список обнаруженных объектов.

- **Информировать**. Если выбран этот вариант действия, то при обнаружении зараженных файлов Kaspersky Security Cloud добавляет информацию об этих файлах в список обнаруженных объектов.

Перед лечением или удалением зараженного файла Kaspersky Security Cloud формирует его резервную копию на тот случай, если впоследствии понадобится восстановить файл или появится возможность его вылечить.

Изменить область проверки (нет в настройках проверки из контекстного меню)	По ссылке открывается окно со списком объектов, которые проверяет Kaspersky Security Cloud. В зависимости от типа проверки (полная проверка, быстрая проверка или выборочная проверка) в список по умолчанию включены разные объекты. 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 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 Kaspersky Security Cloud выполняет задачу проверки по сформированному вами расписанию. Если выбран этот режим запуска задачи проверки, вы также можете запускать задачу проверки вручную.
Запускать проверку с	По ссылке открывается окно, в котором вы можете выбрать, от имени какого пользователя запускать проверку.

правами	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 Kaspersky Security Cloud, и запускать задачу проверки от имени этого пользователя.
Типы файлов	Файлы без расширения Kaspersky Security Cloud считает исполняемыми. Kaspersky Security Cloud проверяет исполняемые файлы всегда, независимо от того, файлы какого типа вы выбрали для проверки. **Все файлы**. Если выбран этот параметр, Kaspersky Security Cloud проверяет все файлы без исключения (любых форматов и расширений). **Файлы, проверяемые по формату**. Если выбран этот параметр, Kaspersky Security Cloud 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, Kaspersky Security Cloud 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 файлы, если их проверка длится более N секунд	Ограничение длительности проверки одного объекта. По истечении заданного времени Kaspersky Security Cloud прекращает проверку файла. Это позволит сократить время выполнения проверки.
Проверять	Проверка архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.

архивы	
Проверять дистрибутивы	Флажок включает / выключает проверку дистрибутивов сторонних программ.
Проверять файлы офисных форматов	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты.
Проверять файлы почтовых форматов	Флажок включает / выключает функцию, с помощью которой Kaspersky Security Cloud проверяет файлы почтовых форматов, а также почтовые базы данных. Программа 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, Kaspersky Security Cloud разбирает файл почтового формата и анализирует на наличие вирусов каждый его компонент (тело письма, вложения). Если флажок снят, Kaspersky Security Cloud проверяет файл почтового формата как единый объект.
Проверять архивы, защищенные паролем	Если флажок установлен, Kaspersky Security Cloud проверяет архивы, защищенные паролем. Перед проверкой файлов, содержащихся в архиве, на экран выводится запрос пароля. Если флажок не установлен, Kaspersky Security Cloud пропускает проверку защищенных паролем архивов.
Не распаковывать составные файлы большого размера **Максимальный размер файла**	Если флажок установлен, то Kaspersky Security Cloud не проверяет составные файлы, размеры которых больше заданного значения. Если флажок снят, Kaspersky Security Cloud проверяет составные файлы любого размера. Kaspersky Security Cloud проверяет файлы больших размеров, извлеченные из архивов, независимо от состояния флажка.

Эвристический анализ	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз программ "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.
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 Kaspersky Security Cloud, 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 программе структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

Настройки проверки съемных дисков

Настройка	Описание
Действие при подключении съемного диска	• **Быстрая проверка**. Если выбран этот вариант, то после подключения внешнего устройства Kaspersky Security Cloud проверяет только файлы определенных форматов, наиболее подверженные заражению, находящиеся в корневой папке подключенного устройства. Также при быстрой проверке программа не распаковывает и не проверяет архивы. • **Подробная проверка**. Если выбран этот вариант, то после подключения внешнего устройства Kaspersky Security Cloud проверяет все файлы, расположенные во всех папках внешнего устройства, а также распаковывает и проверяет архивы, кроме защищенных паролем.

Максимальный размер съемного диска	Если флажок установлен, то Kaspersky Security Cloud проверяет внешние устройства, размер которых не превышает указанный максимальный размер. Если флажок снят, то Kaspersky Security Cloud проверяет внешние устройства любого размера.
Отображать ход проверки	Если флажок установлен, то Kaspersky Security Cloud 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 **Остановить** в окне запуска проверки.

Настройки фоновой проверки

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

Если компьютер работает от аккумулятора, Kaspersky Security Cloud не выполняет фоновую проверку компьютера.

Настройки поиска уязвимостей

Настройка	Описание
Изменить область проверки	По ссылке открывается окно **Область поиска уязвимостей** со списком объектов, которые проверяет Kaspersky Security Cloud при поиске уязвимостей.

	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 проверки	**Вручную**. Режим запуска, при котором вы запускаете поиск уязвимостей вручную в удобное для вас время. **По расписанию**. Режим запуска задачи проверки, при котором Kaspersky Security Cloud выполняет задачу проверки по сформированному вами расписанию. Если выбран этот режим запуска задачи проверки, вы также можете запускать задачу проверки вручную.

Настройки учетной записи

Развернуть всё | Свернуть всё

Запуск от имени

Выбор учетной записи, с правами которой Kaspersky Security Cloud будет запускать задачи проверки. Функция доступна для запуска проверки Kaspersky Security Cloud как вручную, так и по расписанию.

Возможны следующие варианты выбора:

- **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

Развернуть всё | Свернуть всё

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 компьютерных программ. По умолчанию Анти-Баннер блокирует на сайтах баннеры из списка известных баннеров. Список входит в состав баз Kaspersky Security Cloud.

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

Развернуть всё | Свернуть всё

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

Развернуть всё | Свернуть всё

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

Развернуть всё | Свернуть всё

Кнопка

При нажатии на кнопку открывается меню со следующими пунктами:

- **Импортировать и добавить к существующему**. При выборе этого пункта открывается окно, позволяющее загрузить список запрещенных адресов из файла формата CSV. Текущие адреса не будут удалены.
- **Импортировать и заменить существующий**. При выборе этого пункта открывается окно, позволяющее загрузить список запрещенных адресов из файла формата CSV. Текущие адреса будут удалены.
- **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

Развернуть всё | Свернуть всё

Кнопка

При нажатии на кнопку открывается меню со следующими пунктами:

- **Импортировать и добавить к существующему**. При выборе этого пункта можно загрузить список разрешенных адресов из файла формата CSV. Текущие адреса не удаляются.

- **Импортировать и заменить существующий**. 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

Развернуть всё | Свернуть всё

Кнопка

При нажатии на кнопку открывается меню со следующими пунктами:

- **Импортировать и добавить к существующему**. При выборе этого пункта можно загрузить список разрешенных адресов из файла формата CSV. Текущие адреса не удаляются.
- **Импортировать и заменить существующий**. 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". В программе список обновляется автоматически при обновлении баз и программных модулей.

Настройки Анти-Спама

Развернуть всё | Свернуть всё

Включить / выключить Анти-Спам

Переключатель включает / выключает Анти-Спам.

Если переключатель включен, Анти-Спам обнаруживает нежелательную почту (спам) и обрабатывает ее в соответствии с правилами вашего почтового клиента.

Уровень безопасности

В блоке **Уровень безопасности** вы можете выбрать один из предустановленных наборов настроек Анти-Спама (уровней безопасности). Решение о том, какой уровень безопасности выбрать, вы принимаете в зависимости от условий работы и сложившейся ситуации.

Доступны следующие уровни безопасности:

- **Высокий**. Уровень безопасности, при котором Анти-Спам использует максимальный уровень фильтрации спама.

Высокий уровень безопасности рекомендуется устанавливать при работе в опасной среде (например, при использовании бесплатного почтового сервиса).

При установке высокого уровня безопасности может возрасти частота распознавания полезной почты как спама.

- **Рекомендуемый**. Уровень безопасности, при котором обеспечивается оптимальный баланс между производительностью и безопасностью. Он подходит для большинства случаев.

- **Низкий**. Уровень безопасности, при котором Анти-Спам использует минимальный уровень фильтрации спама.

Низкий уровень безопасности рекомендуется устанавливать при работе в безопасной среде (например, при использовании защищенной корпоративной почты).

При установке низкого уровня безопасности может снизиться частота распознавания обычной почты как спама и возможного спама.

Восстановить рекомендуемый уровень безопасности

По ссылке Kaspersky Security Cloud устанавливает уровень безопасности **Рекомендуемый**. Ссылка отображается, если вы изменили настройки в окне **Дополнительные настройки Анти-Спама** в блоке **Считать спамом следующие сообщения**.

Расширенная настройка

По ссылке открывается окно дополнительных настроек Анти-Спама.

Дополнительные настройки Анти-Спама

Развернуть всё | Свернуть всё

В блоке **Считать спамом следующие сообщения** вы можете задать условия фильтрации сообщений, в соответствии с которыми Анти-Спам признает сообщение спамом.

С элементами фишинга

Флажок включает / выключает проверку почтовых сообщений на наличие элементов фишинга в тексте или ссылок, присутствующих в списке фишинговых веб-адресов.

Если флажок установлен, Анти-Спам считает спамом сообщение, в котором есть ссылка из списка фишинговых веб-адресов.

Если флажок снят, Анти-Спам не проверяет ссылки из сообщения по списку фишинговых веб-адресов.

Со ссылками из базы вредоносных веб-адресов

Флажок включает / выключает проверку ссылок, содержащихся в почтовых сообщениях, на принадлежность к списку вредоносных веб-адресов.

От запрещенных отправителей

Флажок включает / выключает фильтрацию сообщений по списку запрещенных отправителей, сообщения от которых Анти-Спам считает спамом.

Выбрать

По ссылке открывается окно **Запрещенные отправители**, в котором вы можете сформировать список запрещенных отправителей.

При создании списка вы можете задавать как адреса, так и маски адресов запрещенных отправителей.

Ссылка доступна, если установлен флажок **От запрещенных отправителей**.

С запрещенными фразами

Флажок включает / выключает фильтрацию сообщений по списку запрещенных фраз, наличие которых в сообщении указывает на то, что письмо является спамом.

Выбрать

По ссылке открывается окно **Запрещенные фразы**, в котором вы можете сформировать список запрещенных фраз.

При создании списка вы можете задавать как отдельные фразы, так и маски запрещенных фраз.

Ссылка доступна, если установлен флажок **С запрещенными фразами**.

