kaspersky

Kaspersky Premium

Руководство по эксплуатации

Версия программы: 21

Уважаемый пользователь!

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

Дата публикации документа: 16.05.2022

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

О «Лаборатории Касперского» (https://www.kaspersky.ru/about/company)

Kaspersky
Premium

Содержание

Предоставление данных

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

Предоставление данных в рамках Лицензионного соглашения

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

Данные для плана Kaspersky Basic

Данные для плана Kaspersky Standard

Данные для планов Kaspersky Plus и Kaspersky Premium

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 приложения, 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":

Данные для планов Kaspersky Basic и Kaspersky Standard

Данные для планов Kaspersky Plus и Kaspersky Premium

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:

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

Откроется окно **Настройка**.

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

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

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

Сохранение данных в отчет о работе приложения

Файлы отчетов могут содержать персональные данные, полученные в результате работы компонентов защиты, таких как Файловый Антивирус, Почтовый Антивирус, Интернет защита и 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\AVP21.7\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 приложении Kaspersky включена самозащита. Если самозащита выключена, файлы отчетов не защищаются.

Сохранение данных для Службы технической поддержки

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

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

  Эти данные хранятся локально в немодифицированном виде и доступны для просмотра под любой учетной записью на компьютере.
- Данные о системной памяти процессов приложения 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 приложения на территории Европейского союза, Великобритании, Бразилии, а также резидентами штата Калифорния

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

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

Кроме этого, мастер установки и удаления предложит вам принять следующие 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 приложениях и о скачиваемых подписанных приложениях, а также информацию об операционной системе для улучшения вашей защиты.

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

- 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** → **Настройки безопасности** → **Kaspersky Security Network**.

О решениях Kaspersky

Новые решения Kaspersky воплотили в себе наше видение современной кибербезопасности. В дополнение к новому названию вас ждет полностью обновленный интерфейс, а также целый ряд ранее не представленных функций.

Решения включают несколько планов, которые отличаются по уровню защиты и количеству доступных функций. Все новые и существующие функции сгруппированы по ключевым областям защиты.

Посмотрите, какие функции доступны вам в каждой из этих областей:

- Безопасность
- Производительность
- Приватность

Сравнение планов подписки

В приложении доступны четыре плана подписки. В таблице ниже можно узнать, какие функции приложения доступны в каждом плане подписки.

Планы подписки

Функциональность	Basic	Standard	Plus	Premium
My Kaspersky	✓	✓	✓	✓
Безопасность				
Быстрая проверка	✓	✓	✓	✓
Полная проверка	✓	✓	✓	✓
Выборочная проверка	✓	✓	✓	✓
Проверка внешних дисков	✓	✓	✓	✓
Фоновая проверка	✓	✓	✓	✓
Поиск уязвимостей	✓	✓	✓	✓
Файловый Антивирус	✓	✓	✓	✓
Интернет-защита	✓	✓	✓	✓
Почтовый Антивирус	✓	✓	✓	✓
Обновление баз и модулей приложения	✓	✓	✓	✓
Отчеты	✓	✓	✓	✓
Карантин	✓	✓	✓	✓
Устранение неполадок Windows	✓	✓	✓	✓
Восстановление зараженного компьютера	✓	✓	✓	✓
Защита от эксплойтов	✓	✓	✓	✓
Мониторинг активности	✓	✓	✓	✓

Поиск небезопасных настроек операционной системы	✓	✓	✓	✓
Защита от сетевых атак	✓	✓	✓	✓
Проверка ссылок	✓	✓	✓	✓
Расширение Kaspersky Protection	✓	✓	✓	✓
Предотвращение вторжений		✓	✓	✓
Сетевой экран		✓	✓	✓
Мониторинг сети		✓	✓	✓
Анти-Фишинг		✓	✓	✓
Новости безопасности		✓	✓	✓
Производительность				
Быстрый запуск		✓	✓	✓
Ускорить работу		✓	✓	✓
Дубликаты файлов		✓	✓	✓
Большие файлы		✓	✓	✓
Неиспользуемые приложения		✓	✓	✓
Обновление приложений		✓	✓	✓
Текущая активность		✓	✓	✓
Игровой режим		✓	✓	✓
Режим "Не беспокоить"		✓	✓	✓
Экономия заряда батареи		✓	✓	✓
Диагностика жесткого диска			✓	✓
Резервное копирование			✓	✓
Приватность				
Поиск утечки данных	один аккаунт	один аккаунт	✓	✓
Защита от сбора данных в интернете		✓	✓	✓
Безопасные платежи		✓	✓	✓

Защита веб-камеры	✓	✓	✓
Сталкерские приложения	✓	✓	✓
Блокировщик скрытых установок	✓	✓	✓
Удаление рекламных приложений	✓	✓	✓
Анти-Баннер	✓	✓	✓
Удаление следов активности	✓	✓	✓
Безопасное VPN-соединение		✓	✓
Устройства в моей сети		✓	✓
Менеджер паролей		✓	✓
Уничтожитель файлов		✓	✓
Секретная папка		✓	✓
Премиальные функции			
Премиальная техническая поддержка			✓
Безопасное хранение документов			✓

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 приложения, использования Kaspersky Security Network, а также обновления баз и модулей приложения).
- Microsoft Windows Installer 4.5 или выше.
- Microsoft .NET Framework 4 или выше.
- Microsoft .NET Desktop Runtime 5.x (не ниже 5.0.10).
- 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 (21H2, 22H2)	1 ГГц или выше	4 ГБ (для 64-разрядной операционной системы)	Приложение имеет следующие ограничения при установке на все версии Microsoft Windows 11: • Подсистема Windows для Linux 2 (WSL2) не поддерживается. • В контекстном меню объектов не отображаются команды приложения. Чтобы команды отображались, требуется развернуть меню.
Microsoft Windows 11 Enterprise (21H2, 22H2)			
Microsoft Windows 11 Pro (21H2, 22H2)			
Microsoft Windows 10 Home (версии: 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, 21H1, 21H2, 22H2)	1 ГГц или выше	1 ГБ (для 32-разрядной операционной системы) или 2 ГБ (для 64-разрядной операционной системы)	
Microsoft Windows 10 Enterprise (версии: 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, 21H1, 21H2, 22H2)			
Microsoft Windows 10 Pro (версии: 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, 21H1, 21H2, 22H2)			
Microsoft Windows 8.1 (Service Pack 0 или	1 ГГц или выше	1 ГБ (для 32-разрядной	

выше, Windows 8.1 Update)		операционной системы) или 2 ГБ (для 64-разрядной операционной системы)
Microsoft Windows 8.1 Pro (Service Pack 0 или выше, Windows 8.1 Update)		
Microsoft Windows 8.1 Enterprise (Service Pack 0 или выше, Windows 8.1 Update)		
Microsoft Windows 8 (Service Pack 0 или выше)	1 ГГц или выше	1 ГБ (для 32-разрядной операционной системы) или 2 ГБ (для 64-разрядной операционной системы)
Microsoft Windows 8 Pro (Service Pack 0 или выше)		
Microsoft Windows 8 Enterprise (Service Pack 0 или выше)		
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
Microsoft Windows 7		

Home Basic (Service Pack 1 или выше)	(для 64-разрядной операционной системы)
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 Интернет-защита, 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 – 99.x;
- Mozilla Firefox версий 52.x – 99.x;
- Mozilla Firefox ESR 52.x, 60.x, 68.x, 78.x, 91.x;
- Google Chrome версий 48.x – 100.x.

Браузеры, которые поддерживают Экранную клавиатуру и Проверку защищенных соединений:

- Microsoft Edge на базе Chromium 77.x – 99.x;
- Mozilla Firefox версий 52.x – 99.x;
- Mozilla Firefox ESR 52.x, 60.x, 68.x, 78.x, 91.x;
- Google Chrome 48.x – 100.x.

Браузеры, которые поддерживают режим Защищенного браузера:

- Microsoft Internet Explorer 11.0;
- Microsoft Edge на базе Chromium 77.x – 99.x;
- Mozilla Firefox версий 52.x – 99.x;
- Mozilla Firefox ESR 52.x, 60.x, 68.x, 78.x, 91.x;
- Google Chrome 48.x – 100.x;
- Яндекс.Браузер 18.3.1 – 22.1.5 (есть ограничения).

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

Kaspersky 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, Microsoft Windows 11;
- 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 1024x768;
- графический чипсет Intel GMA 950 или выше.

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

Совместимость с другими приложениями "Лаборатории Касперского"

Приложение Kaspersky совместимо со следующими приложениями "Лаборатории Касперского":

- Kaspersky Safe Kids 1.5;
- Kaspersky Password Manager 10;
- Kaspersky Software Updater 2.1;
- Kaspersky Virus Removal Tool 2015, 2020;
- Kaspersky Secure Connection 4.0, 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5,7.

Что нового в последней версии приложения

В последней версии приложения появились следующие новые возможности и улучшения:

- Обновлена терминология лицензирования. Добавлены понятные термины, связанные с подписочной моделью лицензирования.
- Обновлен план Kaspersky Premium. В план добавлена интеграция с приложением Kaspersky Password Manager, в связи с чем в основном приложении появились следующие возможности:
  - показ информации о защищаемых паролях.
  - показ информации о защищаемых документах.
- Добавлено окно с возможностью скачать другие приложения «Лаборатории Касперского» и наших партнеров.
- Добавлена возможность менять тему оформления приложения на темную или на ту, которая используется в операционной системе.
- Улучшен графический интерфейс компонента Устройства в моей сети.
- Улучшены статусы безопасности компьютера. В частности, устранена ситуация с одновременным показом красного статуса (например, базы устарели) и желтого или зеленого значка выполнения задачи проверки.
- Улучшена анимация в чате при первом запуске приложения.
- Улучшена функциональность Ускорить работу компьютера. Добавлена возможность выключить автоматический поиск файлов, замедляющих работу компьютера.
- В интерфейс приложения добавлен график со статусами состояния жесткого диска.
- Улучшен сценарий выбора региона при запуске приложения.

Как работает подписка

Как работает платная подписка

Подписка продлевается автоматически в конце каждого периода, пока вы ее не отмените. Ближе к концу оплаченного периода вы получите по электронной почте напоминание о предстоящем списании. Списание денежных средств за следующий период происходит до даты истечения текущего периода, чтобы обеспечить непрерывную защиту от угроз компьютерной безопасности. После успешного продления подписки оставшиеся дни текущего периода добавятся к новому периоду.

Обратите внимание, что стоимость продления подписки может меняться. На момент продления могут быть доступны специальные предложения и скидки, которые не будут действовать для вашей подписки.

Как работает бесплатная пробная подписка

Бесплатная пробная подписка начинает действовать сразу после ее оформления. За несколько дней до окончания пробного периода вы получите напоминание о продлении подписки. Если вы не отмените подписку в течение пробного периода, по его истечении подписка будет автоматически продлена на следующий период.

Если возникла проблема с платежом

Если по каким-то причинам не удалось автоматически продлить вашу подписку (истек срок действия банковской карты, банковская карта была заблокирована или у вас не активирована функция автопродления), по истечении срока действия подписки вам может предоставляться льготный период для продления подписки, в течение которого вы можете использовать функции приложения без ограничений. Если вы не продлили подписку, по истечении льготного периода приложение может перейти в режим ограниченной функциональности. Продолжительность режима ограниченной функциональности зависит от вашего региона и условий лицензирования. Информацию о сроке действия льготного периода и режима ограниченной функциональности вы найдете в разделе Профиль.

О подписках, купленных у поставщиков услуг

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

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

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

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

При использовании приложения по подписке, оформленной у поставщика услуг, недоступно добавление резервного кода активации для продления срока действия подписки.

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

О подписках, купленных в App Store и Google Play

Если вы купили подписку в одном из магазинов приложений App Store или Google Play для использования на устройствах на базе Microsoft Windows, по истечении срока действия подписки вам необходимо снова купить подписку в 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 оформить бесплатную пробную подписку в App Store и Google Play. Обратите внимание, что по истечении пробного периода приложение автоматически переходит на платную подписку и с вашей банковской карты будут списаны средства за использование приложения. Если вы не хотите продолжать пользоваться приложением по этой подписке, отмените подписку до того, как закончится пробный период.

Как купить подписку

Подписку на использование приложения можно приобрести одним из следующих способов:

Купить на сайте "Лаборатории Касперского"

Вы можете приобрести подписку на использование приложения на сайте "Лаборатории Касперского":

Купить Kaspersky Basic

Купить Kaspersky Standard

Купить Kaspersky Plus

Купить Kaspersky Premium

Kaspersky Premium доступен не во всех регионах.

Купить через интерфейс приложения

Чтобы приобрести подписку через интерфейс приложения:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Профиль**. Если вы подключили устройство к аккаунту My Kaspersky, здесь отображается ваш email.
3. В блоке с информацией о подписке нажмите на кнопку **Купить сейчас**.

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

Купить у компании-партнера "Лаборатории Касперского"

Вы можете приобрести подписку в магазине компании-партнера "Лаборатории Касперского".

Как управлять подпиской с помощью аккаунта My Kaspersky

Для работы с приложением требуется *аккаунт My Kaspersky*.

В зависимости от вашей подписки подключение устройства, на которое вы устанавливаете приложение, к вашему аккаунту My Kaspersky может быть обязательным, чтобы иметь доступ к некоторым или всем функциям приложения.

В аккаунте My Kaspersky вы можете:

- просматривать информацию о подписках и сроках их действия;
- управлять защитой устройств удаленно;
- безопасно хранить и синхронизировать пароли и другую личную информацию, если вы используете Kaspersky Password Manager;
- скачивать приобретенные приложения;
- обратиться в Службу технической поддержки за помощью;
- узнавать о новых приложениях и специальных предложениях "Лаборатории Касперского".

Более подробную информацию о всех возможностях аккаунта My Kaspersky вы найдете в Справке My Kaspersky .

Как подключить устройство к аккаунту My Kaspersky

Если вы купили подписку на сайте Kaspersky, то в процессе покупки вам был создан аккаунт. Письмо со ссылкой для создания пароля было отправлено на адрес электронной почты, указанный во время покупки.

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

Вход с помощью аккаунта Facebook и Google доступен не во всех регионах.

Если у вас еще нет аккаунта, вы можете создать его в процессе подключения устройства к аккаунту. Вы также можете использовать для входа в аккаунт учетные данные других ресурсов "Лаборатории Касперского".

Чтобы подключить ваше устройство к аккаунту My Kaspersky:

1. Вы можете подключить устройство к аккаунту:

   - В окне подключения во время активации приложения.
   - В приложении в разделе **Профиль.**

     В блоке **Войти в My Kaspersky** нажмите на кнопку **Войти**.
   - На сайте My Kaspersky .
   - Во время активации некоторых функций приложения.

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

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

     Если в аккаунте My Kaspersky вы настроили двухэтапную проверку, на ваш телефон будет отправлено сообщение с проверочным кодом. Введите проверочный код в поле ввода и нажмите на кнопку **Продолжить**.
   - **Вход с помощью аккаунта Google, Facebook или Apple**.

     a. Нажмите на соответствующую кнопку **Войти с помощью Google**, **Войти с помощью Facebook** или **Войти с помощью Apple**.

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

     Если у вас еще нет аккаунта Google, Facebook или Apple, вы можете создать его, а затем продолжить настройку быстрого входа в My Kaspersky.

     Если в вашем аккаунте My Kaspersky настроена двухэтапная проверка, настройте быстрый вход в своем аккаунте на сайте My Kaspersky, а затем вернитесь в приложение и войдите с помощью Google, Facebook или Apple.

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

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

Ваше устройство будет подключено к аккаунту My Kaspersky. Дополнительно вы можете задать пароль для вашего аккаунта на сайте My Kaspersky.

Обработка данных при входе в аккаунт

При входе в аккаунт My Kaspersky с помощью аккаунта Google, Facebook или Apple осуществляется обработка следующих данных:

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

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

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

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

Как отменить подписку

Вы можете отменить вашу подписку в любое время. После отмены она больше не будет продлеваться автоматически, а ваши устройства останутся под защитой до окончания последнего оплаченного периода.

Подписку следует отменять до даты автоматического списания средств за новый период во избежание лишних расходов. Обратите внимание, что списание за новый период происходит до истечения срока действия текущего периода, чтобы обеспечить непрерывную защиту.

Как отменить подписку на территории России, Беларуси, Абхазии, Армении, Азербайджана, Грузии, Южной Осетии, Кыргызстана, Монголии, Таджикистана, Туркменистана, Узбекистана, Казахстана

Чтобы отменить подписку:

1. Проверьте email, который вы указывали при покупке. В письме с подтверждением заказа или с напоминанием о продлении подписки вы найдете ссылку на страницу управления автоматическим продлением.
2. Пройдите по ссылке.

   В браузере по умолчанию откроется ваша персонализированная страница на сайте поставщика платежных услуг.
3. Отмените подписку на странице с информацией о продлении подписки.

   Подписка будет отменена. На ваш адрес электронной почты вы получите письмо с подтверждением об отмене подписки.

Как отменить подписку на территории других стран

Чтобы отменить подписку:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Профиль**.
3. В блоке с информацией о подписке нажмите на кнопку **Управлять аккаунтом**. Если вы не подключали устройство к аккаунту, нажмите на кнопку **Войти**.

   В браузере по умолчанию откроется окно входа в аккаунт My Kaspersky.
4. В аккаунте My Kaspersky перейдите в раздел **Подписки** и нажмите на панель подписки.

   Откроется окно с информацией о подписке.
5. Нажмите **Управлять подпиской**. В раскрывающемся списке выберите **Отменить подписку**.
6. В новом окне браузера откроется страница управления подпиской на сайте нашего официального реселлера Nexway.
7. Нажмите **Отменить** в блоке **Управление подпиской**.

Подписка будет отменена.

Если вы отменили подписку после автоматического списания средств за следующий период, подписка останется активной до даты окончания оплаченного периода. Если вы хотите отменить списание за период, оплата за который уже была произведена, вы можете оформить возврат в соответствии с политикой возвратов. Как правило, вы можете оформить возврат в течение 30 дней со дня списания денежных средств. Для уточнения условий и возможности возврата, обратитесь в Службу технической поддержки.

При оформлении возврата вам потребуется предоставить следующую информацию:

- дата покупки;
- ваше имя и адрес электронной почты, указанный во время покупки;
- номер заказа.

После проверки предоставленной информации денежные средства поступят на счет в течение 5-7 рабочих дней.

Как изменить способ оплаты

Автоматические списания за продление вашей подписки осуществляются с того способа оплаты, который вы указали в процессе покупки подписки. Вы можете изменить этот способ оплаты.

Как изменить способ оплаты на территории России, Беларуси, Абхазии, Армении, Азербайджана, Грузии, Южной Осетии, Кыргызстана, Монголии, Таджикистана, Туркменистана, Узбекистана, Казахстана

Чтобы изменить способ оплаты:

1. Проверьте email, который вы указывали при покупке. В письме с подтверждением заказа или с напоминанием о продлении подписки вы найдете ссылку на страницу управления автоматическим продлением.
2. Пройдите по ссылке.

   В браузере по умолчанию откроется ваша персонализированная страница на сайте поставщика платежных услуг.
3. На странице с информацией о продлении подписки измените способ оплаты и сохраните изменения.

[Как изменить способ оплаты на территории других стран]

Чтобы изменить способ оплаты:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Профиль**.
3. В блоке с информацией о подписке нажмите на кнопку **Управлять аккаунтом**. Если вы не подключали устройство к аккаунту, нажмите на кнопку **Войти**.

   В браузере по умолчанию откроется окно входа в аккаунт My Kaspersky.
4. Нажмите на ссылку с адресом электронной почты, расположенную в правой верхней части страницы.
5. В раскрывающемся списке выберите **Параметры аккаунта**.
6. Перейдите на закладку **Способ оплаты**.
7. Нажмите на значок  .

   В раскрывающемся меню выберите **Изменить**.
8. В новом окне браузера откроется страница для редактирования способа оплаты на сайте нашего официального реселлера Nexway. Измените способ оплаты, следуя инструкциям на экране.

Как активировать подписку на устройстве

В этом разделе вы узнаете, как начать пользоваться приложениями после того, как вы приобрели подписку. Для активации необходимо подключение к интернету.

Если вы купили подписку на сайте Kaspersky

Если вы купили подписку в интернет-магазине "Лаборатории Касперского", то в процессе покупки вам был создан аккаунт My Kaspersky. Аккаунт My Kaspersky необходим для активации подписки на разных устройствах и для управления подпиской. Активация подписки осуществляется путем входа в аккаунт My Kaspersky с того устройства, на которое вы устанавливаете приложение.

Чтобы активировать подписку на устройствах:

1. Проверьте email, который вы указывали при покупке. Мы отправили вам два письма: чек и инструкцию, как завершить активацию подписки.

2. В письме-инструкции перейдите по ссылке **Перейти на My Kaspersky**, чтобы завершить создание аккаунта и войти в него.

3. Нажмите на кнопку **Скачать**, чтобы скачать приложение на устройство.

4. Установите приложение.

   После успешной установки приложение автоматически подключится к вашему аккаунту и активируется по купленной подписке.

При продлении подписки срок ее действия автоматически обновится в течение 24 часов на всех устройствах, которые были активированы по этой подписке и подключены к аккаунту My Kaspersky.

> Если вы купили подписку в интернет-магазине "Лаборатории Касперского", отсчет срока действия подписки начинается с момента покупки.

Если вы купили коробку или карту активации

Если вы купили коробку или карту активации в магазине, вам нужен код активации, чтобы активировать приложение. Вы можете найти код активации на коробке, в документации или на оборотной стороне карты. Код активации представляет собой уникальную последовательность из двадцати латинских букв и цифр в формате xxxxx-xxxxx-xxxxx-xxxxx.

Отсчет срока действия подписки, активированной кодом активации, начинается с даты активации приложения на первом устройстве.

Если вы купили карту активации:

1. На устройстве, которое вы хотите защитить, пройдите на сайт My Kaspersky.

2. Создайте аккаунт My Kaspersky или войдите в существующий аккаунт.

3. В блоке **Есть код активации?** в нижней части страницы введите код активации в поле ввода.

4. Нажмите на кнопку **Добавить**.

   Если добавление кода активации прошло успешно, в разделе **Подписки** появится панель подписки.

5. Нажмите на панель подписки.

   Откроется окно с информацией о подписке.

6. Нажмите на кнопку **Скачать**, чтобы скачать приложение на устройство.

7. Установите приложение.

   После успешной установки приложение автоматически активируется по подписке.

Если вы купили коробку с установочным диском:

1. Вставьте диск в дисковод.

2. В окне подключения к аккаунту My Kaspersky создайте аккаунт или войдите в существующий аккаунт.

3. В окне добавления кода активации введите код активации в поле ввода и нажмите на кнопку **Добавить**.

   Код активации сохранится в вашем аккаунте в разделе **Подписки**.

4. Нажмите на кнопку **Скачать и установить**, чтобы скачать и установить приложение на устройство.

5. Установите приложение.

   После успешной установки приложение автоматически активируется по подписке.

Ваш код активации теперь хранится в аккаунте My Kaspersky. Чтобы защитить новое устройство, войдите в аккаунт и скачайте приложение. Вы также можете вручную ввести код активации в приложении.

Активация подписки, если приложение уже установлено на устройстве

В этом разделе вы узнаете, как обновить истекшую подписку, добавить новый код активации в приложение с активной подпиской для ее автоматического продления и перейти с пробной подписки на платную подписку.

Ваша подписка истекла

Если у вас активирована функция автопродления, подписка будет автоматически продлена на новый срок без вашего участия. Если у вас не активирована функция автопродления, вам необходимо продлить подписку самостоятельно.

Если вы самостоятельно продлеваете подписку, и ранее добавляли в приложение резервный код активации, по истечении срока действия подписки приложение автоматически активируется с помощью резервного кода активации.

Чтобы продлить подписку:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Профиль**. Если вы подключили устройство к аккаунту My Kaspersky, здесь отображается ваш email.
3. В блоке с информацией о подписке нажмите на кнопку **Продлить сейчас**.

   В браузере по умолчанию откроется интернет-магазин "Лаборатории Касперского" или одного из наших партнеров.

   В процессе покупки укажите email от вашего аккаунта My Kaspersky. Если у вас еще нет аккаунта, он будет создан на указанный email. После покупки и подключения приложения к аккаунту My Kaspersky, подписка автоматически активируется на устройстве в течение часа с момента продления.

Вы также можете отправить новую подписку на устройства из аккаунта My Kaspersky. Подробную информацию о том, как отправить подписку на подключенное к аккаунту устройство, вы найдете в Справке My Kaspersky.

Если вы не продлили срок действия подписки, приложение может перейти в режим ограниченной функциональности.

Продление подписки с помощью резервного кода активации

Если у вас есть новый код активации, вы можете добавить его в приложение в качестве резервного кода. По истечении подписки приложение будет автоматически активировано с помощью резервного кода активации. Таким образом вы можете обеспечить непрерывную защиту устройства.

В некоторых случаях добавление резервного кода активации **может быть недоступно**.