С нецензурными словами

Ссылка, по которой открывается окно **Нецензурные слова**. В окне вы можете сформировать список нецензурных слов. Наличие этих слов в сообщении свидетельствует о том, что письмо является спамом.

Ссылка доступна, если установлен флажок **С нецензурными словами**.

В блоке **Считать полезными следующие сообщения** вы можете задать признаки, при наличии которых Анти-Спам считает сообщение полезным.

От разрешенных отправителей

Флажок включает / выключает проверку адреса отправителя по списку разрешенных отправителей.

Если флажок установлен, Анти-Спам считает полезными письма от разрешенных отправителей.

Если флажок снят, Анти-Спам не считает полезными письма от разрешенных отправителей. Фильтрация сообщений по списку разрешенных отправителей не производится.

Выбрать

По ссылке открывается окно **Разрешенные отправители**, в котором вы можете сформировать список разрешенных отправителей.

При создании списка вы можете задавать как адреса, так и маски адресов разрешенных отправителей.

Ссылка доступна, если установлен флажок **От разрешенных отправителей**.

С разрешенными фразами

Флажок включает / выключает проверку сообщения по списку разрешенных фраз.

Если флажок установлен, Анти-Спам считает полезным сообщение, в котором есть фразы из этого списка.

Если флажок снят, Анти-Спам не фильтрует сообщения по списку разрешенных фраз и не считает полезными сообщения, в которых есть фразы из этого списка.

Выбрать

По ссылке открывается окно **Разрешенные фразы**, в котором вы можете сформировать список разрешенных фраз.

При создании списка вы можете задавать как отдельные фразы, так и маски разрешенных фраз.

Ссылка доступна, если установлен флажок **С разрешенными фразами**.

В блоке **Действия с сообщениями** вы можете указать, какие метки должны добавляться к теме сообщения, которому Анти-Спам присвоил статус *Спам* или *Возможный спам*.

Добавлять метку [!! SPAM] к теме сообщения, признанного спамом

Автоматическое добавление текстовой метки в тему сообщений, которым Анти-Спам присвоил статус *Спам*.

Текст метки указывается в поле напротив флажка. По умолчанию Анти-Спам добавляет метку **[!! SPAM]**.

Добавлять метку [?? Probable SPAM] к теме сообщения, признанного возможным спамом

Автоматическое добавление текстовой метки в тему сообщений, которым Анти-Спам присвоил статус *Возможный спам*.

Текст метки указывается в поле напротив флажка. По умолчанию Анти-Спам добавляет метку **[?? Probable Spam]**.

Окно Добавление / изменение запрещенной фразы

Развернуть всё | Свернуть всё

Маска фразы

Фраза или маска фразы, наличие которой в сообщении является признаком спама.

Весовой коэффициент фразы

Числовое значение, выражающее вероятность того, что письмо, содержащее запрещенную фразу, является спамом. Чем выше весовой коэффициент, тем выше вероятность того, что письмо, в котором содержится запрещенная фраза, является спамом.

Анти-Спам определяет письмо как спам, если сумма весовых коэффициентов запрещенных фраз в письме превышает установленное значение.

Статус

В блоке **Статус** вы можете указать, должен ли Анти-Спам проверять сообщения на наличие запрещенной фразы:

- **Активно**. Анти-Спам проверяет сообщения на наличие запрещенной фразы.
- **Неактивно**. Анти-Спам не проверяет сообщения на наличие запрещенной фразы.

Окно Запрещенные отправители

Развернуть всё | Свернуть всё

Кнопка

При нажатии на кнопку открывается меню, в котором можно выбрать действие:

- **Импортировать и добавить к существующему**. При выборе этого действия можно загрузить список запрещенных отправителей из файла формата CSV. Текущий список отправителей не удаляется.
- **Импортировать и заменить существующий**. При выборе этого действия можно загрузить список запрещенных отправителей из файла формата CSV. Текущий список отправителей удаляется.
- **Экспортировать**. При выборе этого действия можно сохранить список запрещенных отправителей в файле формата CSV.

Список Запрещенные отправители

Содержит список адресов, сообщения с которых Анти-Спам считает спамом.

Вы можете добавить в список адрес или маску адреса.

Если в графе **Статус** в строке адреса установлено значение *Активно*, Анти-Спам считает адрес запрещенным.

Если в графе **Статус** в строке адреса установлено значение *Неактивно*, Анти-Спам исключает выбранный адрес из списка.

Адрес отправителя

Графа, в которой указывается адрес или маска адреса электронной почты запрещенного отправителя.

Статус

Графа, в которой указано, считает ли Анти-Спам сообщения, присылаемые с этого адреса, спамом.

Если в строке адреса установлено значение *Активно*, Анти-Спам считает сообщения с этого адреса спамом.

Если в строке адреса установлено значение *Неактивно*, Анти-Спам исключает выбранный адрес из списка.

Изменить

При нажатии на кнопку открывается окно для изменения выбранного в списке адреса или маски адреса.

Удалить

При нажатии на кнопку Анти-Спам удаляет из списка выбранный адрес или маску адреса.

Добавить

При нажатии на кнопку открывается окно добавления в список адреса или маски адреса.

Окно Запрещенные фразы

Развернуть всё | Свернуть всё

Кнопка

При нажатии на кнопку открывается меню, в котором можно выбрать действие:

- **Импортировать и добавить к существующему**. При выборе этого действия можно загрузить список запрещенных фраз из файла формата CSV. Текущие фразы не удаляются.
- **Импортировать и заменить существующий**. При выборе этого действия можно загрузить список запрещенных фраз из файла формата CSV. Текущие фразы удаляются.
- **Экспортировать**. При выборе этого действия можно сохранить список запрещенных фраз в файле формата CSV.

Список запрещенных фраз

Содержит ключевые фразы, которые указывают на то, что содержащее их письмо является спамом.

Вы можете добавить в список фразу или маску фразы.

Если в графе **Статус** в строке фразы установлено значение *Активно*, Анти-Спам использует фразу при фильтрации сообщений.

Если в графе **Статус** в строке фразы установлено значение *Неактивно*, Анти-Спам исключает фразу из списка и не использует ее при фильтрации сообщений.

Изменить

При нажатии на кнопку открывается окно, в котором можно изменить выбранную в списке фразу или маску фразы.

Удалить

При нажатии на кнопку Анти-Спам удаляет из списка выбранную фразу или маску фразы.

Добавить

При нажатии на кнопку открывается окно, в котором можно добавить в список фразу или маску фразы.

Окно Добавление / изменение адреса электронной почты

Развернуть всё | Свернуть всё

Маска адреса электронной почты

В окне вы можете указать адрес или маску адреса электронной почты.

При вводе маски вы можете использовать символы `*` и `?` (где `*` – любая последовательность символов, а `?` – любой один символ).

Статус

В блоке **Статус** вы можете указать, должен ли Анти-Спам блокировать сообщения, отправленные с этого адреса, при проверке сообщений по списку разрешенных / запрещенных отправителей:

- **Активно**. Анти-Спам блокирует сообщения, отправленные с этого адреса.
- **Неактивно**. Анти-Спам не блокирует сообщения, отправленные с этого адреса.

Окно Добавление / изменение разрешенной фразы

Развернуть всё | Свернуть всё

Маска фразы

Фраза или маска фразы, наличие которой в сообщении свидетельствует о том, что письмо не является спамом.

Весовой коэффициент фразы

Числовое значение, выражающее вероятность того, что письмо, содержащее разрешенную фразу, не является спамом. Чем выше весовой коэффициент, тем выше вероятность того, что письмо, в котором содержится разрешенная фраза, не является спамом.

Анти-Спам не определяет письмо как спам, если сумма весовых коэффициентов разрешенных фраз в письме превышает установленное значение.

Статус

В блоке **Статус** вы можете указать, должен ли Анти-Спам проверять сообщения на наличие разрешенной фразы:

- **Активно**. Анти-Спам проверяет сообщения на наличие разрешенной фразы.
- **Неактивно**. Анти-Спам не проверяет сообщения на наличие разрешенной фразы.

Окно Разрешенные отправители

Развернуть всё | Свернуть всё

Кнопка

При нажатии на кнопку открывается меню, в котором можно выбрать действие:

- **Импортировать и добавить к существующему**. При выборе этого действия можно загрузить список разрешенных отправителей из файла формата CSV. Текущий список отправителей не удаляется.
- **Импортировать и заменить существующий**. При выборе этого действия можно загрузить список разрешенных отправителей из файла формата CSV. Текущий список отправителей удаляется.

- **Экспортировать**. При выборе этого действия можно сохранить список разрешенных отправителей в файле формата CSV.

Список Разрешенные отправители

Содержит список адресов отправителей, сообщения от которых Анти-Спам считает полезными.

Вы можете добавить в список адрес или маску адреса.

Если в графе **Статус** в строке адреса установлено значение *Активно*, Анти-Спам считает письмо от этого отправителя полезным.

Если в графе **Статус** в строке адреса установлено значение *Неактивно*, Анти-Спам не считает все письма от этого отправителя полезными и проверяет эти письма на основе стандартных методов проверки.

Адрес отправителя

Графа, в которой указывается адрес или маска адреса электронной почты разрешенного отправителя.

Статус

Графа, в которой указано, считает ли Анти-Спам сообщения, присылаемые с этого адреса, полезными.

Если в строке адреса установлено значение *Активно*, Анти-Спам считает сообщения с этого адреса полезными.

Если в строке адреса установлено значение *Неактивно*, Анти-Спам исключает выбранный адрес из списка.

Изменить

Кнопка, по которой открывается окно, в котором вы можете изменить адрес или маску адреса в списке разрешенных отправителей.

Удалить

Кнопка, по которой Анти-Спам удаляет из списка выбранный адрес или маску адреса.

Добавить

При нажатии на кнопку открывается окно, в котором вы можете добавить адрес или маску адреса в список разрешенных отправителей.

Добавлять получателей моих писем в разрешенные отправители

Если флажок установлен, программа добавляет получателей ваших писем в список разрешенных отправителей.

Окно Разрешенные фразы

Развернуть всё | Свернуть всё

Кнопка

При нажатии на кнопку открывается меню, в котором можно выбрать действие:

- **Импортировать и добавить к существующему**. При выборе этого действия можно загрузить список разрешенных фраз из файла формата CSV. Текущие фразы не удаляются.
- **Импортировать и заменить существующий**. При выборе этого действия можно загрузить список разрешенных фраз из файла формата CSV. Текущие фразы удаляются.
- **Экспортировать**. При выборе этого действия можно сохранить список разрешенных фраз в файле формата CSV.

Список разрешенных фраз

Содержит ключевые фразы, наличие которых в сообщении считается признаком полезного письма.

Вы можете добавить в список фразу или маску фразы.

Если в графе **Статус** в строке фразы установлено значение *Активно*, Анти-Спам использует фразу при фильтрации сообщений.

Если в графе **Статус** в строке фразы установлено значение *Неактивно*, Анти-Спам не использует фразу при фильтрации сообщений.

Изменить

Кнопка, при нажатии на которую открывается окно, в котором вы можете изменить выбранную в списке фразу или маску фразы.

Удалить

При нажатии на кнопку Анти-Спам удаляет из списка выбранную фразу или маску фразы.

Добавить

При нажатии на кнопку открывается окно, в котором вы можете добавить в список фразу или маску фразы.

Настройки Безопасных платежей

Развернуть всё | Свернуть всё

Включить / выключить Безопасные платежи

Переключатель включает / выключает Безопасные платежи.

Если переключатель включен, Kaspersky Security Cloud 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 Kaspersky Security Cloud запрашивает подтверждение пользователя на запуск Защищенного браузера.

Если переключатель выключен, Kaspersky Security Cloud 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 Kaspersky Security Cloud совершает при первом обращении к сайтам банков и платежных систем.

Запускать Защищенный браузер

Если Kaspersky Security Cloud обнаруживает попытку доступа к указанному сайту, то открывает этот сайт в Защищенном браузере. В обычном браузере, использованном для обращения к сайту, отображается сообщение о запуске Защищенного браузера.

Спрашивать пользователя

Если Kaspersky Security Cloud обнаруживает попытку доступа к указанному сайту, то предлагает запустить Защищенный браузер либо открыть сайт при помощи обычного браузера.

Не запускать Защищенный браузер

Когда вы обращаетесь к указанному сайту, Kaspersky Security Cloud не использует Защищенный браузер. Сайт открывается в обычном браузере.

Блок **Дополнительно** позволяет настроить дополнительные настройки работы Безопасных платежей.

Для перехода к сайтам из окна Безопасных платежей использовать <браузер>

В раскрывающемся списке можно выбрать браузер, в котором Kaspersky Security Cloud будет открывать сайты банков или платежных систем, выбранные из окна Безопасные платежи.

Безопасные платежи доступны при работе с браузерами Microsoft Internet Explorer, Microsoft Edge на базе Chromium, Mozilla Firefox, Google Chrome и Яндекс.Браузер.

По умолчанию Безопасные платежи используют браузер, установленный в операционной системе в качестве браузера по умолчанию.

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 браузер.

В 64-разрядной версии Windows 8, Windows 8.1 и Windows 10 для защиты браузера используется аппаратная виртуализация.

Настройки Веб-Антивируса

Настройка	Описание

Уровень безопасности	Для работы Веб-Антивируса Kaspersky Security Cloud применяет разные наборы настроек. Наборы настроек, сохраненные в программе, называются *уровнями безопасности*. • **Высокий**. Уровень безопасности веб-трафика, при котором компонент Веб-Антивирус максимально проверяет веб-трафик, поступающий на компьютер по HTTP- и FTP-протоколам. Веб-Антивирус детально проверяет все объекты веб-трафика, используя полный набор баз программы, а также выполняет максимально глубокий эвристический анализ. • **Рекомендуемый**. Уровень безопасности веб-трафика, обеспечивающий оптимальный баланс между производительностью Kaspersky Security Cloud и безопасностью веб-трафика. Компонент Веб-Антивирус выполняет эвристический анализ на уровне **Средний**. 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 Веб-Антивирус выполняет эвристический анализ на уровне **Поверхностный**.
Действие при обнаружении угрозы	• **Спрашивать пользователя.** Веб- Антивирус информирует вас об обнаружении зараженного или возможно зараженного объекта и запрашивает дальнейшее действие над ним. Этот вариант доступен, если в разделе **Настройки** → **Общие** снят флажок **Автоматически выполнять рекомендуемые действия**. • **Выбирать действие автоматически.** Веб-Антивирус выбирает действие автоматически на основе установленных настроек. Если веб-ресурс находится в списке исключений или не содержит зараженных или возможно зараженных объектов, то Веб-Антивирус разрешает доступ к нему. Если в результате проверки Веб-Антивирус обнаруживает, что веб-ресурс

содержит зараженный или возможно зараженный объект, он блокирует доступ к веб-ресурсу.

Этот вариант доступен, если в разделе **Настройки** → **Общие** установлен флажок **Автоматически выполнять рекомендуемые действия**.

- **Запрещать загрузку**. Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта компонент Веб-Антивирус блокирует доступ к объекту и показывает сообщение в браузере.

- **Информировать**. Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта, Kaspersky Security Cloud разрешает загрузку этого объекта на компьютер и добавляет информацию о зараженном объекте в список обнаруженных объектов.

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 программы и пополняется при обновлении баз Kaspersky Security Cloud.
Проверять веб-адрес по базе веб-адресов, на которых находятся рекламные программы	Примером такой программы может быть программа, которая 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 программы, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или вашим данным	Примером программы из этой категории может быть программа удаленного администрирования, которую легально используют системные администраторы для диагностики и устранения неполадок. Злоумышленник может без вашего ведома установить такую программу на ваш компьютер, получить к нему доступ и использовать в своих целях.

Использовать эвристический анализ	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз программ "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 программ, 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.
Проверять веб-адрес по базе фишинговых веб-адресов	В состав базы фишинговых веб-адресов включены веб-адреса известных на настоящее время веб-сайтов, которые используются для фишинг-атак. Базу фишинговых веб-адресов специалисты "Лаборатории Касперского" пополняют веб-адресами, предоставленными международной организацией по борьбе с фишингом The Anti-Phishing Working Group. База фишинговых веб-адресов входит в комплект поставки программы и пополняется при обновлении баз Kaspersky Security Cloud.
Анти-Фишинг **Использовать эвристический анализ**	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз программ "Лаборатории Касперского". Позволяет обнаружить фишинг, даже если веб-адрес отсутствует в базе фишинговых веб-адресов.
Проверять ссылки	Компонент Проверка ссылок проверяет ссылки на веб-странице, открытой в браузере Microsoft Edge на базе Chromium, Google Chrome или Mozilla Firefox. Рядом с проверенной ссылкой Kaspersky Security Cloud 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, 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 Kaspersky Security Cloud 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 Security Cloud 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**. Kaspersky Security Cloud проверяет ссылки на всех типах веб-страниц. • **Только ссылки в результатах поиска**. Kaspersky Security Cloud проверяет ссылки на веб-страницах с результатами поиска при использовании поисковых систем.
Категории сайтов	Если установлен флажок **Отображать информацию о категориях содержимого сайтов**, Kaspersky Security Cloud добавляет в комментарий к ссылке сведения о том, не принадлежит ли сайт к одной из указанных категорий (например, **Насилие** 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 Веб-Антивирус 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 **с 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". В программе список обновляется автоматически при обновлении баз и программных модулей.

Настройки Защиты от сетевых атак

Компонент Защита от сетевых атак (англ. IDS – Intrusion Detection System) отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на компьютер пользователя, Kaspersky Security Cloud блокирует сетевое соединение с атакующим компьютером.

Описания известных в настоящее время видов сетевых атак и методов борьбы с ними содержатся в базах Kaspersky Security Cloud. Список сетевых атак, которые обнаруживает компонент Защита от сетевых атак, пополняется в процессе обновления баз и модулей программы.

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.
Добавить атакующий компьютер в список блокирования на N минут	Если переключатель включен, 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.
Настроить исключения	Список содержит IP-адреса, сетевые атаки с которых компонент Защита от сетевых атак не блокирует. Kaspersky Security Cloud не заносит в отчет информацию о сетевых атаках с IP-адресов, входящих в список исключений.

Настройки Контроля программ

Развернуть всё | Свернуть всё

Включить / выключить Контроль программ

Переключатель включает / выключает Контроль программ.

Узнать больше

По ссылке открывается окно браузера на странице с более подробной информацией о компоненте.

Доверять программам, имеющим цифровую подпись

Если флажок установлен, Контроль программ считает доверенными программы, имеющие цифровую подпись. Контроль программ помещает такие программы в группу **Доверенные** и не проверяет их активность.

Если флажок снят, Контроль программ не считает программы с обычной цифровой подписью доверенными и проверяет их активность. Программы доверенных поставщиков программного обеспечения (например, Microsoft) Контроль программ считает доверенными независимо от того, установлен флажок или снят.

Загружать правила для программ из Kaspersky Security Network (KSN)

Если флажок установлен, для определения группы доверия программы Контроль программ отправляет запрос в базу Kaspersky Security Network.

Если флажок снят, Контроль программ не ищет информацию в базе Kaspersky Security Network для определения группы доверия, к которой относится программа.

Группа доверия для программ, которые не удалось распределить по другим группам

По ссылке открывается окно **Группа доверия для программ, которые не удалось распределить по другим группам**. В окне можно выбрать группу доверия, в которую будут помещаться неизвестные программы.

Можно выбрать один из следующих вариантов:

- Доверенные;
- Слабые ограничения;

- Сильные ограничения;
- Недоверенные.

Изменить группу доверия для программ, запущенных до начала работы Kaspersky Security Cloud

По ссылке открывается окно **Группа доверия для программ, запущенных до начала работы Kaspersky Security Cloud**. В окне можно изменить группу доверия для программ, запущенных до начала работы Kaspersky Security Cloud. Сетевая активность программ, запущенных до начала работы Kaspersky Security Cloud, будет контролироваться в соответствии с правилами выбранной вами группы доверия.

По умолчанию программы, запущенные до начала работы Kaspersky Security Cloud, помещаются в одну из групп доверия на основании правил, заданных специалистами "Лаборатории Касперского".

Управление программами

По ссылке открывается окно **Управление программами**. В нем вы можете отредактировать список правил для программ.

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 Контроль программ.

Окно Веб-маяки

В окне представлен список веб-маяков.

Список составляют и обновляют специалисты "Лаборатории Касперского". В программе список обновляется автоматически при обновлении баз и программных модулей.