Добавление резервного кода активации может быть недоступно из-за следующих ограничений:

- Если вы используете приложение по подписке с автопродлением, добавление резервного кода активации недоступно.

- Код активации для подписки с автопродлением не может быть добавлен в качестве резервного кода активации.
- Если вы используете приложение по пробной подписке, добавление резервного кода недоступно.
- В приложение уже добавлен резервный код активации.
- Добавление резервного кода недоступно, если текущая подписка истекла.
- Подписка еще недоступна в вашем регионе.

Чтобы добавить резервный код активации:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Профиль**. Если вы подключили устройство к аккаунту My Kaspersky, здесь отображается ваш email.
3. В блоке с информацией о подписке нажмите на три точки и выберите опцию **Ввести код активации**.
4. Введите код активации в поле ввода и нажмите на кнопку **Сохранить код активации**.

   Резервный код активации будет отображаться в окне **Информация о подписке**.

Если вы указываете резервный код активации, который может быть использован на нескольких устройствах, то вы должны повторить процедуру добавления резервного кода на всех устройствах, на которых вы хотите автоматически продлить подписку.

Попытка активации и полная проверка резервного кода будет выполнена после истечения срока действия текущей подписки, а также в случае удаления подписки с устройства. Приложение проверит срок действия резервного кода, ограничение на количество устройств, на которых можно использовать подписку, а также совместимость подписки с установленной версией приложения. В процессе активации резервного кода может потребоваться подключение к аккаунту My Kaspersky.

Если вы добавляете в качестве резервного код активации, уже примененный ранее на этом или другом устройстве, при продлении подписки с помощью этого резервного кода датой активации считается дата первой активации приложения с помощью этого кода. Для продления подписки добавляйте в приложение резервный код активации, срок действия которого заканчивается позже, чем у подписки, используемой в приложении.

Если приложение не активировалось автоматически с помощью резервного кода активации, вы можете самостоятельно активировать его нажатием на кнопку **Попробовать еще раз**. Если текущая подписка заблокирована, вы можете активировать приложение с помощью резервного кода нажатием на кнопку **Активировать сейчас**.

Вы также можете отправить резервный код активации на устройства из аккаунта My Kaspersky. Подробную информацию о том, как отправить подписку на подключенное к аккаунту устройство, вы найдете в Справке My Kaspersky .

Переход с пробной подписки на платную подписку

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

В некоторых регионах может быть не предусмотрен автоматический переход на платную подписку. Если в процессе оформления бесплатной пробной подписки вы не указывали платежные данные для последующего продления подписки, по истечении пробного периода вам потребуется купить подписку, чтобы продолжить защищать ваши устройства.

Чтобы перейти с пробной подписки на платную подписку:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Профиль**. Если вы подключили устройство к аккаунту My Kaspersky, здесь отображается ваш email.
3. В блоке с информацией о подписке нажмите на кнопку **Купить сейчас**.

   В браузере по умолчанию откроется сайт "Лаборатории Касперского" или одного из наших партнеров. В процессе покупки укажите email от вашего аккаунта My Kaspersky.

После покупки подписка автоматически активируется на вашем устройстве.

Как установить и удалить приложение

Как установить приложение

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

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

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

Чтобы установить приложение на ваш компьютер,

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

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

Вы можете установить Kaspersky с помощью командной строки.

> Некоторые команды можно выполнить только под учетной записью администратора.

Синтаксис командной строки:

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

Чтобы установить приложение из командной строки:

1. Запустите командную строку от имени администратора.
2. Введите адрес установочного файла и команду для запуска установки с нужными параметрами и свойствами. Параметры и свойства установки описаны ниже.
3. Следуйте инструкциям мастера установки.

Основные параметры

Имя команды	Значение	Пример
`/s`	Неинтерактивный (silent) режим установки — без вывода диалоговых окон при установке.	`saas21.exe /s`
`/mybirthdate=YYYY-MM-DD`	Дата рождения. Если вы младше 16 лет, установка не осуществляется. Этот параметр является: • обязательным для неинтерактивной установки; • необязательным для установки приложения в OEM-режиме.	`saas21.exe /mybirthdate=1986-12`
`/l`	Выбор языка, используемого при установке мультиязычной версии.	`saas21.exe /lru-ru`
`/t`	Папка, в которую будет сохранен журнал установки.	`saas21.exe /tC:\KasperskyLab`
`/p<свойство>=<значение>`	Задает свойства для установки.	`saas21.exe /pALLOWREBOOT=1 /pSKIPPRODUCTCHECK=1`
`/h`	Вызов справки.	`saas21.exe /h`

Дополнительные параметры

Имя команды	Значение	Пример
`/x`	Удаление продукта.	`saas21.exe /x`

Наиболее значимые свойства установки

Имя команды	Значение	При

Имя команды	Значение	Пр
ACTIVATIONCODE=<значение>	Ввод кода активации.	
AGREETOEULA=1	Подтвердить согласие с Лицензионным соглашением.	
AGREETOPRIVACYPOLICY=1	Подтвердить согласие с Политикой конфиденциальности.	
JOINKSN_ENHANCE_PROTECTION=1	Подтвердить согласие предоставлять персональные данные в целях улучшения основной функциональности продукта.	
JOINKSN_MARKETING=1	Подтвердить согласие предоставлять персональные данные для маркетинговых целей.	
INSTALLDIR=<значение>	Задать место установки.	saas21.exe /p"INSTALLDIR and Settings\
KLPASSWD=<значение>	Установить пароль на различные функции продукта. Если при этом не задано значение параметра KLPASSWDAREA, используется область действия пароля по умолчанию: • изменение настроек приложения;	saas21.exe /pKLPASSWD=12

	• завершение работы приложения.	
`KLPASSWDAREA=[SET|EXIT|UNINST]`	Задать область действия пароля, заданного параметром KLPASSWD: • SET — Изменение настроек параметров приложения. • EXIT — Завершение работы приложения. • UNINST — Удаление приложения. Возможно множественное значение этого параметра, при этом значения должны разделяться символом «;».	
`SELFPROTECTION=1`	Включить самозащиту продукта при установке.	`saas21.exe /pSELFPROTECT`
`ALLOWREBOOT=1`	Разрешить перезагрузку в случае необходимости.	`saas21.exe /p`
`SKIPPRODUCTCHECK=1`	Не выполнять поиск приложений, несовместимых с Kaspersky.	`saas21.exe /pSKIPPRODUCT`

-oembackupmode	Не запускать приложение после установки в случае загрузки Windows в режиме аудита.	saas21.exe /s oembackupmode

Используя значение параметра SKIPPRODUCTCHECK=1, вы принимаете на себя ответственность за возможные последствия несовместимости Kaspersky с другими приложениями.

Параметр SKIPPRODUCTCHECK=1 позволяет игнорировать только приложения, которые удаляются вручную.

Пример составной команды, которая позволяет во время установки разрешить перезагрузку компьютера и не выполнять поиск несовместимых приложений:

```
saas21.exe /pALLOWREBOOT=1 /pSKIPPRODUCTCHECK=1
```

Мастером установки будут выполнены следующие шаги:

1. Начало установки

   На этом шаге мастер предлагает вам установить приложение.

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

   Просмотр Лицензионного соглашения

   Этот шаг мастера отображается для некоторых языков локализации при установке приложения, скачанного через интернет.

   На этом шаге мастер предлагает вам ознакомиться с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского".

   Внимательно прочитайте Лицензионное соглашение и, если вы согласны со всеми его пунктами, нажмите на кнопку **Продолжить** (в некоторых регионах эта кнопка называется **Принять**).

   В некоторых версиях приложения Лицензионное соглашение можно открыть по ссылке на приветственном экране мастера. В этом случае в окне с текстом лицензионного соглашения доступна только кнопка **Назад**. Нажимая на кнопку **Установить** вы принимаете условия лицензионного соглашения.

Установка приложения на ваш компьютер будет продолжена.

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

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

Просмотр Положения о Kaspersky Security Network

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

Ознакомьтесь с Положением о Kaspersky Security Network и выполните следующие действия:

- Если вы согласны со всеми его пунктами, оставьте флажок в окне мастера **Я хочу участвовать в Kaspersky Security Network** установленным и нажмите на кнопку **Продолжить**.

- Если вы не хотите принимать участие в программе Kaspersky Security Network, снимите флажок **Я хочу участвовать в Kaspersky Security Network** и нажмите на кнопку **Продолжить**.

В некоторых версиях приложения, чтобы принять Положение о Kaspersky Security Network вам нужно установить флажок **Я хочу участвовать в Kaspersky Security Network** на приветственном экране мастера. Ознакомиться с положением вы можете по ссылке Kaspersky Security Network. После того как вы ознакомились с текстом положения, нажмите на кнопку **Назад**, чтобы продолжить установку. Если флажок **Я хочу участвовать в Kaspersky Security Network** установлен, нажимая на кнопку **Установить** вы принимаете условия Положения о Kaspersky Security Network.

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

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

2. Установка приложения

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

Проверки во время установки приложения

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

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

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

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

Установка Kaspersky Password Manager вместе с приложением Kaspersky Plus или Kaspersky Premium

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

Приложение Kaspersky Password Manager не входит в планы Kaspersky Basic и Kaspersky Standard. Если вы хотите использовать приложение для защиты паролей Kaspersky Password Manager, вы можете скачать и установить его как отдельное приложение или перейти на план Kaspersky Plus.

3. Завершение установки

   На этом шаге мастер информирует вас о завершении установки приложения.

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

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

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

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

При установке приложения Kaspersky Plus или Kaspersky Premium устанавливается приложение Kaspersky Secure Connection, предназначенное для включения безопасного VPN-соединения с помощью Virtual Private Network (VPN). Вы можете удалить Kaspersky Secure Connection независимо от приложения Kaspersky. Если в вашей стране запрещено использование VPN, приложение Kaspersky Secure Connection не устанавливается.

Для дальнейшей работы с приложением вам потребуется подключиться к My Kaspersky и завершить активацию, подробная информация представлена в соответствующих разделах:

Для чего нужен My Kaspersky

Как активировать подписку на устройстве

Установка поверх других приложений "Лаборатории Касперского"

Приложение может быть установлено поверх следующих приложений "Лаборатории Касперского":

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

Во время установки нового приложения удаляется установленное приложение Kaspersky Anti-Virus, Kaspersky Internet Security, Kaspersky Security Cloud, Kaspersky Total Security. Лицензия на удаленное приложение может быть применена в новом приложении Kaspersky за исключением лицензии Kaspersky Total Security. Настройки удаляемого приложения сохраняются.

Во время установки нового приложения удаляется установленное приложение Kaspersky Free. Настройки приложения Kaspersky Free не сохраняются.

При переходе с Kaspersky Total Security на приложение Kaspersky Basic или Kaspersky Standard резервные копии файлов сохраняются, но не отображаются в этих приложениях. Вы можете добавить резервные копии файлов вручную. При переходе с Kaspersky Total Security на приложение Kaspersky Plus копии файлов сохраняются и отображаются автоматически.

Расширение Kaspersky Protection для браузеров

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

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

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

Управлять Защитой от сбора данных в интернете

Управлять Анти-Баннером

Сообщить о подозрении на фишинг

Чтобы сообщить о подозрении на фишинговый сайт:

1. Убедитесь, что вы находитесь на странице сайта, который подозреваете в фишинге.
2. В панели инструментов браузера нажмите на кнопку **Kaspersky Protection**.
3. В меню расширения выберите **Сообщить о подозрении на фишинг**.
4. Проверьте, что в открывшемся окне отображается веб-адрес сайта, который вы подозреваете в фишинге.
5. Нажмите на кнопку **Сообщить**.

Сообщение будет доставлено в Kaspersky Security Network.

Сообщить о проблеме с сайтом

Чтобы сообщить о проблеме с сайтом:

1. Убедитесь, что вы находитесь на странице сайта, о проблеме которого вы хотели бы сообщить.
2. В панели инструментов браузера нажмите на кнопку **Kaspersky Protection**.
3. В меню расширения выберите **Сообщить о проблеме с сайтом**.
4. Проверьте, что в открывшемся окне отображается веб-адрес сайта.
5. Опишите проблему в поле ввода.
6. Нажмите на кнопку **Сообщить**.

Сообщение будет доставлено.

Открыть экранную клавиатуру

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

В браузерах Google Chrome и Mozilla Firefox расширение Kaspersky Protection устанавливается автоматически. Приложение Kaspersky предлагает вам активировать расширение. В браузере Microsoft Edge на базе Chromium расширение Kaspersky Protection также устанавливается автоматически, однако приложение не предлагает вам активировать расширение. Необходимо активировать расширение самостоятельно.