Защита от сбора данных. Категории и исключения

Развернуть всё | Свернуть всё

Сервисы веб-аналитики

Если флажок установлен, компонент Защита от сбора данных 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 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 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 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 программа должна 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". В программе список обновляется автоматически при обновлении баз и программных модулей.

Окно Настройки Защиты от сбора данных

Развернуть всё | Свернуть всё

Включить / выключить Защиту от сбора данных

Если переключатель включен, то, когда вы находитесь в интернете, компонент Защита от сбора данных 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 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 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, Kaspersky Security Cloud 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, Kaspersky Security Cloud 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". В программе список обновляется автоматически при обновлении баз и программных модулей.

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". В программе список обновляется автоматически при обновлении баз и программных модулей.

Настройки Почтового Антивируса

Настройка	Описание
Уровень безопасности	Для работы Почтового Антивируса Kaspersky Security Cloud применяет разные наборы параметров. Наборы параметров, сохраненные в программе, называются *уровнями безопасности*. • **Высокий**. 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. Уровень безопасности почты **Высокий** 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. • **Рекомендуемый**. Уровень безопасности почты, обеспечивающий оптимальный баланс между производительностью Kaspersky Security Cloud 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 поверхностный эвристический анализ и 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. Уровень безопасности почты **Низкий** 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 **Настройки** → **Общие** 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 **Настройки** → **Общие** установлен флажок **Автоматически выполнять рекомендуемые действия**. • **Лечить; удалять, если лечение невозможно**. При обнаружении зараженного объекта во входящем или исходящем сообщении Kaspersky Security Cloud пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, Kaspersky Security Cloud удаляет зараженный объект. Kaspersky Security Cloud добавит информацию о выполненном действии в тему сообщения: `[Зараженный объект удален] <тема сообщения>`. • **Лечить; блокировать, если лечение невозможно**. При обнаружении зараженного объекта во входящем сообщении Kaspersky Security Cloud пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, Kaspersky Security Cloud добавит предупреждение к теме сообщения: `[Сообщение заражено] <тема сообщения>`. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении

Kaspersky Security Cloud пытается вылечить обнаруженный объект. Если вылечить объект не удалось, Kaspersky Security Cloud блокирует отправку сообщения, почтовый клиент показывает ошибку.

- **Блокировать**. При обнаружении зараженного объекта во входящем сообщении Kaspersky Security Cloud добавит предупреждение к теме сообщения: `[Сообщение заражено] <тема сообщения>`. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении Kaspersky Security Cloud 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.
Подключить расширение для Microsoft Outlook	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.
Эвристический анализ	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз программ "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.
Проверять вложенные архивы	Проверка архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.
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. **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)

Развернуть всё | Свернуть всё

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

Развернуть всё | Свернуть всё

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 программ (в том числе программ-вымогателей) и восстановить состояние операционной системы до появления в ней программы (отменить последствия вредоносной или другой активности программы). В некоторых случаях отменить последствия действий программ невозможно, например, если программа была обнаружена компонентом Контроль программ.

Мониторинг активности собирает данные из разных источников, в том числе и от других компонентов Kaspersky Security Cloud. Мониторинг активности анализирует активность программ и предоставляет собранную информацию о событиях другим компонентам Kaspersky Security Cloud.

В блоке **Защита от эксплойтов** вы можете настроить действия программы при запуске исполняемых файлов из уязвимых программ.

Контролировать попытки выполнить несанкционированные операции

Флажок включает / выключает функцию защиты от эксплойтов.

Если флажок установлен, Kaspersky Security Cloud отслеживает исполняемые файлы, запускаемые уязвимыми программами. Если Kaspersky Security Cloud обнаруживает, что попытка запустить исполняемый файл из уязвимой программы 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 программ.

Список содержит следующие варианты действий:

- **Спрашивать пользователя**. Мониторинг активности запрашивает действие у пользователя. Этот вариант доступен, если в разделе **Настройки** → **Общие** снят флажок **Автоматически выполнять рекомендуемые действия**.
- **Выбирать действие автоматически**. Мониторинг активности автоматически выполняет действие, указанное в настройках программы и добавляет информацию о выбранном действии в отчет. Этот вариант доступен, если в разделе **Настройки** → **Общие** 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 программы

В раскрывающемся списке можно выбрать действие, которое должен выполнять Мониторинг активности, если в результате анализа активности была замечена вредоносная или другая активность программы.

- **Спрашивать пользователя**. Мониторинг активности запрашивает действие у пользователя. Этот вариант доступен, если в разделе **Настройки** → **Общие** снят флажок **Автоматически выполнять рекомендуемые действия**.
- **Выбирать действие автоматически**. Мониторинг активности автоматически выполняет над программой действие, рекомендуемое специалистами "Лаборатории Касперского". Этот вариант доступен, если в разделе **Настройки** → **Общие** установлен флажок **Автоматически выполнять рекомендуемые действия**.
- **Выбирать действие автоматически**. Мониторинг активности автоматически выполняет над программой действие, рекомендуемое специалистами "Лаборатории Касперского".
- **Удалять программу**. Мониторинг активности удаляет программу.
- **Завершать работу программы**. Мониторинг активности завершает все процессы программы.
- **Пропускать**. Мониторинг активности не предпринимает никаких действий с программой.

При возможности отменить последствия вредоносной или другой активности программы

В раскрывающемся списке можно выбрать действие, которое Мониторинг активности должен выполнять при наличии возможности отменить последствия вредоносной или другой активности программы.

- **Запрашивать действие.** 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 **Настройки** → **Общие** снят флажок **Автоматически выполнять рекомендуемые действия**.

- **Выбирать действие автоматически**. Если по результатам анализа активности программы Мониторинг активности признает ее вредоносной, то он выполняет отмену последствий активности программы и уведомляет об этом пользователя. Этот вариант доступен, если в разделе **Настройки** → **Общие** установлен флажок **Автоматически выполнять рекомендуемые действия**.
- **Выполнять откат**. Мониторинг активности выполняет отмену последствий вредоносной или другой активности программы.
- **Не выполнять откат**. Мониторинг активности сохраняет информацию о вредоносной или другой активности программы, но не выполняет отмену действий программы.

В блоке **Защита от программ блокировки экрана** вы можете настроить действия Kaspersky Security Cloud при активизации программ блокировки экрана. Программы блокировки экрана – это вредоносные программы, которые ограничивают возможность работы на компьютере, блокируя экран, клавиатуру, доступ к панели задач и ярлыкам. Программы блокировки экрана могут требовать выкуп за возврат возможности работы с операционной системой. С помощью функции защита от программ блокировки экрана можно завершить работу программы блокировки экрана по нажатию определенной комбинации клавиш.

Распознавать и закрывать программы блокировки экрана

Флажок включает / выключает использование функции защиты от программ блокировки экрана.

Если флажок установлен, при обнаружении действий программы блокировки экрана вы можете остановить ее работу по нажатию комбинации клавиш, указанной в раскрывающемся списке под флажком.

Для закрытия программы блокировки экрана вручную использовать комбинацию клавиш

В раскрывающемся списке можно выбрать клавишу или комбинацию клавиш, при нажатии которой функция защиты от программ блокировки экрана обнаруживает и удаляет программу блокировки экрана.

По умолчанию используется следующая комбинация клавиш: CTRL+ALT+SHIFT+F4.

Настройки Файлового Антивируса

Настройка	Описание
Уровень безопасности	Для работы Файлового Антивируса Kaspersky Security Cloud применяет разные наборы настроек. Наборы настроек, сохраненные в программе, называются *уровнями безопасности*. • **Высокий**. 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. • **Рекомендуемый**. 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 **Настройки** → **Общие** 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 **Настройки → Общие** установлен флажок **Автоматически выполнять рекомендуемые действия**.

- **Лечить; удалять, если лечение невозможно**. Если выбран этот вариант действия, то Kaspersky Security Cloud автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Security Cloud их удаляет.

- **Лечить; блокировать, если лечение невозможно**. Если выбран этот вариант действия, то Kaspersky Security Cloud автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Security Cloud 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 Kaspersky Security Cloud 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, Kaspersky Security Cloud проверяет все файлы без исключения (любых форматов и расширений).

	Файлы, проверяемые по формату. Если выбран этот параметр, Kaspersky Security Cloud 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, Kaspersky Security Cloud 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.
Эвристический анализ	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз программ "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 форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.
Проверять дистрибутивы	Флажок включает / выключает проверку дистрибутивов сторонних программ.

Проверять файлы офисных форматов	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты.
Не распаковывать составные файлы большого размера **Максимальный размер файла**	Если флажок установлен, то Kaspersky Security Cloud не проверяет составные файлы, размеры которых больше заданного значения. Если флажок снят, Kaspersky Security Cloud проверяет составные файлы любого размера. Kaspersky Security Cloud проверяет файлы больших размеров, извлеченные из архивов, независимо от состояния флажка.
Распаковывать составные файлы в фоновом режиме **Минимальный размер файла**	Если флажок установлен, Kaspersky Security Cloud предоставляет доступ к составным файлам, размер которых превышает заданное значение, до проверки этих файлов. При этом Kaspersky Security Cloud в фоновом режиме распаковывает и проверяет составные файлы. Kaspersky Security Cloud предоставляет доступ к составным файлам, размер которых меньше данного значения, только после распаковки и проверки этих файлов. Если флажок снят, Kaspersky Security Cloud 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 Kaspersky Security Cloud 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.
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.
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 Kaspersky Security Cloud, 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 программе структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).
Исключения	Объекты, исключаемые из проверки. Указываются по ссылке **Настроить исключения**, в окне **Исключения**.
Приостановка работы Файлового Антивируса	Временная автоматическая приостановка работы Файлового Антивируса в указанное время или во время работы с указанными программами. Настраивается по ссылке **Приостановить работу Файлового Антивируса**.

Настройки AMSI-защиты

Настройка	Описание
Проверять архивы	Проверка архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.
Проверять дистрибутивы	Флажок включает / выключает проверку дистрибутивов сторонних программ.
Проверять файлы офисных форматов	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты.