Поддержка Яндекс.Браузера

При использовании Яндекс.Браузера работают следующие компоненты приложения:

- Защищенный браузер;
- Проверка ссылок;
- Интернет-защита;
- Анти-Фишинг.

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

Поддержка Internet Explorer

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

Как удалить приложение

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

Удаление приложения выполняется с помощью мастера установки и удаления.

Как удалить приложение в операционной системе Windows 7

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

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

Как удалить приложение в операционной системе Windows 8 и выше

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

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

Будет запущен мастер удаления приложения.

В процессе удаления необходимо выполнить следующие шаги:

1. Чтобы удалить приложение, требуется ввести пароль для доступа к настройкам приложения. Если вы по каким-либо причинам не можете указать пароль, удаление приложения будет невозможно. После ввода пароля нажмите на кнопку **Подтвердить**.

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

2. Сохранение данных для повторного использования

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

Вы можете сохранить следующие данные:

- **Информация о подписке** – данные, позволяющие в дальнейшем не активировать устанавливаемое приложение, а использовать его по уже действующей подписке, если срок действия подписки не истечет к моменту установки.
- **Файлы карантина** – файлы, проверенные приложением и помещенные на карантин.

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

- **Настройки работы приложения** – параметры работы приложения, установленные во время его настройки.

> Вы также можете экспортировать настройки защиты при помощи командной строки, используя команду `avp.com EXPORT <имя_файла>`

- **Данные iChecker** – файлы, содержащие информацию об объектах, уже проверенных с помощью технологии iChecker.
- **Базы Анти-Спама** – базы с образцами спам-сообщений, добавленных пользователем.
- **Секретная папка** – файлы, которые вы помещали на хранение в секретную папку.

Для продолжения удаления приложения нажмите на кнопку **Далее.**

3. Подтверждение удаления

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

4. Завершение удаления

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

> Эта функциональность может быть недоступна в некоторых регионах.

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

5. Чтобы перезагрузить компьютер, нажмите на кнопку **Да**.

Как обновить приложение

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

Также приложение автоматически обновляется, если вы устанавливаете новую версию приложения поверх старой.

Как защитить другие устройства

Доступно только в Kaspersky Standard, Kaspersky Plus и Kaspersky Premium.

По вашей подписке вы можете защитить другие устройства на операционных системах Microsoft Windows, Android, iOS, и macOS. Пробная подписка недоступна на macOS. Количество устройств, на которых вы можете использовать подписку, определяется планом подписки и условиями Лицензионного соглашения.

Ваша подписка позволяет защищать не только ваши устройства, но и устройства ваших близких. Вы можете поделиться защитой с другими пользователями и удаленно следить за безопасностью их устройств.

В приложении в разделах **Профиль** или **Главная** вы можете посмотреть какое количество устройств вы можете защитить по вашей подписке, какое количество устройств вы защищаете, а также начать защищать новые устройства. Если ваша подписка истекла или была заблокирована, возможность добавлять новые устройства будет недоступна.

Информация обновляется при запуске приложения, если вы подключили устройство к вашему аккаунту My Kaspersky. Все ваши устройства, которые вы защищаете по подписке, должны быть также подключены к вашему аккаунту My Kaspersky.

> В зависимости от вашей подписки может быть доступна только информация об общем количестве устройств, которые вы можете защитить.

Детальную информацию о каждом устройстве и статусе его защиты можно посмотреть в вашем аккаунте My Kaspersky.

Как защитить ваше мобильное устройство

Чтобы защитить ваше мобильное устройство:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Профиль**.
3. В блоке **Защитите до N устройств** нажмите на кнопку ••• .
4. В раскрывающемся списке выберите **Защитить устройство**.
5. В открывшемся окне выберите закладку **QR-код**.
6. Отсканируйте QR-код с помощью QR-сканера вашего мобильного устройства.

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

Используя QR-код на Android-устройстве, вы соглашаетесь с передачей одноразового пароля в Google Play для активации приложения на вашем смартфоне.

Как защитить другие устройства Windows и Mac

Чтобы защитить другие ваши устройства:

1. На устройстве, которое вы хотите защитить, войдите в ваш аккаунт на сайте My Kaspersky .
2. Перейдите в раздел **Подписки** и нажмите на панель подписки.
3. Нажмите на кнопку **Защитить другое устройство** → **Новое устройство**.
4. Выберите операционную систему и приложение.
5. Скачайте приложение на ваше устройство.

   Приложение автоматически подключится к вашему аккаунту и активируется по подписке.

Вы также можете отправить ссылку на скачивание приложения по электронной почте, нажав на кнопку **Другие загрузки**.

Защита близких

Ваша подписка позволяет вам поделиться защитой с устройствами других пользователей и удаленно следить за безопасностью этих устройств. Пользователи также могут использовать приложения, входящие в состав вашей подписки.

Как владелец подписки вы сможете управлять защитой близких из своего аккаунта My Kaspersky. Например, просматривать информацию о статусе защиты устройства, удаленно запускать сканирование устройства, обновлять подписку.

У владельца подписки нет доступа к банковским картам или личной информации пользователей, с которыми он поделился защитой.

О том, как поделиться защитой с устройствами ваших близких, управлять защитой устройств удаленно, отозвать подписку у пользователя или отозвать подписку с устройства вы можете прочитать в Справке My Kaspersky .

Основные возможности приложения

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

Анализ состояния защиты компьютера и устранение проблем безопасности

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

Нажав на кнопку **Подробнее** в главном окне приложения, 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 **Статус** отображается информация о состоянии защиты компьютера и подписки на приложение. В случае обнаружения проблем, которые требуют исправления, напротив уведомления отображается кнопка **Исправить**, при нажатии на которую можно устранить возникшие проблемы безопасности.

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

В разделе **Новости** отображаются новости кибербезопасности.

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

Как исправить проблемы безопасности компьютера

Чтобы исправить проблемы безопасности компьютера:

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

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, приложение 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 приложений). 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. 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 приложения после установки.

Как включить и выключить новости безопасности

Чтобы включить или выключить новости безопасности:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки интерфейса**.

   Откроется окно **Настройки интерфейса**.
4. В блоке **Уведомления о новостях** 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:

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

   Откроется окно просмотра уведомлений.
4. По ссылке **Настройки** перейдите в окно настройки 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**.

История действий приложения и подробный отчет

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

Чтобы посмотреть историю действий приложения:

1. Откройте главное окно приложения.

   В разделе **Главная** в блоке **История** отображается краткая история действий приложения.

2. Чтобы посмотреть подробную историю действий приложения, нажмите на кнопку **Посмотреть все события**.

   Откроется окно с подробным описанием действий приложения и времени возникновения событий.

3. Чтобы посмотреть подробный отчет о работе приложения, нажмите на кнопку **Посмотреть отчет**.

   Будет выполнен переход в окно **Отчеты**.

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

Как настроить интерфейс приложения

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

Как настроить уведомления приложения

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

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

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

- *Информационные* – информируют о событиях, не имеющих первостепенной важности для обеспечения безопасности компьютера. Окна информационных уведомлений и всплывающих сообщений – зеленые.

При появлении на экране уведомления следует выбрать один из предложенных в уведомлении вариантов действия. Оптимальный вариант – тот, который рекомендован специалистами "Лаборатории Касперского" по умолчанию.

Уведомление может быть закрыто автоматически при перезагрузке компьютера, закрытии приложения Kaspersky или в режиме Connected Standby в Windows 8. Уведомления компонента Предотвращение вторжений автоматически закрываются по истечении 500 секунд. Уведомления о запуске приложения автоматически закрываются по истечении 1 часа. При автоматическом закрытии уведомления, приложение Kaspersky выполняет действие, рекомендованное по умолчанию.

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

Как настроить получение уведомлений

Чтобы создать правила уведомлений:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки интерфейса**.
4. В блоке **Уведомления** по ссылке **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 приложения в области уведомлений панели задач.

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

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

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

   Откроется окно **Настройка**.
3. Перейдите в раздел **Настройки интерфейса**.
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 подписки**, если вы хотите получать уведомления о новостях безопасности от "Лаборатории Касперского" после истечения срока действия подписки.

Как настроить сопровождение уведомлений звуковыми сигналами

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

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

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

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

Как настроить показ уведомлений при использовании приложения ребенком

Если на вашем компьютере установлено приложение Kaspersky Safe Kids, вы можете включить или выключить показ уведомлений о работе Kaspersky, когда компьютером пользуется ребенок.

Чтобы настроить показ уведомлений при использовании приложения ребенком:

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

   Откроется окно **Настройка**.
3. Перейдите в раздел **Настройки интерфейса**.

4. Выберите действие:

   - Снимите флажок **Показывать уведомления в учетной записи ребенка**, чтобы выключить показ уведомлений Kaspersky, когда компьютером пользуется ребенок.
   - Установите флажок **Показывать уведомления в учетной записи ребенка**, чтобы включить показ уведомлений Kaspersky, когда компьютером пользуется ребенок.

Подробнее о том, как настроить работу приложения Kaspersky, если компьютером пользуется ребенок.

Как сменить тему оформления приложения

Смена темы оформления приложения доступна не во всех регионах.

Чтобы сменить тему оформления приложения:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки интерфейса**.
4. В блоке **Тема оформления** выберите один из вариантов:

   - **Как в операционной системе**. Будет использована текущая тема оформления операционной системы.
   - **Светлая**. Будет использована светлая тема оформления приложения.
   - **Темная**. Будет использована темная тема оформления приложения.
5. Установите флажок **Использовать альтернативную тему оформления**, если вы хотите использовать альтернативную тему оформления. По ссылке **Выбрать** и укажите путь к zip-архиву или папке, в котором содержатся файлы с альтернативной темой оформления.

Тема оформления будет применена после перезапуска приложения.

Как настроить значок приложения

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

Как сменить значок приложения

Чтобы сменить значок приложения:

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

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

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

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

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

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

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

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

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

Как защитить доступ к управлению приложением с помощью пароля

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

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

Чтобы создать пароль администратора `KLAdmin`:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки интерфейса**.
4. Переведите переключатель **Защита паролем** в положение **Вкл**.
5. В открывшемся окне заполните поля ввода **Имя пользователя** (рекомендованное значение KLAdmin), **Введите пароль** и **Подтвердите пароль**.

   Рекомендации по созданию надежного пароля:

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

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

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

- Группа пользователей `Все`. В эту группу входят все пользователи операционной системы. Если вы выдаете разрешение на какое-либо действие для этой группы, то пользователям, входящим в эту группу, всегда будет разрешено выполнение этого действия, даже если это действие запрещено для конкретного пользователя или группы пользователей, входящих в группу `Все`. По умолчанию для группы `Все` запрещены все действия.

- `<пользователь системы>`. По умолчанию выбранному пользователю запрещены все действия. Это значит, что при попытке выполнения запрещенного действия будет запрошен ввод пароля для учетной записи `KLAdmin`.

Как добавить пользователя или группу пользователей

1. В разделе **Интерфейс** в блоке **Защита паролем** нажмите на кнопку **Добавить**.

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

2. По ссылке **Выбрать пользователя или группу** 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 **ОК**.

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**, приложение запросит ввод пароля. В окне ввода пароля укажите имя пользователя и пароль от учетной записи текущего пользователя. Действие будет выполнено, если у указанной учетной записи есть разрешение на выполнение этого действия. В окне ввода пароля вы можете указать время, в течение которого пароль не будет запрашиваться повторно.

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

Как восстановить стандартные настройки приложения

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

Чтобы восстановить стандартные настройки приложения:

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

   Откроется окно **Настройка**.

3. Выберите раздел **Управление настройками**.

4. По ссылке **Восстановить** запустите мастер восстановления настроек.

5. Нажмите на кнопку **Далее**.

   В окне мастера отобразится процесс восстановления настроек работы приложения до тех, которые заданы специалистами "Лаборатории Касперского" по умолчанию.

6. После того как процесс восстановления стандартных настроек работы приложения будет завершен, нажмите на кнопку **Готово**.

Как применить настройки приложения на другом компьютере

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

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

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

1. Сохранение настроек приложения Kaspersky в конфигурационном файле.

2. Перенос конфигурационного файла на другой компьютер (например, по электронной почте или на внешнем диске).

3. Импорт настроек из конфигурационного файла в приложение Kaspersky, установленное на другом компьютере.

Как экспортировать настройки

Чтобы экспортировать настройки Kaspersky:

1. Откройте главное окно приложения.

2. Нажмите на кнопку в нижней части главного окна.

   Откроется окно **Настройка**.

3. В окне **Настройка** выберите раздел **Управление настройками**.

4. Выберите элемент **Экспортировать**.