Не распаковывать составные файлы большого размера **Максимальный размер файла**	Если флажок установлен, то Kaspersky Security Cloud не проверяет составные файлы, размеры которых больше заданного значения. Если флажок снят, Kaspersky Security Cloud проверяет составные файлы любого размера. Kaspersky Security Cloud проверяет файлы больших размеров, извлеченные из архивов, независимо от состояния флажка.

Информация о категориях сайтов

Развернуть всё | Свернуть всё

По ссылке вы можете ознакомиться с описанием категорий веб-сайтов .

Окно Управление программами

Развернуть всё | Свернуть всё

Запуск / Ограничения

По ссылкам изменяется способ отображения программ в списке:

- По ссылке **Запуск** список программ в списке распределяются по двум группам: **Запретить запуск** и **Разрешить запуск**.
- По ссылке **Ограничения** программы в списке распределяются по группам доверия. Например, доверенные программы будут располагаться в группе **Доверенные**.

Очистка

По ссылке Kaspersky Security Cloud удаляет из списка несуществующие программы.

Вид

В раскрывающемся списке можно выбрать вид отображения программ и процессов.

- **Развернуть все**. При выборе этого варианта в списке отображаются все программы, установленные на компьютере.
- **Свернуть все**. При выборе этого варианта в списке отображаются группы доверия.

В раскрывающемся списке можно выбрать способ отображения программ и процессов:

- **Показывать как список**. При выборе этого варианта программы / процессы отображаются в виде списка.
- **Показывать как дерево**. При выборе этого варианта программы / процессы отображаются в виде иерархической структуры в соответствии с последовательностью вызова процессов.

В раскрывающемся списке также можно выключить отображение системных программ, программ "Лаборатории Касперского" и несетевых программ:

- **Скрывать системные программы**. При выборе этого элемента в общем списке программ и процессов не отображаются программы, необходимые для работы операционной системы. По умолчанию системные программы скрыты.
- **Скрывать Kaspersky Security Cloud**. При выборе этого элемента в общем списке программ и процессов не отображаются программы "Лаборатории Касперского". По умолчанию программы "Лаборатории Касперского" скрыты.
- **Показывать только сетевые программы**. При выборе этого элемента в общем списке программ и процессов отображаются только сетевые программы. Сетевые программы – это программы, предназначенные для организации совместной работы группы пользователей на разных компьютерах.

Список программ

В списке содержатся программы, установленные на вашем компьютере. Для каждой программы в списке отображается информация о статусе, цифровой подписи, группе доверия, популярности программы среди пользователей KSN и времени последнего запуска.

По двойному щелчку мышью на строке программы или процесса открывается окно **Правила программы**. В окне можно настроить правила для контроля действий программы.

По правой клавише мыши на строке программы открывается контекстное меню. В контекстном меню можно выполнить следующие действия:

- открыть окно **Правила программы**, в котором можно настроить разрешения для действий программы;
- разрешить или запретить запуск программы;
- переместить программу в другую группу доверия;
- установить для программы настройки контроля активности, предусмотренные по умолчанию (сбросить настройки программы);
- удалить программу из списка;
- открыть папку, содержащую исполняемый файл программы.

Программы в списке объединены в группы и подгруппы. По правой клавише мыши на строке группы открывается контекстное меню. В контекстном меню можно выполнить следующие действия:

- открыть окно **Правила группы**, в котором можно настроить разрешения для действий программ из этой группы, используемые по умолчанию;
- создать подгруппу внутри группы; по умолчанию к подгруппе применяются правила, указанные для группы, в которую она входит;
- добавить программу в группу; по умолчанию к программе применяются правила, указанные для группы, в которую она входит;
- установить для группы и всех входящих в нее подгрупп и программ настройки контроля активности, предусмотренные по умолчанию (сбросить настройки группы);

- установить для подгрупп и программ, входящих в группу, настройки контроля активности, предусмотренные по умолчанию, оставив настройки группы без изменений (сбросить настройки подгрупп и программ);
- удалить входящие в группу подгруппы и программы.

Программа

В графе отображается название программы.

Ограничения

В графе отображается группа доверия, в которую помещена программа. Группа доверия определяет правила использования программы на компьютере: запрет или разрешение запуска, доступ программы к файлам и системному реестру, ограничения сетевой активности программы.

Популярность

В графе отображается уровень популярности программы среди участников Kaspersky Security Network (KSN). Уровень популярности соответствует числу участников KSN, использующих программу.

Сеть

В этой графе можно выбрать действие при попытке программы получить доступ к сети.

В таблице ниже приведено описание действий Kaspersky Security Cloud, если программа или группа программ пытается получить доступ к сети.

Описание действий Kaspersky Security Cloud

Действие	Описание
Наследовать	Программа или группа наследует реакцию из вышестоящей группы.
Разрешить	Kaspersky Security Cloud разрешает программам, входящим в выбранную группу, доступ к сети.
Запретить	Kaspersky Security Cloud запрещает программам, входящим в выбранную группу, доступ к сети.
Спрашивать пользователя	Если в разделе **Настройки** → **Общие** установлен флажок **Автоматически выполнять рекомендуемые действия**, Kaspersky Security Cloud автоматически выбирает действие по правилам, созданным специалистами "Лаборатории Касперского". По сноске вы можете прочитать, какое именно действие будет выбрано. Если этот флажок снят, программа спрашивает пользователя, предоставлять этой программе доступ к сети или нет.
Записывать в отчет	Помимо заданной реакции, Kaspersky Security Cloud записывает в отчет информацию о попытке доступа программы к сети.

Запуск

В графе с помощью переключателя можно разрешить или запретить запуск выбранной программы. По умолчанию запуск программы разрешен или запрещен в зависимости от ограничений группы, в которую входит программа.

Устранение следов активности / Отмена изменений

В этом окне отображается процесс устранения следов вашей активности в операционной системе. Устранение может занять некоторое время. Для устранения некоторых следов активности может потребоваться перезагрузка компьютера.

Если на первом шаге был выбран вариант **Отменить внесенные ранее изменения**, мастер устранения следов активности выполняет откат действий, выбранных на предыдущем шаге.

Общие

Настройка	Описание
Автоматически выполнять рекомендуемые действия	Если флажок снят, основные компоненты программы работают в интерактивном режиме. Это значит, что Kaspersky Security Cloud запрашивает ваше решение при выборе действия с обнаруженными объектами и угрозами, если в настройках Файлового Антивируса, Веб-Антивируса, Почтового Антивируса, Мониторинга активности и Контроля программ выбран вариант действия **Спрашивать пользователя**. Если флажок установлен, Kaspersky Security Cloud выбирает действие автоматически на основе правил, заданных специалистами "Лаборатории Касперского".
Удалять вредоносные утилиты, рекламные программы, программы автодозвона и подозрительные упаковщики	Если флажок установлен, Kaspersky Security Cloud удаляет вредоносные утилиты, рекламные программы, программы автодозвона и подозрительные упаковщики в автоматическом режиме защиты. Функция доступна, если установлен флажок **Автоматически выполнять рекомендуемые действия**.
Не запускать задачи по расписанию при работе от аккумулятора	Если флажок установлен, то режим экономии питания аккумулятора включен. Kaspersky Security Cloud откладывает выполнение задач, для которых задан запуск по расписанию. По мере необходимости вы можете самостоятельно запускать задачи проверки и обновления.
Использовать	Если флажок установлен, Kaspersky Security Cloud не запускает задачи проверки и обновления, не отображает

Игровой режим	уведомления, когда вы играете или работаете с программами в полноэкранном режиме. Если флажок установлен, вы также можете установить дополнительный флажок **Использовать режим Не беспокоить**. В этом режиме не показываются уведомления, если вы активно работаете с некоторыми программами, а также не запускаются задачи проверки и обновления.
Откладывать выполнение задач проверки компьютера при высокой нагрузке на центральный процессор и дисковые системы	Когда Kaspersky Security Cloud выполняет задачи по расписанию, может увеличиваться нагрузка на центральный процессор и дисковые подсистемы, что замедляет работу других программ. Если флажок установлен, то при увеличении нагрузки Kaspersky Security Cloud приостанавливает выполнение задач по расписанию и высвобождает ресурсы операционной системы для других программ.
Запускать Kaspersky Security Cloud при включении компьютера (рекомендуется)	Если флажок установлен, то Kaspersky Security Cloud запускается после загрузки операционной системы и защищает компьютер пользователя в течение всего сеанса работы. Если флажок не установлен, то Kaspersky Security Cloud не запускается после загрузки операционной системы до того момента, как пользователь запустит программу вручную. Защита компьютера выключена и данные пользователя могут находиться под угрозой.
Применять технологию лечения активного заражения	Если флажок установлен, при обнаружении вредоносной активности в операционной системе на экране отображается всплывающее уведомление. В уведомлении Kaspersky Security Cloud предлагает провести процедуру лечения активного заражения компьютера. После подтверждения пользователем этой процедуры Kaspersky Security Cloud устраняет угрозу. Завершив процедуру лечения активного заражения, Kaspersky Security Cloud выполняет перезагрузку компьютера. Применение технологии лечения активного заражения требует значительных ресурсов компьютера, что может замедлить работу других программ.
Включить	Если флажок установлен, то Kaspersky Security Cloud предотвращает изменение и удаление файлов

самозащиту	программы на жестком диске, процессов в памяти и записей в системном реестре.
Разрешить управление настройками Kaspersky Security Cloud через программы удаленного управления	Если флажок установлен, доверенные программы удаленного администрирования (такие как TeamViewer, LogMeIn Pro и Remotely Anywhere) могут изменять настройки Kaspersky Security Cloud. Недоверенным программам удаленного администрирования изменение настроек Kaspersky Security Cloud будет запрещено, даже если флажок установлен.
Включить возможность внешнего управления системными службами	Если флажок установлен, то Kaspersky Security Cloud разрешает управление службами программы с удаленного компьютера. При попытке управления службами программы с удаленного компьютера, над значком программы в области уведомлений панели задач Microsoft Windows отображается уведомление (если служба уведомлений не выключена пользователем).
Включить запись дампов	Если флажок установлен, то Kaspersky Security Cloud записывает дампы в случае сбоев в работе. Если флажок снят, то Kaspersky Security Cloud не записывает дампы. Программа 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.

Угрозы и исключения

Настройка	Описание
Типы обнаруживаемых объектов	Kaspersky Security Cloud обнаруживает объекты разных типов, такие как, например, вирусы и черви, троянские программы, рекламные программы. Подробнее о них читайте в Энциклопедии "Касперского". Вы можете выключить обнаружение объектов следующих типов: • Другие программы, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя. К таким программам относятся, например, программы удаленного администрирования, которые используют системные администраторы; чтобы получать доступ к интерфейсу удаленного компьютера для наблюдения и управления. • Многократно упакованные файлы. Файлы, которые упакованы несколько раз, в том числе разными упаковщиками. Многократная упаковка затрудняет проверку объектов.
Настроить исключения	По ссылке открывается окно **Исключения** со списком исключений из проверки. *Исключение из проверки* – это совокупность условий, при выполнении которых Kaspersky Security Cloud не проверяет объект на вирусы и другие программы, 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 (Kaspersky Security Cloud не будет их проверять): • Файл или папка, которые нужно исключить из проверки (в том числе можно исключить исполняемые файлы программ и процессов). Вы можете использовать маски в соответствии со следующими правилами: • 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 папке

`Folder` и вложенных папках. 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*`, Kaspersky Security Cloud 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 программы

По ссылке открывается окно со списком доверенных программ. Kaspersky Security Cloud не контролирует файловую и сетевую активность доверенных программ (в том числе и вредоносную), а также обращения этих программ к системному реестру.

Вы можете добавлять, изменять и удалять доверенные программы из списка.

> Даже если программа включена в список доверенных, Kaspersky Security Cloud продолжает проверить исполняемый файл и процесс этой программы на вирусы и другие угрозы. Если вы хотите, чтобы исполняемый файл и процесс доверенной программы не проверялись, добавьте их в список исключений.

При добавлении или изменении доверенной программы вы можете указать правила, в соответствии с которыми Kaspersky Security Cloud контролирует активность доверенной программы, в окне **Исключения для программы**.

В окне **Исключения для программы** доступны для выбора следующие правила:

- Не проверять открываемые файлы.
- Не контролировать активность программы. Не контролируется любая активность программы в рамках работы Контроля программ.
- Не наследовать ограничения родительского процесса (программы). Если ограничения родительского процесса или программы не наследуются, активность программы контролируется по заданным вами правилам или по правилам группы доверия, в которую входит эта программа.
- Не контролировать активность дочерних программ.
- Не блокировать взаимодействие с интерфейсом Kaspersky Security Cloud. Программе разрешено управлять программой Kaspersky Security Cloud, используя графический интерфейс Kaspersky Security Cloud. Необходимость разрешить программе управлять интерфейсом Kaspersky Security Cloud может возникнуть при использовании программы для удаленного доступа к рабочему столу или программы, обеспечивающей 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**) Kaspersky Security Cloud исключает из проверки весь сетевой трафик программы или трафик, передаваемый по протоколу SSL. Значение настройки не влияет на работу Сетевого экрана: Сетевой экран проверяет трафик программы в соответствии с установленными для него настройками. Исключения влияют на работу Почтового Антивируса, Веб-Антивируса и Анти-Спама. Вы можете уточнить IP-адреса или сетевые порты, на которые должно распространяться ограничение контроля трафика.

	Если в окне **Исключения для программы** изменить статус на **Неактивно**, Kaspersky Security Cloud не относит программу к доверенным. Таким образом можно временно исключить программу из доверенных, не удаляя из списка.
Использовать доверенное системное хранилище сертификатов	Если выбрано одно из доверенных системных хранилище сертификатов, Kaspersky Security Cloud исключает из проверки программы, подписанные доверенной цифровой подписью. Kaspersky Security Cloud автоматически помещает такие программы в группу *Доверенные*. Если выбрано **Не использовать**, то Kaspersky Security Cloud проверяет программы независимо от наличия цифровой подписи. Kaspersky Security Cloud помещает программу в группу доверия в зависимости от уровня опасности, которую эта программа может представлять для компьютера.

Настройки сети

Настройка	Описание
Ограничивать трафик при лимитном подключении	Если флажок установлен, программа ограничивает собственный сетевой трафик в том случае, если подключение к интернету является лимитным. Kaspersky Security Cloud 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, Kaspersky Security Cloud внедряет в трафик скрипт взаимодействия с веб-страницами. Этот скрипт обеспечивает работу таких компонентов как Безопасные платежи, Защита от сбора данных, Анти-Баннер, Проверка ссылок.
Поддерживать работу DNS поверх HTTPS (DoH)	Если флажок установлен, программа 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, Анти-Спам и Веб-Антивирус контролируют все открытые порты вашего компьютера. **Контролировать только выбранные сетевые порты**. Режим контроля портов, при котором Почтовый Антивирус, Анти-Спам и Веб-Антивирус 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 программ нужно контролировать все сетевые порты, используемые этими программами: • **Контролировать все порты для программ из списка, рекомендованного "Лабораторией Касперского"**. Список таких программ задан по умолчанию и входит в комплект поставки Kaspersky Security Cloud. Если установлен этот флажок, Kaspersky Security Cloud контролирует все порты для следующих программ: • Adobe 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 программ**. Указать программы можно в окне **Программы**, которое открывается по ссылке **Выбрать**.
Сетевые порты	Список портов, которые обычно используются для передачи почты и веб-трафика, включен в комплект поставки Kaspersky Security Cloud. По умолчанию Kaspersky Security Cloud 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 Kaspersky Security Cloud контролирует трафик, проходящий через этот порт. Если в графе **Статус** в строке порта установлено значение *Неактивно*, то Kaspersky Security Cloud 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**, Kaspersky Security Cloud использует установленный сертификат "Лаборатории Касперского" для проверки SSL-соединений, если этого требуют компоненты защиты Веб-Антивирус и Проверка ссылок. Если эти компоненты выключены, Kaspersky Security Cloud не проверяет SSL-соединения. После того как Kaspersky Security Cloud проверит SSL-соединение, в сертификатах сайтов может не отображаться название организации, на которую зарегистрирован сайт. Если вы не хотите, чтобы программа проверяла SSL-соединение с сайтом, вы можете добавить сайт в список исключений по ссылке **Настроить исключения**.
В случае возникновения ошибки при проверке защищенного соединения	В раскрывающемся списке вы можете выбрать действие, которое выполняет программа, если на каком-либо сайте возникла ошибка проверки защищенных соединений. • **Игнорировать**. Программа разрывает соединение с сайтом, на котором возникла ошибка проверки. • **Спрашивать**. Программа показывает вам уведомление с предложением добавить адрес сайта в список сайтов, на которых возникли ошибки проверки. Адрес сайта будет проверен по базе вредоносных объектов. • **Добавить домен в исключения**. Программа 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 исключения	По ссылке открывается окно **Исключения** со списком сайтов, которые вы добавили как исключение для компонентов Веб-Антивирус и Проверка ссылок.
Доверенные программы	Список программ, активность которых Kaspersky Security Cloud не проверяет в процессе своей работы. Вы можете выбрать виды активности программы, которые Kaspersky Security Cloud не будет контролировать

	(например, не проверять сетевой трафик). Kaspersky Security Cloud поддерживает переменные среды и символы `*` и `?` для ввода маски.
Блокировать соединения по протоколу SSL 2.0 (рекомендуется)	Если флажок установлен, то Kaspersky Security Cloud блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0. Если флажок снят, то Kaspersky Security Cloud не блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0, и не контролирует сетевой трафик, передаваемый по этим соединениям.
Расшифровывать защищенные соединения 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, Kaspersky Security Cloud расшифровывает и контролирует защищенные соединения с EV-сертификатом. Если флажок снят, Kaspersky Security Cloud не имеет доступа к содержанию HTTPS-трафика. Поэтому программа контролирует HTTPS-трафик только по адресу веб-сайта, например, `https://facebook.com`. Если вы впервые открываете веб-сайт с EV-сертификатом, защищенное соединение будет расшифровано независимо от того, установлен флажок или нет.
Настройка прокси-сервера	Параметры прокси-сервера для доступа пользователей клиентских компьютеров в интернет. Kaspersky Security Cloud использует эти параметры в работе некоторых компонентов защиты, в том числе для обновления баз и модулей программы. Для автоматической настройки прокси-сервера Kaspersky Security Cloud использует протокол WPAD (Web Proxy Auto-Discovery Protocol). В случае если по этому протоколу не удается определить IP-адрес прокси-сервера, Kaspersky Security Cloud использует адрес прокси-сервера, указанный в параметрах браузера Microsoft Internet Explorer.
Проверять	Если флажок установлен, Kaspersky Security Cloud проверяет зашифрованный трафик в браузере Mozilla Firefox и

защищенный трафик в продуктах Mozilla	почтовом клиенте Thunderbird. Доступ к некоторым сайтам по протоколу HTTPS может быть заблокирован. Kaspersky Security Cloud расшифровывает и анализирует зашифрованный трафик с помощью корневого сертификата "Лаборатории Касперского". Вы можете выбрать хранилище сертификатов, в котором будет находиться корневой сертификат "Лаборатории Касперского": • **Использовать хранилище сертификатов Windows**. Это хранилище, в которое корневой сертификат "Лаборатории Касперского" добавляется при установке Kaspersky Security Cloud. • **Использовать хранилище сертификатов Mozilla**. Программы Mozilla Firefox и Thunderbird используют собственное хранилище сертификатов. Если выбрано хранилище сертификатов Mozilla, корневой сертификат "Лаборатории Касперского" нужно добавить в это хранилище вручную через свойства браузера.

Управление настройками программы

Настройка	Описание
Импортировать	Извлечь настройки работы программы из файла формата CFG и применить их.
Экспортировать	Сохранить текущие настройки работы программы в файл формата CFG.
Восстановить	Вы в любое время можете восстановить настройки Kaspersky Security Cloud, рекомендуемые "Лабораторией Касперского". В результате восстановления настроек для всех компонентов защиты будет установлен уровень безопасности **Рекомендуемый**.

Сетевой экран

Настройка	Описание
Уведомлять об уязвимостях	Если флажок установлен, Kaspersky Security Cloud показывает уведомления при обнаружении

при подключении к сети Wi-Fi	уязвимостей сети Wi-Fi. Флажок доступен для изменения, если на компьютере не установлена программа Kaspersky Secure Connection. По ссылке **Выбрать категории** открывается окно **Категории**, в котором вы можете указать типы уязвимостей сетей Wi-Fi. Программа 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 Kaspersky Security Cloud.
Правила программ	По ссылке открывается окно **Сетевые правила программ**. В окне отображается информация, связанная с контролем сетевой активности программ и групп программ. Сетевую активность программ в соответствии с сетевыми правилами программ и групп программ регулирует компонент Контроль программ. Вы можете настроить разрешения на сетевую активность программы или группы программ через меню ячейки в графе **Сеть**. Элементы меню описаны в разделе Правила Контроля программ.