5. Откроется окно **Сохранение**.

6. Задайте имя конфигурационного файла и нажмите на кнопку **Сохранить**.

   Настройки приложения будут сохранены в конфигурационный файл.

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

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

Как импортировать настройки

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

1. Откройте главное окно приложения Kaspersky, установленного на другом компьютере.

2. Нажмите на кнопку в нижней части окна.

   Откроется окно **Настройка**.

3. В окне **Настройка** выберите раздел **Управление настройками**.

4. Выберите элемент **Импортировать**.

   Откроется окно **Открыть**.

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

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

Как приостановить и возобновить защиту компьютера

Приостановка защиты означает выключение на некоторое время всех ее компонентов.

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

Чтобы приостановить защиту компьютера:

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

   Откроется окно **Приостановка защиты**.

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

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

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

Как возобновить защиту компьютера

Чтобы возобновить защиту компьютера,

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

Оценка работы приложения

Вы можете отправить в "Лабораторию Касперского" вашу оценку работы нашего приложения.

По истечении некоторого времени с момента установки приложение предлагает вам оценить его работу.

Чтобы оценить работу приложения:

1. В окне **Нам важно ваше мнение** выполните одно из следующих действий:

    - Если вы готовы оценить работу приложения, поставьте оценку по 10-балльной шкале.

    - Если вы не хотите оценивать работу приложения, нажмите на кнопку ✕, чтобы закрыть окно оценки.

2. Нажмите на кнопку **Отправить**.

3. Нажмите на кнопку **Закрыть**, чтобы закрыть окно.

Какие данные передаются при отправке оценки

Вместе с оценкой приложения "Лаборатории Касперского" обрабатывает следующую информацию, необходимую для анализа опроса:

- название и версия приложения "Лаборатории Касперского";

- версия операционной системы;

- регион активации и язык интерфейса приложения "Лаборатории Касперского";

- период пользования приложения "Лаборатории Касперского".

Безопасность

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

Проверка компьютера

Во время проверки приложение ищет зараженные файлы и вредоносные приложения. 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 внешних дисков. Проверка внешних дисков, например, жестких дисков и USB-флешек, подключенных к компьютеру.
- Проверка из контекстного меню. Проверка файлов через контекстное меню.
- Фоновая проверка. Проверка системной памяти, системного раздела, загрузочных секторов и объектов автозапуска, а также поиск руткитов.
- Поиск уязвимостей в приложениях. Проверка компьютера на наличие уязвимостей в приложениях, через которые способны проникнуть вредоносные приложения.

После установки приложения мы рекомендуем выполнить полную проверку компьютера.

Как запустить быструю проверку

Во время быстрой проверки приложение по умолчанию проверяет следующие объекты:

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

Чтобы запустить быструю проверку:

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

Приложение начнет быструю проверку компьютера.

Как запустить полную проверку

Во время полной проверки по умолчанию приложение проверяет следующие объекты:

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

Рекомендуется выполнить полную проверку сразу после установки приложения на компьютер.

Чтобы запустить полную проверку:

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

   Откроется окно **Проверка**.
3. В окне **Проверка** выберите раздел **Полная проверка**.
4. В раскрывающемся списке рядом с кнопкой **Запустить проверку** выберите действие по окончании проверки.
5. Нажмите на кнопку **Запустить проверку**.

Приложение начнет полную проверку компьютера.

Как запустить выборочную проверку

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

Чтобы запустить выборочную проверку:

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

   Откроется окно **Проверка**.
4. В окне **Проверка** выберите раздел **Выборочная проверка**.

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

6. Нажмите на кнопку **Запустить проверку**.

Как запустить проверку внешних дисков

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

Чтобы проверить внешний диск вручную:

1. Откройте главное окно приложения.

2. Перейдите в раздел **Безопасность**.

3. В блоке **Проверка** нажмите на кнопку **Выбрать проверку**.

   Откроется окно **Проверка**.

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

5. В раскрывающемся списке выберите внешнее устройство (отображается в виде буквы латинского алфавита) и нажмите на кнопку **Запустить проверку**.

Приложение начнет проверку подключенного устройства.

Как запустить проверку файла или папки из контекстного меню

Чтобы запустить проверку файла или папки из контекстного меню:

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

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

Приложение начнет проверку выбранного файла или папки.

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

Как включить или выключить фоновую проверку

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

Фоновая проверка запускается в следующих случаях:

- после обновления баз и модулей приложения;
- через 30 минут после запуска приложения;
- каждые шесть часов;
- если компьютер не используется в течение пяти и более минут (запущена экранная заставка).

Фоновая проверка прерывается при выполнении любого из следующих условий:

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

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

Чтобы включить или выключить фоновую проверку:

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

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

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

Как создать расписание проверки

Чтобы создать расписание проверки:

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

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

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

Как выполнить поиск уязвимостей в приложениях, установленных на вашем компьютере

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

Чтобы запустить поиск уязвимостей в приложениях:

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

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

Приложение начнет проверку вашего компьютера на наличие уязвимостей в приложениях.

Как исключить файл, папку или тип угрозы из проверки

Чтобы исключить файл, папку или тип угрозы из проверки:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки безопасности** → **Угрозы и исключения**.
4. По ссылке **Настроить исключения** откройте окно **Исключения**.
5. Нажмите на кнопку **Добавить**.
6. Добавьте исключение одним из следующих способов:

   - Нажмите **Обзор** и выберите папку или файл, который вы хотите исключить из проверки. Нажмите на кнопку **Выбрать**.
   - В поле **Файл или папка** введите полное имя или маску имени файла или папки вручную.
   - В поле **Объект** введите полное имя или маску имени типа угрозы по классификации детектируемых объектов "Лаборатории Касперского".
   - Заполните оба поля: **Файл или папка** и **Объект**, чтобы приложение не проверяло в выбранном файле или папке указанный тип угрозы.
   - В поле **Хеш файла** укажите хеш сумму, если вы хотите, чтобы файлы исключались из проверки по хеш сумме.
7. Снимите флажки с компонентов защиты, для которых не будет действовать правило исключения. При желании укажите свой комментарий.
8. Выберите статус правила **Активно** и нажмите на кнопку **Добавить**.

Указанные объекты будут исключены из проверки.

Подробнее о настройках в окне Угрозы и исключения

Проверка файлов в облачном хранилище OneDrive

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

Следующие компоненты не проверяют файлы в облачном хранилище OneDrive:

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

Отчет о работе приложения содержит список файлов в облачном хранилище OneDrive, пропущенных во время проверки.

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

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

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

Обновление антивирусных баз и модулей приложения

Этот раздел содержит информацию об обновлении баз и модулей приложения.

Об обновлении антивирусных баз и модулей приложения

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

- Приложение обнаруживает большинство угроз с помощью Kaspersky Security Network, для чего требуется подключение к интернету.

- Приложение обнаруживает рекламные приложения, приложения автодозвона и другие легальные приложения, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

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

Обновление баз и модулей приложения выполняется поэтапно:

1. Приложение запускает обновление баз и модулей приложения согласно указанным настройкам: автоматически, по расписанию или по вашему требованию. Приложения обращается к источнику обновлений, где хранится пакет обновлений антивирусных баз и модулей приложения.

2. Приложение сравнивает имеющиеся базы с базами, находящимися в источнике обновлений. Если базы отличаются, приложение скачивает отсутствующие части баз.

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

Источники обновлений

Вы можете использовать следующие источники обновлений:

- Серверы обновлений "Лаборатории Касперского".

- HTTP или FTP-сервер.

- Сетевая папка.

Особенности обновления антивирусных баз и модулей приложения

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

- Антивирусные базы устаревают по истечении одного дня и сильно устаревают по истечении семи дней.

- Для скачивания пакета обновлений с серверов обновлений "Лаборатории Касперского" требуется соединение с интернетом.

- Обновление антивирусных баз и модулей приложения недоступно в следующих случаях:

- Истек срок действия 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 антивирусных баз и модулей приложения, требуется снять флажок **Ограничивать трафик при лимитном подключении** в окне **Настройка → Настройки безопасности → Расширенные настройки → Настройки сети**.

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

Установка пакета исправлений

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

Как запустить обновление баз и модулей приложения

Чтобы запустить обновление баз и модулей приложения:

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

Предотвращение вторжений

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

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

О Предотвращении вторжений

Доступно только в Kaspersky Standard, Kaspersky Plus и Kaspersky Premium.

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

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

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

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

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

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

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

Сетевую активность приложений контролирует компонент Сетевой экран.

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

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

Вы можете изменить правила контроля действий приложения вручную.

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

Как изменить настройки Предотвращения вторжений

Доступно только в Kaspersky Standard, Kaspersky Plus и Kaspersky Premium.

Чтобы изменить настройки Предотвращения вторжений:

1. Откройте главное окно приложения.

2. Нажмите на кнопку  в нижней части главного окна.

   Откроется окно **Настройка**.

3. Выберите раздел **Настройки безопасности**.

4. Выберите компонент **Предотвращение вторжений**.

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

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

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

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

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

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

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

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

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

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

      Откроется окно **Сетевое правило**.

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

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

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

11. Нажмите на кнопку **Сохранить**.

    Все исключения, созданные в правилах Предотвращения вторжений, доступны в окне настройки приложения Kaspersky в разделе **Угрозы и исключения**.

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

Проверка репутации приложения

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

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

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

Чтобы узнать репутацию приложения,

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

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

О защите аудиосигнала, поступающего с устройств записи звука

Доступно только в Kaspersky Standard, Kaspersky Plus и Kaspersky Premium.

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

По умолчанию приложениям из групп доверия "Недоверенные" и "Сильные ограничения" запрещено получать аудиосигнал, поступающий с подключенных к компьютеру устройств записи звука. Вы можете вручную разрешать приложениям получать аудиосигнал с устройств записи звука.

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

Для всех приложений, 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 Предотвращение вторжений.
- При изменении настроек доступа приложения к устройствам записи звука (например, приложению было запрещено получение аудиосигнала в окне настроек Предотвращения вторжений), чтобы приложение перестало получать аудиосигнал, требуется перезапуск этого приложения.
- Контроль получения аудиосигнала с устройств записи звука не зависит от настроек доступа приложения к веб-камере.
- Приложение Kaspersky защищает доступ только к встроенным микрофонам и внешним микрофонам. Другие устройства передачи звука не поддерживаются.
- Приложение Kaspersky разрешает приложению получение аудиосигнала и не показывает никаких уведомлений, если приложение начало получать аудиосигнал до запуска

приложения Kaspersky, или если вы поместили приложение в группу "Недоверенные" или "Сильные ограничения" после того, как приложение начало получать аудиосигнал.

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

Как изменить настройки защиты аудиосигнала

Доступно только в Kaspersky Standard, Kaspersky Plus и Kaspersky Premium.

Чтобы изменить настройки защиты аудиосигнала:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Безопасность**.
3. Выберите компонент **Предотвращение вторжений**.
4. По ссылке **Управлять приложениями** откройте окно **Управление приложениями**.
5. Выберите приложение в списке, которому вы хотите разрешить доступ к устройствам записи звука, и откройте окно **Правила приложения** двойным щелчком мыши.
6. В окне **Правила приложения** перейдите на закладку **Права**.
7. В списке категорий прав выберите пункт **Изменение операционной системы** → **Подозрительные изменения в операционной системе** → **Доступ к устройствам записи звука**.
8. В графе **Действие** нажмите на значок и выберите один из пунктов меню:
   - Чтобы разрешить приложению получение аудиосигнала, выберите пункт **Разрешить**.
   - Чтобы запретить приложению доступ к аудиосигналу, выберите пункт **Запретить**.
9. Если вы хотите получать уведомления о том, что приложению был запрещен или разрешен доступ к аудиосигналу, в графе **Действие** нажмите на значок и выберите пункт **Записывать в отчет**.
10. Нажмите на кнопку **Сохранить**.

Поиск 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 приложений, 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.

Приложение по умолчанию выполняет поиск небезопасных настроек операционной системы не реже чем раз в день. Если приложение обнаружило 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 **Поиск 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 **Поиск 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.

Приложение 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.

Как найти и исправить небезопасные настройки операционной системы

Чтобы найти и исправить небезопасные настройки операционной системы:

1. Откройте главное окно приложения.
2. Выберите раздел **Безопасность**.
3. В разделе **Безопасность** выберите блок **Поиск небезопасных настроек**.
4. Нажмите на кнопку **Проверить**.

   Будет выполнен поиск небезопасных настроек. По окончании поиска в блоке **Поиск небезопасных настроек** отобразится информация о результатах поиска.
5. Нажмите на кнопку **Посмотреть**, чтобы перейти в окно **Поиск небезопасных настроек**.
6. В окне **Поиск 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 приложения, нажмите на кнопку **Посмотреть**, чтобы ознакомиться со списком мешающих приложений.

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

       - Нажмите на кнопку ✕ справа от названия мешающего приложения, чтобы закрыть приложение в штатном режиме. Если приложение обнаружит

несохраненные изменения, оно предложит сохранить их.

- Нажмите на ссылку **Закрыть принудительно**, чтобы закрыть все мешающие приложения 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**.

Как включить поиск небезопасных настроек операционной системы

Чтобы выключить поиск небезопасных настроек операционной системы:

1. Откройте главное окно приложения.

2. Нажмите на кнопку  в нижней части главного окна.

   Откроется окно **Настройка**.

3. Перейдите в раздел **Настройки производительности**.

4. Нажмите на кнопку **Потребление ресурсов компьютера**.

5. Снимите флажок **Выполнять поиск небезопасных настроек операционной системы**.

Приложение не будет выполнять поиск небезопасных настроек операционной системы и показывать уведомления о них.

Мониторинг сети

Доступно только в Kaspersky Standard, Kaspersky Plus и Kaspersky Premium.

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

Чтобы перейти к настройке Мониторинга сети:

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

Откроется окно **Мониторинг сети**.

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

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

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

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

Восстановление компьютера

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

О восстановлении операционной системы после заражения

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

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

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

Восстановление операционной системы с помощью мастера восстановления

Чтобы запустить мастер восстановления после заражения:

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

   Откроется окно мастера восстановления после заражения.

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

Рассмотрим подробнее шаги мастера.

Запуск восстановления операционной системы

a. Выберите один из двух вариантов работы мастера:

- **Выполнить поиск повреждений, связанных с активностью вредоносных приложений**. Мастер выполнит поиск проблем и возможных повреждений.

- **Отменить изменения**. Мастер отменит исправления ранее выявленных проблем и повреждений.

b. Нажмите на кнопку **Далее**.

Поиск проблем

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

Выбор действий для устранения повреждений

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

Всего выделено три группы:

- *Настоятельно рекомендуемые действия* помогут избавиться от повреждений, представляющих серьезную проблему. Рекомендуем вам устранить все повреждения из этой группы.

- *Рекомендуемые действия* направлены на устранение повреждений, которые могут представлять опасность. Повреждения из этой группы также рекомендуется устранить.

- *Дополнительные действия* предназначены для устранения неопасных в данный момент повреждений операционной системы, которые в дальнейшем могут поставить безопасность компьютера под угрозу.

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

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

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

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

Устранение повреждений

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

Завершение работы мастера

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

Об аварийном восстановлении операционной системы

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

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

Как восстановить удаленный или вылеченный файл

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

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

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

Чтобы восстановить удаленный или вылеченный файл:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Безопасность**.
3. Нажмите на кнопку **Карантин** в правом верхнем углу окна Kaspersky.

Откроется окно **Карантин**.

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

Защита электронной почты

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

Настройка Почтового Антивируса

Приложение Kaspersky 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:

1. Откройте главное окно приложения.

2. Нажмите на кнопку  в нижней части главного окна.

   Откроется окно **Настройка**.

3. Выберите блок **Настройки безопасности**.

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

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

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

6. Выберите уровень безопасности:

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

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

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

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

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

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

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

Блокирование нежелательной почты (спама)

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

Чтобы включить Анти-Спам и установить уровень безопасности Оптимальный:

1. Откройте главное окно приложения.

2. Нажмите на кнопку  в нижней части главного окна.

   Откроется окно **Настройка**.

3. Выберите раздел **Настройки приватности**.

4. Выберите компонент Анти-Спам.

В окне отобразятся настройки Анти-Спама.

5. Включите Анти-Спам с помощью переключателя.

6. Убедитесь, что в блоке **Уровень безопасности** установлен уровень безопасности **Оптимальный**.

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 приложения компонент Анти-Спам выключается. Вы можете включить компонент вручную.

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

Участие в Kaspersky Security Network

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

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

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

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

Как включить и выключить участие в Kaspersky Security Network

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

Чтобы включить или выключить участие в Kaspersky Security Network:

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

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

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

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

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

В некоторых версиях приложения Kaspersky вместо информации о Kaspersky Security Network в окне **Kaspersky Security Network** отображается **Положение о Kaspersky Security Network**.

Чтобы принять Положение о Kaspersky Security Network:

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

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

Чтобы отказаться от Положения о Kaspersky Security Network,

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

Как проверить подключение к Kaspersky Security Network

Подключение к Kaspersky Security Network может отсутствовать по следующим причинам:

- Вы не участвуете в Kaspersky Security Network.
- Ваш компьютер не подключен к интернету.
- Текущий статус ключа не позволяет осуществить подключение к Kaspersky Security Network. Например, подключение к KSN может отсутствовать по следующим причинам:
  - Приложение не активировано.
  - Срок действия лицензии или подписки истек.
  - Выявлены проблемы, связанные с лицензионным ключом (например, ключ попал в список запрещенных ключей).

> Текущий статус ключа отображается на My Kaspersky.

Чтобы проверить подключение к Kaspersky Security Network:

1. Откройте главное окно приложения.
2. Выберите раздел **Настройки безопасности** → **Kaspersky Security Network**.

В окне **Kaspersky Security Network** 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

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

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

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

- Функциональность недоступна при запуске гипервизора сторонним приложением, например, приложения для виртуализации компании VMware. После завершения работы гипервизора стороннего приложения функциональность защиты от создания снимков экрана снова становится доступной.

- Функциональность недоступна, если центральный процессор вашего компьютера не поддерживает технологию аппаратной виртуализации. Уточнить, поддерживает ли процессор вашего компьютера технологию аппаратной виртуализации, можно в технической документации для вашего компьютера или на сайте производителя процессора.

- Функциональность недоступна, если в момент запуска Защищенного браузера обнаружен работающий гипервизор стороннего приложения, например, приложения компании VMware.

- Функциональность недоступна, если на вашем компьютере выключена аппаратная виртуализация. Уточнить, как включить аппаратную виртуализацию на вашем компьютере, можно в технической документации для вашего компьютера или на сайте производителя процессора.

- Функциональность недоступна, если на операционной системе Microsoft Windows 10 включен режим Device Guard.

- Функциональность недоступна, если на операционной системе Microsoft Windows 10 включен режим Virtualization Based Security (VBS).

Как включить защиту с помощью аппаратной виртуализации

Чтобы включить защиту с помощью аппаратной виртуализации:

1. Откройте главное окно приложения.

2. Нажмите на кнопку  в нижней части главного окна.

Откроется окно **Настройка**.

3. Выберите раздел **Безопасность** → **Защита ввода данных**.

4. Установите флажок **Использовать аппаратную виртуализацию, если она доступна**. Флажок отображается в 64-разрядной версии Windows 8, Windows 8.1 и Windows 10.

5. Установите флажок **Использовать расширенные возможности аппаратной виртуализации**, если вы хотите, чтобы аппаратная виртуализация включалась при запуске операционной системы.

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

Защита с помощью Antimalware Scan Interface (AMSI)

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

О защите с помощью Antimalware Scan Interface

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

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

Приложение Kaspersky может отклонить запрос от стороннего приложения, например, если это приложение превысило максимальное количество запросов за промежуток времени. В этом случае приложение Kaspersky 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:

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

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

Как исключить скрипт из проверки с помощью Antimalware Scan Interface

Чтобы исключить скрипт из проверки с помощью Antimalware Scan Interface:

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

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

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

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

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

Удаленное управление защитой компьютера

Если на компьютере установлено приложение Kaspersky и компьютер подключен к My Kaspersky, вы можете управлять защитой этого компьютера удаленно.

Чтобы удаленно управлять защитой компьютера, вам нужно войти в свой аккаунт My Kaspersky 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 приложения, представляющие угрозу;
- обновлять базы и модули приложения;
- настраивать компоненты приложения Kaspersky.

Если проверка компьютера запущена из My Kaspersky, то Kaspersky обрабатывает обнаруженные объекты в автоматическом режиме без вашего участия. В случае обнаружения вируса или другого приложения, представляющего угрозу, приложение Kaspersky 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 приложения, установленного на компьютере.

Как перейти к удаленному управлению защитой компьютера

Чтобы перейти к удаленному управлению защитой компьютера:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Профиль**.
3. В блоке **Войти в My Kaspersky** нажмите на кнопку **Войти**.
4. В открывшемся окне выполните одно из следующих действий:

- Если у вас есть аккаунт, укажите адрес электронной почты и пароль и подключитесь к My Kaspersky.

- Если у вас нет аккаунта, укажите адрес электронной почты в поле ввода и нажмите на кнопку **Создать**. Письмо со ссылкой для создания пароля будет отправлено на указанный адрес электронной почты.

После успешного подключения в разделе **Профиль** отобразится информация о том, что вы подключены к аккаунту. Теперь защитой компьютера можно управлять удаленно из вашего аккаунта на My Kaspersky.

Подробнее о том, как управлять защитой устройств удаленно, вы можете прочитать в Справке My Kaspersky.

Производительность

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

Быстрый запуск

Ваш компьютер загружается слишком медленно? Обычно это происходит, если при старте операционной системы запускается много приложений. Мы расскажем вам, какие приложения тормозят компьютер при старте и поможем выключить их автозапуск.

Чтобы ускорить загрузку компьютера:

1. Откройте главное окно приложения.

2. Перейдите в раздел **Производительность**.

3. Нажмите на кнопку **Показать приложения** в блоке **Быстрый запуск**.

   Откроется окно **Ускорить запуск компьютера**, в котором представлен список приложений, которые запускаются при запуске.

   В графе **Влияние на запуск** отображается информация о том, какое влияние каждое приложение оказывает на запуск компьютера. Эта информация берется из операционной системы и зависит от того, какое количество ресурсов компьютера (загрузка процессора и объем оперативной памяти) потребляет приложение.

4. Выберите приложение из списка и в графе **Автозапуск** переведите переключатель в положение **Выкл**.

Приложение больше не будет запускаться при загрузке компьютера.

Ускорить работу

Со временем в операционной системе скапливается всякий мусор, который приводит к замедлению работы компьютера: большое количество лишних файлов и неполадок реестра Windows. Приложение Kaspersky подскажет, если таких данных слишком много, а вы сами решите, что удалить.

Чтобы очистить операционную систему от мусора:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Производительность**.
3. В блоке **Ускорить работу** нажмите на кнопку **Найти** (или **Посмотреть**, если поиск уже выполнялся).

   Приложение выполнит поиск и предоставит вам отчет следующего содержания:

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

Очистка и исправление найденных проблем ускорят работу вашего компьютера.

Обновление приложений

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

Доступно только в Kaspersky Standard, Kaspersky Plus и Kaspersky Premium.

Об обновлении приложений

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

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

Приложение Kaspersky подразделяет обновления приложений на два типа:

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

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

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

Вы также можете запустить поиск обновлений для приложений вручную.

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

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

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

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

Перед первым поиском обновлений для приложений, может потребоваться обновление баз и модулей приложения Kaspersky.

Поиск обновлений для приложений

Чтобы запустить поиск обновлений для приложений:

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

Запустится поиск обновлений для приложений.

Как изменить настройки Обновления приложений

Чтобы изменить настройки Обновления приложений:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки производительности**.
4. Нажмите на кнопку **Обновление приложений**.

   Откроется окно **Настройки Обновления приложений**.
5. Если вы не хотите, чтобы приложение Kaspersky автоматически скачивало и устанавливало обновления приложений, для которых не требуется принимать новое лицензионное соглашение, снимите флажок **Автоматически скачивать и устанавливать обновления, если не требуется принимать новое лицензионное соглашение**.

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

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

Как настроить режим поиска обновлений

Чтобы настроить режим поиска обновлений для установленных приложений:

1. Откройте главное окно приложения.

2. Нажмите на кнопку  в нижней части главного окна.

   Откроется окно **Настройка**.

3. Выберите раздел **Настройки производительности**.

4. Нажмите на кнопку **Обновление приложений**.

   Откроется окно **Настройки обновления приложений**.

5. В блоке **Обновление** установите флажок **Включить поиск обновлений для приложений**.

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, приложение Kaspersky будет выполнять поиск обновлений для приложений минимум раз в сутки согласно внутренним настройкам приложения.

   - **По дням** / **Еженедельно** / **Ежемесячно**. Если вы выберете один из этих пунктов, приложение Kaspersky будет запускать поиск обновлений по заданному вами расписанию, с точностью до минуты. При выборе одного из этих вариантов доступен список **Отложить запуск после старта приложения на N минут**.