	Выбрав в контекстном меню строки пункт **Подробности и правила,** вы можете перейти к настройке сетевых правил программы или группы программ.

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 программы. Такие правила ограничивают входящую и исходящую сетевую активность по определенным портам выбранного протокола передачи данных.
	
	Сетевые пакетные правила имеют приоритет над сетевыми правилами программ.
	
	При добавлении или изменении пакетного правила вы можете установить следующие настройки:
	• Действие:
	  • **Разрешить**. Kaspersky Security Cloud разрешает сетевое соединение.
	  • **Запретить**. Kaspersky Security Cloud запрещает сетевое соединение.
	  • **По правилам программы**. Kaspersky Security Cloud не обрабатывает поток данных в соответствии с пакетным правилом, а применяет правило для программы (см. **Правила программ** выше).
	• Название.
	• Направление:

- **Входящее**. Kaspersky Security Cloud применяет правило к сетевому соединению, которое открыл удаленный компьютер.

- **Исходящее**. Kaspersky Security Cloud применяет правило к сетевому соединению, которое открыл ваш компьютер.

- **Входящее/Исходящее**. Kaspersky Security Cloud 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)**. Kaspersky Security Cloud применяет правило к пакетам данных, которые принимает ваш компьютер.

- **Исходящее (пакет)**. Kaspersky Security Cloud применяет правило к пакетам данных, которые передает ваш компьютер.

- 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**. Kaspersky Security Cloud 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**. Kaspersky Security Cloud применяет правило к IP-адресам, входящим в заданный диапазон. Вы можете указать IP-адреса в полях **Удаленные адреса** и **Локальные адреса**, которые отображаются ниже, если выбрано **Адреса из списка**. IP-адреса можно добавлять через запятую.

- 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.
- Сетевые адаптеры, через которые передаются сетевые пакеты.
- Использование TTL. Kaspersky Security Cloud контролирует передачу сетевых пакетов, у которых время жизни (TTL, Time to Live) не превышает указанного значения.
- Запись событий в отчет Kaspersky Security Cloud.

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. 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).

Правила программы / Правила группы

Настройка	Описание
Файл	Справочная информация о программе и об исполняемом файле программы. Kaspersky Security Cloud получает

(только в окне **Правила программы**)	информацию о программе как из исполняемого файла программы, 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 Контроля программ.
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 Контроля программ.

Сетевые правила	Правила, в соответствии с которыми Kaspersky Security Cloud регулирует сетевую активность программы или группы программ.
	По умолчанию в списке отображаются предустановленные сетевые правила программ, 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 Контроля программ).
	При добавлении правила или его изменении вы можете установить следующие настройки:
	• Действие:
	  • **Разрешить**. Kaspersky Security Cloud разрешает сетевое соединение.
	  • **Запретить**. Kaspersky Security Cloud запрещает сетевое соединение.
	  • **Спрашивать пользователя**. Kaspersky Security Cloud спрашивает пользователя о разрешении или запрете сетевого соединения, если в разделе **Настройки → Общие** снят флажок **Автоматически выполнять рекомендуемые действия**. Если флажок установлен, действие выбирается автоматически. По сноске в окне программы вы можете прочитать, какое именно действие будет выбрано.

- Название.
- Направление:
  - **Входящее**. Kaspersky Security Cloud применяет правило к сетевому соединению, которое открыл удаленный компьютер.
  - **Исходящее**. Kaspersky Security Cloud применяет правило к сетевому соединению, которое открыл ваш компьютер.
  - **Входящее/Исходящее**. Kaspersky Security Cloud 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**. Kaspersky Security Cloud 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**. Kaspersky Security Cloud 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. Kaspersky Security Cloud контролирует передачу сетевых пакетов, у которых время жизни (TTL, Time to Live) не превышает указанного значения.

- Запись событий в отчет Kaspersky Security Cloud.

Для быстрого добавления правила вы можете выбрать один из готовых шаблонов в раскрывающемся списке в нижней части окна.

Исключения (только в окне **Правила программы**)

Вы можете выбрать правила, в соответствии с которыми Kaspersky Security Cloud исключает программу из проверки:

- Не проверять открываемые файлы.

- Не контролировать активность программы. Не контролируется любая активность программы в рамках работы Контроля программ.

- Не наследовать ограничения родительского процесса (программы). Если ограничения родительского процесса или программы не наследуются, активность программы контролируется по заданным вами правилам или по правилам группы доверия, в которую входит эта программа.

- Не контролировать активность дочерних программ.

- Не блокировать взаимодействие с интерфейсом Kaspersky Security Cloud. Программе разрешено управлять программой Kaspersky Security Cloud, используя графический интерфейс Kaspersky Security Cloud. Необходимость разрешить программе управлять интерфейсом Kaspersky Security Cloud может возникнуть при использовании программы для удаленного доступа к рабочему столу или программы, обеспечивающей 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**) Kaspersky Security Cloud исключает из проверки весь сетевой трафик программы или трафик, передаваемый по протоколу SSL. Значение настройки не влияет на работу Сетевого экрана: Сетевой экран проверяет трафик программы в соответствии с установленными для него настройками. Исключения влияют на работу Почтового Антивируса, Веб-Антивируса и Анти-Спама. Вы можете уточнить IP-адреса или сетевые порты, на которые должно распространяться ограничение контроля трафика.

История (только в окне **Правила программы**)	Справочная информация о действиях с программой, например, о запуске программы или присвоении группы доверия .

Правила Контроля программ

Правило – это набор реакций Контроля программ на действия программы над различными категориями ресурсов операционной системы и персональных данных.

Возможны следующие реакции Контроля программ на действия программы:

- **Наследовать**. Контроль программ применяет правило к активности программы, заданное для того статуса, который Контроль программ присвоил программе.

Эта реакция применяется по умолчанию. По умолчанию Контроль программ наследует права доступа из статуса, который Контроль программ присвоил программе.

Если вы изменили правило для программы, то в этом случае параметры правила для программы будут иметь более высокий приоритет, чем параметры правила для статуса, который присвоен программе.

- **Разрешить**. Контроль программ позволяет программе совершать действие.
- **Запретить**. Контроль программ запрещает программе совершать действие.
- **Спрашивать пользователя**. Контроль программ запрашивает решение пользователя, если в разделе **Настройки** → **Общие** снят флажок **Автоматически выполнять рекомендуемые действия**. Если флажок установлен, действие выбирается автоматически. По сноске в окне программы вы можете прочитать, какое именно действие будет выбрано.
- **Записывать в отчет**. Контроль программ записывает в отчет информацию об активности программы и своей реакции. Добавление информации в отчет может быть использовано в комбинации с любым другим действием Контроля программ.

Дополнительно

Настройка	Описание
Использовать аппаратную виртуализацию, если она доступна	Если флажок установлен, для работы Защищенного браузера используется аппаратная виртуализация (гипервизор). Программа использует технологию гипервизора для дополнительной защиты от сложных вредоносных программ, 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 ввода данных с аппаратной клавиатуры	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). По ссылке **Изменить категории** открывается окно **Категории**. В этом окне вы можете указать, на каких сайтах нужно защищать ввод данных с аппаратной клавиатуры.

По ссылке **Настроить исключения** в окне **Категории** 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 программы-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).

> Чтобы Экранная клавиатура включилась, после установки Kaspersky Security Cloud нужно перезагрузить компьютер.

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.

По ссылке **Изменить категории** открывается окно **Категории**. В этом окне можно указать, на каких сайтах нужно отображать значок быстрого вызова Экранной клавиатуры.

По ссылке **Настроить исключения** в окне **Категории** 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 надежность создаваемого пароля

Если флажок установлен, Kaspersky Security Cloud 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), Kaspersky Security Cloud 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. По ссылке **Удалить сохраненные данные** вы можете удалить все сохраненные ранее пароли.

Окно Выберите файлы для удаления

Развернуть всё | Свернуть всё

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

Развернуть всё | Свернуть всё

Поле для ввода пути к файлу или папке

Поле содержит путь к файлу или папке, которые нужно добавить в сейф. Файл или папку можно выбрать в дереве, расположенном выше поля ввода, или указать вручную.

Окно открывания сейфа

Развернуть всё | Свернуть всё

Пароль для доступа к сейфу

Пароль для доступа к файлам в сейфе.

Открыть в Проводнике

При нажатии на кнопку в Проводнике открывается папка со списком файлов и папок, хранящихся в сейфе.

Окно удаления сейфа

Развернуть всё | Свернуть всё

Пароль для доступа к сейфу

Пароль для доступа к файлам в сейфе.

Удалить сейф

При нажатии на кнопку Kaspersky Security Cloud удаляет сейф и все файлы в нем.

Файлы и папки, находящиеся в сейфе, удаляются без возможности восстановления.

Окно переименования сейфа

Развернуть всё | Свернуть всё

Новое название сейфа

Новое название, которое будет присвоено сейфу.

Сохранить

При нажатии на кнопку Kaspersky Security Cloud присваивает сейфу новое название.

Окно изменения пароля от сейфа

Развернуть всё | Свернуть всё

Старый пароль

Текущий пароль от сейфа.

Новый пароль

Новый пароль от сейфа.

Подтверждение пароля

Повторный ввод пароля, введенного в поле **Новый пароль**.

Сохранить

При нажатии на кнопку текущий пароль от сейфа заменяется новым.

Окно Выбор файла сейфа

Развернуть всё | Свернуть всё

Поле для ввода пути к файлу

Поле содержит путь к файлу сейфа. Файл можно выбрать в дереве, расположенном выше поля ввода, или указать путь к файлу вручную.

Окно Резервное копирование

Развернуть всё | Свернуть всё

Выбрать файлы для резервного копирования

При нажатии на кнопку запускается мастер создания задачи резервного копирования.

Восстановить файлы из моего набора резервных копий

По ссылке открывается окно со списком хранилищ резервных копий. В окне вы можете выбрать хранилище, в котором находится ранее созданный вами набор резервных копий.