8. Установите флажок **Запускать поиск обновлений на следующий день, если компьютер был выключен**, чтобы запускать поиск после включения компьютера в случае пропуска запланированного времени поиска. Если флажок не установлен, приложение будет запускать поиск обновлений только в заданное по расписанию время, когда компьютер включен.

9. Нажмите на кнопку **Сохранить**, чтобы сохранить настройки.

Просмотр списка обновлений для приложений

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

Чтобы просмотреть список, сформированный в результате поиска обновлений приложений:

1. Откройте главное окно приложения.

2. Нажмите на кнопку **Подробнее** в верхней части окна.

Откроется окно **Центр уведомлений**.

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

   Откроется окно **Обновление приложений**, которое содержит список найденных обновлений для приложений.

4. Если вы хотите обновить все приложения, которые отображаются в списке, нажмите на кнопку **Обновить все** (доступно не во всех регионах).

5. Если вы хотите принять решение по каждому приложению, которую предлагается обновить, выполните одно из следующих действий:

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

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

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

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

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

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

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

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

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

Удаление обновления или приложения из списка исключений

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

Чтобы удалить обновление или приложение из списка исключений:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки производительности**.
4. Нажмите на кнопку **Обновление приложений**.

   Откроется окно **Настройки обновления приложений**.
5. По ссылке **Исключения** откройте окно **Исключения**.

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

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

Дубликаты файлов

На компьютере могут храниться файлы с одинаковым названием и одинаковым содержимым. Такие дубликаты засоряют память, съедают свободное место и замедляют компьютер. С помощью функциональности Дубликаты файлов, вы можете найти такие файлы и удалить лишнюю копию.

Чтобы удалить дубликаты:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Производительность**.
3. В блоке **Дубликаты файлов** в раскрывающемся списке укажите область поиска.
4. Нажмите на кнопку **Найти**.
5. В окне с результатами поиска выберите файлы и нажмите на кнопку **Удалить**.

Дубликаты будут удалены с вашего компьютера, а исходные данные останутся.

Большие файлы

Вы сохраняете данные на компьютер, но вдруг обнаруживаете, что на диске не хватает свободного места. Знакомая ситуация? В этом случае вы, возможно, захотите найти и удалить большие ненужные файлы, а мы поможем вам в этом.

Чтобы найти и удалить большие файлы с компьютера:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Производительность**.
3. В блоке **Большие файлы** в раскрывающемся списке **Файлы размером более** укажите размер файлов, которые вы хотите обнаруживать, например, **> 1 ГБ**.
4. Укажите папку для поиска или оставьте значение по умолчанию **Папки пользователя**.
5. Нажмите на кнопку **Найти**.

   Будет выполнен поиск больших файлов, по окончании которого откроется окно **Большие файлы**. В списке отобразятся найденные большие файлы. Вы можете отсортировать файлы по типу: для этого выберите категорию файлов, например, **Изображения**.
6. Выполните следующие действия:

   - Установите флажок **Выбрать все**, если вы хотите удалить все файлы и нажмите на кнопку **Удалить**.
   - Установите флажки напротив конкретных файлов и нажмите на кнопку **Удалить**.

   Выбранные файлы будут удалены с вашего компьютера.

Неиспользуемые приложения

На скорость работы вашего компьютера влияет несколько факторов, в том числе количество установленных приложений. Чем больше приложений установлено, тем медленнее работает компьютер. Это связано с тем, что некоторые приложения, в том числе установленные без вашего ведома, могут запускаться самостоятельно, потреблять ресурсы процессора и оперативную память, а также выполнять ненужные и даже вредоносные действия.

Приложение Kaspersky поможет вам найти и удалить такие приложения.

Чтобы удалить неиспользуемые приложения:

1. Откройте главное окно приложения Kaspersky.
2. Перейдите в раздел **Производительность**.
3. Нажмите на кнопку **Найти** в блоке **Неиспользуемые приложения**.

   После окончания поиска приложение Kaspersky покажет вам список неиспользуемых приложений. В списке вы можете самостоятельно выбрать, какие приложения вы хотите удалить, а какие оставить.
4. Чтобы удалить приложение, нажмите на кнопку **Удалить** напротив этого приложения.

Приложение будет удалено с вашего компьютера.

Диагностика жесткого диска

Этот раздел содержит информацию о том, как проверить состояние жесткого диска вашего компьютера или подключенного внешнего жесткого диска с помощью приложения Kaspersky.

О диагностике жесткого диска

Доступно только в Kaspersky Plus и Kaspersky Premium.

Неожиданный выход из строя жесткого диска может привести к потере данных, хранящихся на этом жестком диске. С помощью приложения Kaspersky 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 приложения Kaspersky 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, приложение Kaspersky 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, приложение Kaspersky 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 приложение Kaspersky больше не уведомляет вас об изменениях состояния ваших жестких дисков и не предлагает вам скопировать данные с поврежденных дисков на другие носители.

Как включить и выключить диагностику жесткого диска

Чтобы включить или выключить диагностику жесткого диска:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки производительности** → **Потребление ресурсов компьютера**.
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

Приложение Kaspersky 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, приложение 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 приложение Kaspersky 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:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Производительность**.
3. В разделе **Позаботьтесь о жестком диске и данных** выполните одно из следующих действий:

- Если вы хотите просмотреть график, нажмите на кнопку **История**.
- Если вы хотите просмотреть отчет, нажмите на кнопку **Подробнее**.

Будет выполнен переход в окно, в котором вы можете более детально ознакомиться с состоянием жесткого диска.

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, приложение Kaspersky 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:

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:

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 приложение уведомило 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 приложение Kaspersky 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.

- Приложение Kaspersky не поддерживает:

  - тип подключенного жесткого диска;

  - тип USB-контроллера жесткого диска.

- Жесткий диск отключен.
- Жесткий диск принадлежит виртуальной машине, например, VMWare. Данные о состоянии таких дисков или не отображаются, или отображаются некорректно.

Резервное копирование данных

Этот раздел содержит информацию о резервном копировании данных.

О резервном копировании данных

Доступно только в Kaspersky Plus и Kaspersky Premium.

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

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

Сохранять резервные копии данных рекомендуется на внешних дисках или в Онлайн-хранилище.

> Приложение Kaspersky не может создавать полную копию диска с активной операционной системой Microsoft Windows.

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

- локальный диск;
- внешний 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 приложение Kaspersky действует по-разному в зависимости от того, скачан ли облачный файл в папку OneDrive:

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

Как создать задачу резервного копирования

Чтобы создать задачу резервного копирования:

1. Откройте главное окно приложения.
2. Выберите раздел **Производительность**.
3. В блоке **Резервное копирование** нажмите на кнопку **Выбрать файлы**.

   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".

  > Приложение Kaspersky 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 приложения.

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, приложение Kaspersky 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.

- **Внешний диск**. Если вы хотите хранить резервные копии на внешнем диске, выберите нужный внешний диск в списке.

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

Как добавить сетевое хранилище

Чтобы добавить сетевое хранилище:

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 внешний диск в качестве хранилища

Чтобы добавить внешний диск в качестве хранилища резервных копий:

1. По ссылке **Подключить имеющееся хранилище** откройте окно **Подключение хранилища**.

2. Выберите раздел **Внешний диск**.

3. Нажмите на кнопку **Обзор** и в открывшемся окне укажите внешний 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 Windows на этом компьютере. Данные учетной записи Windows 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 приложение запускало резервное копирование при первой возможности после включения компьютера. 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.

Приложение запрашивает у вас ввод пароля в следующих случаях:

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

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

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

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 настройки**, 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:

1. Откройте главное окно приложения.
2. Выберите раздел **Производительность**.
3. В блоке **Резервное копирование** нажмите на кнопку **Посмотреть мои резервные копии**.
4. 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:

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

   Откроется окно **Резервное копирование**.

   - 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**.

4. Если при создании резервной копии был задан пароль, укажите этот пароль в окне **Введите пароль для доступа к хранилищу**.

5. В раскрывающем списке **Дата / время копирования** выберите дату и время создания резервной копии.

6. 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**.

7. Если вы хотите восстановить только определенные типы файлов, в раскрывающемся списке **Тип файлов** выберите эти типы файлов.

8. Нажмите на кнопку **Восстановить выбранные файлы**.

   Откроется окно **Восстановление файлов из резервных копий**.

9. Выберите один из двух вариантов:

   - **В исходную папку**. Если выбран этот вариант, приложение восстанавливает данные в исходную папку.

   - **В указанную папку**. Если выбран этот вариант, приложение восстанавливает данные в указанную папку. Нажмите на кнопку **Обзор**, чтобы выбрать папку, в которую вы хотите восстановить данные.

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

    - **спрашивать** – приложение при совпадении имен файлов предлагает выбрать один из вариантов: заменить файл резервной копией, сохранить оба файла или не восстанавливать этот файл.

    - **заменить файл резервной копией** – приложение Kaspersky удаляет существующий файл и помещает на его место файл, восстановленный из резервной копии.

- **сохранить оба файла** – приложение Kaspersky оставляет существующий файл без изменений и сохраняет файл, восстановленный из резервной копии, под новым именем в этой же папке.

- **не восстанавливать этот файл** – приложение Kaspersky оставляет существующий файл без изменений, не восстанавливая одноименный файл из резервной копии.

11. Нажмите на кнопку **Восстановить**.

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

Восстановление данных из FTP-хранилища

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

Чтобы восстановить резервные копии из FTP-хранилища:

1. Откройте главное окно приложения.

2. Выберите раздел **Производительность**.

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

   Откроется окно **Резервное копирование**.

4. По ссылке **Управление хранилищами** откройте окно **Хранилища**.

5. Откройте в проводнике папку FTP-хранилища.

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

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

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

   Хранилище будет удалено.

9. В окне **Управление хранилищами** нажмите на кнопку **Подключить имеющееся хранилище**.

10. 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.

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

12. Следуйте стандартной процедуре восстановления.

Восстановление данных из резервной копии с помощью Kaspersky Restore Utility

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

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

Как запустить утилиту восстановления

Чтобы запустить утилиту восстановления:

1. Откройте внешний 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 приложении. Вы можете указать путь к другому хранилищу.

Как открыть хранилище с помощью утилиты восстановления

Чтобы открыть хранилище с помощью утилиты восстановления:

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:

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 должно выполнять приложение, если в папке, куда требуется поместить восстановленный файл, уже находится файл с таким же именем:
   - **спрашивать** – приложение при совпадении имен файлов предлагает выбрать один из вариантов: заменить файл резервной копией, сохранить оба файла или не восстанавливать этот файл.
   - **заменить файл резервной копией** – приложение Kaspersky удаляет существующий файл и помещает на его место файл, восстановленный из резервной копии.

- **сохранить оба файла** – приложение Kaspersky оставляет существующий файл без изменений и сохраняет файл, восстановленный из резервной копии, под новым именем в этой же папке.

- **не восстанавливать этот файл** – приложение Kaspersky 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

Приложение Kaspersky 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 установлено приложение Kaspersky.

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

Как активировать Онлайн-хранилище

Чтобы активировать Онлайн-хранилище:

1. Откройте главное окно приложения.
2. Выберите раздел **Производительность**.
3. В блоке **Резервное копирование** нажмите на кнопку **Выбрать файлы**.

   Будет запущен мастер создания задачи резервного копирования.
4. В окне выбора типа данных выберите категорию данных или вручную укажите файлы, для которых нужно создавать резервные копии.
5. 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.
6. В открывшемся окне выполните одно из следующих действий:

   - Если вы не зарегистрированы на сайте Dropbox, пройдите процедуру регистрации.
   - Если вы зарегистрированы на сайте Dropbox, войдите в учетную запись Dropbox.
7. Для завершения активации Онлайн-хранилища подтвердите, что приложение Kaspersky может использовать вашу учетную запись Dropbox для резервного копирования данных и восстановления данных из резервной копии. Приложение Kaspersky 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 приложение Kaspersky не учитывает регистр в названии файла и / или названии пути к этому файлу. При попытке создания резервных копий файлов, названия и / или пути которых отличаются только регистром, приложение Kaspersky создает только одну резервную копию, так как в Dropbox возникает конфликт регистров.

Текущая активность

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

Чтобы просмотреть текущую активность и / или завершить работу приложения:

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

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

Работа приложения будет завершена.

Режим "Не беспокоить"

В режиме "Не беспокоить" приложение Kaspersky не показывает всплывающие уведомления о событиях, произошедших на вашем компьютере, когда вы работаете, учитесь, общаетесь по видеосвязи или смотрите фильм. Режим "Не беспокоить" включается и выключается автоматически. Вам не нужно менять настройки приложения.