Кнопки  /  / 

С помощью кнопок вы можете управлять процессом резервного копирования:

 – прервать резервное копирование. Кнопка отображается, если резервное копирование выполняется в настоящее время или приостановлено.

 – приостановить резервное копирование. Кнопка отображается, если резервное копирование выполняется в настоящее время.

 – начать резервное копирование или возобновить прерванное. Кнопка отображается, если резервное копирование завершено или приостановлено.

Начать копирование

При нажатии на кнопку запускается создание резервных копий файлов. Кнопка отображается, если резервное копирование не выполняется в данный момент.

При нажатии на кнопку  раскрывается меню, в котором можно выбрать дополнительное действие с выбранными настройками резервного копирования:

- **Изменить настройки** – запустить мастер изменения настроек резервного копирования.
- **Удалить настройки** – удалить настройки резервного копирования.

Восстановить файлы

При нажатии на кнопку открывается окно **Восстановление файлов из резервных копий**. В окне вы можете выбрать резервные копии, из которых нужно восстановить файлы.

Войти в Dropbox

Кнопка, при нажатии на которую открывается окно входа в веб-сайт Dropbox. Если у вас нет учетной записи, вы можете перейти к регистрации на веб-сайте Dropbox.

Кнопка отображается, если вы еще не входили в веб-сайт Dropbox на этом компьютере.

Обновить статус

При нажатии на кнопку Kaspersky Security Cloud подключается к Онлайн-хранилищу и обновляет информацию о размере Онлайн-хранилища и о размере сохраненных в нем файлов.

Кнопка отображается, если программе ранее не удалось получить информацию об Онлайн-хранилище (например, если компьютер не был подключен к интернету).

Подробнее

По ссылке открывается окно **Подробные отчеты**. В окне отображается детальная информация о выполненных задачах резервного копирования.

Режим запуска

По ссылке открывается окно **Расписание резервного копирования**. В окне вы можете изменить режим запуска задачи резервного копирования.

Очистить

При нажатии на кнопку открывается окно **Очистка хранилища**, в котором вы можете удалить ненужные резервные копии из хранилища резервных копий.

Создать резервные копии других файлов

Кнопка, при нажатии на которую открывается окно мастера создания задачи резервного копирования.

Восстановить файлы из набора резервных копий, которого нет в списке

По ссылке открывается окно **Поиск резервных копий**. В окне вы можете указать хранилище резервных копий, в котором хранятся ранее созданные вами резервные копии.

Управление хранилищами

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.

Окно Выбор папки для резервного копирования

Развернуть всё | Свернуть всё

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

Развернуть всё | Свернуть всё

Копировать утилиту восстановления Kaspersky Restore Utility в хранилище

Если флажок установлен, Kaspersky Security Cloud 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 программа Kaspersky Security Cloud повреждена или не установлена.

Окно Файлы, выбранные для резервного копирования

Развернуть всё | Свернуть всё

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, Kaspersky Security Cloud создает резервную копию этого файла.

Если флажок напротив названия файла снят, Kaspersky Security Cloud не создает резервную копию этого файла.

Раздел Сетевой диск

Развернуть всё | Свернуть всё

Диск

Путь к сетевой папке, используемой в качестве хранилища резервных копий.

Обзор

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

Развернуть всё | Свернуть всё

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 **Обзор** и выбрать локальный диск в открывшемся окне **Выбор папки для резервного копирования**.

Обзор

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 Съемный диск

Развернуть всё | Свернуть всё

Список подключенных съемных дисков

В списке перечислены съемные диски, подключенные к компьютеру. Вы можете выбрать один из съемных дисков в качестве хранилища резервных копий.

Если съемный диск отсутствует в списке, вы можете указать путь к нему в поле, расположенном ниже, или нажать на кнопку **Обзор** и выбрать съемный диск в открывшемся окне **Выбор папки для резервного копирования**.

Обзор

При нажатии на кнопку открывается окно **Выбор папки для резервного копирования**. В этом окне можно выбрать съемный диск, используемый в качестве хранилища резервных копий.

Раздел Онлайн-хранилище

Развернуть всё | Свернуть всё

Для использования Онлайн-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

Развернуть всё | Свернуть всё

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.

Восстановить 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:

- **Изменить настройки** – запустить мастер изменения настроек хранилища.

- **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 сетевое хранилище

По ссылке открывается окно **Добавление сетевого хранилища**. В окне вы можете указать настройки сетевого диска, который нужно добавить в список хранилищ.

Подключить имеющееся хранилище

По ссылке открывается окно **Подключение хранилища**. В окне вы можете указать настройки локального, съемного, сетевого диска или Онлайн-хранилища, которое нужно добавить в список хранилищ.

Окно со списком наборов резервных копий в хранилище

Развернуть всё | Свернуть всё

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.

Восстановить файлы

При нажатии на кнопку открывается окно **Восстановление файлов из резервных копий**. В окне вы можете выбрать резервные копии, из которых нужно восстановить файлы.

Окно Очистка хранилища

Развернуть всё | Свернуть всё

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 Kaspersky Security Cloud удаляет 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 файлов, оригиналы которых удалены

Флажок включает / выключает удаление из хранилища резервных копий тех файлов, которые удалены с компьютера.

Окно Выбор версии резервной копии для восстановления

Развернуть всё | Свернуть всё

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 программы, соответствующей формату файла.
- **Восстановить версию резервной копии** – открывается окно **Выбор папки для восстановленных файлов**. В окне вы можете выбрать папку, в которую нужно поместить восстановленный файл.

Восстановить

При нажатии на кнопку открывается окно, в котором вы можете изменить настройки восстановления файлов.

Окно Выбор папки для восстановленных файлов

Развернуть всё | Свернуть всё

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

Развернуть всё | Свернуть всё

Остановить

При нажатии на кнопку Kaspersky Security Cloud прекращает восстановление файлов из резервных копий.

Окно Восстанавливаемый файл уже существует

Развернуть всё | Свернуть всё

Заменить файл резервной копией

Kaspersky Security Cloud удаляет существующий файл и помещает на его место файл, восстановленный из резервной копии.

Не восстанавливать этот файл

Kaspersky Security Cloud оставляет существующий файл без изменений, не восстанавливая одноименный файл из резервной копии.

Сохранить оба файла

Kaspersky Security Cloud 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, Kaspersky Security Cloud выполняет выбранное действие в отношении всех восстанавливаемых файлов.

Окно Восстановление файлов

Развернуть всё | Свернуть всё

Остановить

При нажатии на кнопку Kaspersky Security Cloud прекращает восстановление файлов из резервных копий.

Окно Настройки хранилища

Развернуть всё | Свернуть всё

Название хранилища

Поле содержит название хранилища резервных копий.

Окно Kaspersky Restore Utility

Развернуть всё | Свернуть всё

Задача резервного копирования

В раскрывающемся списке можно выбрать данные, которые требуется восстановить.

Дата / время 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 **Выбор версии резервной копии для восстановления**. В окне вы можете выбрать версию резервной копии, из которой требуется восстановить файл.

Если флажок напротив имени резервной копии файла установлен, Kaspersky Security Cloud восстанавливает этот файл.

Если флажок напротив имени резервной копии файла снят, то Kaspersky Security Cloud не восстанавливает этот файл.

По правой клавише мыши отображается контекстное меню элемента списка, содержащее следующие пункты:

- **Открыть файл** – файл открывается с помощью программы, предназначенной для работы с файлами этого типа.

- **Восстановить последнюю версию резервной копии** – открывается окно **Выбор папки для восстановленных файлов**, в котором вы можете указать, в какую папку следует восстановить файл из последней версии резервной копии.

- **Версии резервных копий файла** – открывается окно **Выбор версии резервной копии для восстановления**. В окне вы можете выбрать версию резервной копии, из которой требуется восстановить файл.

Версия

По ссылке открывается окно **Выбор версии резервной копии для восстановления**, в котором вы можете просмотреть все версии выбранного файла, доступные для восстановления.

Выбрать другое хранилище

По ссылке открывается окно выбора резервного хранилища.

Восстановить выбранные данные

При нажатии на кнопку открывается окно, в котором вы можете изменить настройки восстановления файлов.

Окно Категории сайтов

Развернуть всё | Свернуть всё

Интернет-банки и платежные системы

Если флажок установлен, программа показывает предупреждение, если вы создаете или вводите в интернете пароль, который ранее использовали на сайтах банков и платежных систем.

Социальные сети

Если флажок установлен, программа показывает предупреждение, если вы создаете или вводите в интернете пароль, который ранее использовали в социальных сетях.

Почтовые сервисы

Если флажок установлен, программа показывает предупреждение, если вы создаете или вводите в интернете пароль, который ранее использовали на сайтах почтовых сервисов.

Окно Помогите нам стать лучше! Оставьте свой отзыв

Развернуть всё | Свернуть всё

Набор настроек в этом окне зависит от того, какую оценку вы поставили компоненту. Настройка Категория вопроса доступна, если вы поставили компоненту оценку от 1 до 2.

Тема

Раскрывающийся список, где вы можете выбрать категорию, к которой относится ваш отзыв. Категория отзыва может затрагивать проблему с компонентом Устройства в моей сети.

- **Неудобно пользоваться**. Выберите этот элемент, если вы испытываете неудобства при использовании компонента Устройства в моей сети.

- **Программа долго ищет устройства в сети**. Выберите этот элемент, если компонент Устройства в моей сети работает слишком медленно.
- **Программа неправильно определяет устройства в сети**. Выберите этот элемент, если программа неправильно определяет названия и / или типы устройств, подключенных к сети.
- **Много сообщений о новых устройствах в сети**. Выберите этот элемент, если программа показывает вам слишком много уведомлений о новых устройствах в сети.
- **Снижается производительность компьютера**. Выберите этот элемент, если использование компонента Устройства в моей сети замедляет работу вашего компьютера.
- **Нельзя настроить компонент**. Выберите этот элемент, если у вас возникли трудности с настройкой компонента Устройства в моей сети.
- **Другое**. Выберите этот элемент, если ваша проблема не относится к указанным в других пунктах.

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 компоненте Устройства в моей сети в сутки. Если программе не удается отправить отзыв (например, отсутствует соединение с интернетом), программа сохраняет отзыв на вашем компьютере. Отзывы хранятся в открытом виде в течение 30 дней.