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

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

Подробнее о показе уведомлений вы можете прочитать в разделе справки Об уведомлениях.

Игровой режим

При одновременной работе приложения Kaspersky и некоторых приложений (в особенности компьютерных игр) в полноэкранном режиме иногда могут возникать следующие неудобства:

- работа приложения или игры замедляется из-за недостатка системных ресурсов;
- окна уведомлений приложения Kaspersky отвлекают от игры.

Чтобы не изменять настройки приложения Kaspersky вручную перед каждым переходом в полноэкранный режим, вы можете использовать Игровой режим. Если Игровой режим используется и вы играете или работаете с приложением в полноэкранном режиме, приложение Kaspersky не запускает задачи проверки и обновления, не отображает уведомления.

Чтобы включить использование Игрового режима:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки производительности** → **Потребление ресурсов компьютера**.
4. Установите флажок **Игровой режим**.

Дополнительно установите флажок **Режим "Не беспокоить"**. В этом режиме не показываются уведомления, если вы активно работаете с некоторыми приложениями, а также не запускаются задачи проверки и обновления.

Экономия заряда батареи

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

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

Оптимизация нагрузки на операционную систему

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

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

Чтобы оптимизировать нагрузку на операционную систему:

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

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

Премиальная техническая поддержка

Премиальная техническая поддержка по телефону доступна не во всех регионах.

Помощь наших специалистов в установке приложения

Если у вас возникли проблемы с установкой приложения на компьютер, вы можете позвонить нам и специалисты "Лаборатории Касперского" удаленно:

- запустят установку приложения;
- убедятся, что установка приложения прошла без ошибок;
- расскажут о функциональности и настройках приложения;
- ответят на любые ваши вопросы о приложении и его установке;

- выполнят настройку приложения исходя из ваших потребностей;
- убедятся, что приложение установлено, настроено и корректно работает.

Обращение в Службу технической поддержки без очереди

Вы можете обратиться без очереди к сотруднику Службы технической поддержки по телефону или в чате. Ваш звонок будет обработан с высоким приоритетом. Также вы можете написать сотруднику Службы технической поддержки в чат-приложение, с помощью которого специалисты "Лаборатории Касперского" могут помочь вам удаленно.

Удаленная поддержка

В один клик вы можете связаться со специалистом "Лаборатории Касперского", который при необходимости подключится к вашему компьютеру и поможет решить вашу проблему удаленно!

Поиск и удаление вирусов

Профессиональная помощь в поиске и удалении вирусов и приложений-шпионов с компьютера, на котором установлено приложение "Лаборатории Касперского".

Проверка исправности компьютера

Наши специалисты проведут тщательный анализ вашего устройства, чтобы гарантировать его высокую производительность и безопасность.

> Чтобы воспользоваться премиальной технической поддержкой, позвоните по номеру телефона в регионе, в котором вы приобрели подписку на приложение Kaspersky Premuim.

Приватность

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

Безопасное VPN-соединение

Доступно только в Kaspersky Plus и Kaspersky Premium.

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

Чтобы запустить Kaspersky Secure Connection из окна приложения Kaspersky:

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

   Откроется главное окно приложения Kaspersky Secure Connection.

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

Поиск утечки данных

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

О поиске утечки данных

Поиск утечки данных в Kaspersky Basic и Kaspersky Standard позволяет вам вручную проверить только аккаунт My Kaspersky. Автоматическая проверка аккаунта My Kaspersky и других учетных записей доступна только в планах Kaspersky Plus и Kaspersky Premium.

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 приложения Kaspersky вы можете проверить ваши учетные записи на предмет возможной утечки. Если при проверке будет обнаружено, что ваши данные могли попасть в публичный доступ, приложение 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.

Также приложение Kaspersky проверяет ваши учетные записи на предмет утечки данных в Даркнет. В случае обнаружения такой утечки, приложение предупредит вас об этом.

Поиск утечки данных 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 приложение Kaspersky не получает доступа к самим пользовательским данным и предоставляет информацию только о категориях данных, которые могли попасть в публичный доступ.

Приложение Kaspersky 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 приложение Kaspersky 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 Поиск утечки данных.

Вы можете добавить до 50 учетных записей для автоматической проверки. Списки учетных записей в приложении Kaspersky 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.

Приложение Kaspersky периодически проверяет по базе, предоставленной сайтом www.haveibeenpwned.com, адрес электронной почты, привязанный к вашему аккаунту My Kaspersky. Первая такая проверка осуществляется через двое суток после установки приложения Kaspersky. Далее проверка производится каждые 24 часа.

Поиск утечки данных для аккаунта My Kaspersky не работает, если приложение Kaspersky не подключен к My Kaspersky или в приложении не введен пароль от аккаунта My Kaspersky.

Как включить и выключить поиск утечки данных

Чтобы включить или выключить проверку учетных записей:

1. Откройте главное окно приложения.
2. Выберите раздел **Приватность**.
3. В блоке **Поиск утечки данных** нажмите на кнопку **Найти утечки**.

   Откроется окно **Поиск утечки данных**.
4. Включите / выключите компонент Поиск утечки данных с помощью переключателя.

Как проверить, могли ли ваши данные попасть в публичный доступ

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

1. Откройте главное окно приложения.
2. Выберите раздел **Приватность**.
3. В блоке **Поиск утечки данных** нажмите на кнопку **Найти утечки**.

   Откроется окно **Поиск утечки данных**.
4. Укажите адрес вашей электронной почты в поле ввода и нажмите на кнопку **Проверить**.

   Приложение Kaspersky начнет проверку указанного адреса по базе, предоставленной сайтом www.haveibeenpwned.com. Если при проверке будет обнаружено, что ваши данные могли попасть в публичный доступ, приложение 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 приложение Kaspersky, 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:

1. Откройте главное окно приложения.
2. Выберите раздел **Приватность**.
3. В блоке **Поиск утечки данных** нажмите на кнопку **Найти утечки**.

   Откроется окно **Поиск утечки данных**.
4. В поле **Проверьте другие аккаунты** укажите электронный адрес учетной записи, которую вы хотите добавить в список для автоматической проверки, и нажмите на кнопку **Проверить**.

   Добавленная вами запись отобразится в списке **Аккаунты**.

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

Защита от сбора данных в интернете

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

О защите от сбора данных в интернете

Доступно только в Kaspersky Standard, Kaspersky Plus и Kaspersky Premium.

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

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

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

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

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

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

Защита от сбора данных в интернете имеет следующие ограничения:

- Приложение не блокирует сбор данных сервисом отслеживания из категории "Социальные сети", если вы находитесь на сайте соответствующей социальной сети.
- Если веб-страницу, на которой выполнена попытка сбора данных, не удалось определить, то приложение Kaspersky 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 приложение Kaspersky применяет то действие, которое задано в настройках Защиты от сбора данных (запрещает или разрешает сбор данных). Приложение отображает информацию о попытке сбора данных в отчетах, но не включает эту информацию в статистику Защиты от сбора данных, отображаемую в браузере.

По умолчанию компонент выключен.

Запрет на сбор данных

Чтобы запретить сбор данных:

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

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

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

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

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

Разрешение на сбор данных на всех сайтах

Чтобы разрешить сбор данных на всех сайтах:

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

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

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

Разрешение на сбор данных в виде исключения

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

Чтобы разрешить сбор данных в виде исключения:

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

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

   Приложение Kaspersky 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 в интернете**.

   c. Нажмите на кнопку **Добавить**.

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

Чтобы просмотреть отчет о попытках сбора данных в интернете:

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

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

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

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

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

Управление защитой от сбора данных в браузере

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

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

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

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

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

Устройства в моей сети

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

О компоненте Устройства в моей сети

Доступно только в Kaspersky Plus и Kaspersky Premium.

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

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

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

- Если вы отказываетесь, приложение Kaspersky 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. Приложение Kaspersky 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 приложения "Лаборатории Касперского" установлены на других устройствах, подключенных к одному аккаунту My Kaspersky.

Вы можете выключить компонент Устройства в моей сети. После выключения компонента приложение Kaspersky 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:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки безопасности**.
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

Приложение Kaspersky 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;
- приложения "Лаборатории Касперского", установленные на устройстве.

Чтобы просмотреть устройства, подключенные к вашей сети:

1. Откройте главное окно приложения.

2. Выполните одно из следующих действий:

   - Перейдите в раздел **Приватность** и в блоке **Устройства в моей сети** нажмите на кнопку **Подробнее**.
   - В главном окне найдите блок **Устройства в моей сети** и нажмите на кнопку **Подробнее**.
   - Пройдите по ссылке **<название сети>**, которая отображается в нижней части главного окна.

   Откроется окно **Устройства в моей сети**, в котором будет показана сеть, к которой подключен ваш компьютер.

3. Установите флажок **Показывать информацию об устройствах в сети на моих мобильных устройствах**, если вы хотите передать информацию об устройствах, подключенных к этой сети, на ваши мобильные устройства.

4. Чтобы посмотреть устройства, подключенные к сети, нажмите на кнопку **Да, показать мои устройства**.

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

   - 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:

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:

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

Чтобы запретить устройству доступ в сеть:

1. Откройте главное окно приложения.
2. Выполните одно из следующих действий:
   - Перейдите в раздел **Приватность** и в блоке **Устройства в моей сети** нажмите на кнопку **Подробнее**.
   - В главном окне найдите блок **Устройства в моей сети** и нажмите на кнопку **Подробнее**.
   - Пройдите по ссылке **<название сети>**, которая отображается в нижней части главного окна.
3. В окне **Устройства в моей сети** выберите устройство, которое хотите отключить.

   Откроется окно с данными об этом устройстве, в котором отображается информация о MAC-адресе устройства.
4. Запишите MAC-адрес устройства.
5. 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

Чтобы удалить из списка сеть, к которой нет подключения:

1. Откройте главное окно приложения.
2. Выполните одно из следующих действий:
   - Перейдите в раздел **Приватность** и в блоке **Устройства в моей сети** нажмите на кнопку **Подробнее**.
   - В главном окне найдите блок **Устройства в моей сети** и нажмите на кнопку **Подробнее**.

3. Пройдите по ссылке **<название сети>**, которая отображается в нижней части главного окна.

   Будет выполнен переход в окно **Устройства в моей сети**.

4. Разверните список с названием сети с помощью стрелочки в правой части списка 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:

1. Откройте главное окно приложения.
2. Выполните одно из следующих действий:

   - Перейдите в раздел **Приватность** и в блоке **Устройства в моей сети** нажмите на кнопку **Подробнее**.
   - В главном окне найдите блок **Устройства в моей сети** и нажмите на кнопку **Подробнее**.
   - Пройдите по ссылке **<название сети>**, которая отображается в нижней части главного окна.

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

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

> Также вы можете отключить уведомления для выбранной сети, когда приложение Kaspersky 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:

1. Откройте главное окно приложения.

2. Выполните одно из следующих действий:

   - Перейдите в раздел **Приватность** и в блоке **Устройства в моей сети** нажмите на кнопку **Подробнее**.

   - В главном окне найдите блок **Устройства в моей сети** и нажмите на кнопку **Подробнее**.

   - Пройдите по ссылке **<название сети>**, которая отображается в нижней части главного окна.

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.

      - **Приложение долго ищет устройства в сети**. Выберите этот элемент, если компонент Устройства в моей сети работает слишком медленно.

      - **Приложение неправильно определяет устройства в сети**. Выберите этот элемент, если приложение 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 приложение 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 установленном приложении и его 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".

Менеджер паролей

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

Проверка и безопасное хранение паролей

Доступно только в Kaspersky Plus и Kaspersky Premium.

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

Приложение Kaspersky проверяет надежность паролей, которые вы создаете в интернете. Если пароли недостаточно надежны, Kaspersky поможет вам создать надежные пароли и хранить их в безопасном месте.

Защита от использования одинаковых паролей

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

Если защита от использования одинаковых паролей включена, приложение Kaspersky 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, приложение Kaspersky уведомляет вас об этом и предлагает создать новый пароль. Вы можете выбрать категории сайтов, для которых необходимо контролировать использование одинаковых паролей.

Безопасное хранение паролей и документов

Для безопасного хранения паролей и документов предназначено приложение Kaspersky Password Manager, которое использует специальное зашифрованное хранилище для безопасного хранения вашей личной информации: паролей, паспортных данных, финансовых или медицинских сведений.

Вы можете скачать Kaspersky Password Manager в окне приложения Kaspersky.

Как скачать и установить Kaspersky Password Manager

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

1. Откройте главное окно Kaspersky.
2. Перейдите в раздел **Приватность**.
3. В блоке **Менеджер паролей** нажмите на кнопку **Скачать**.

   Установочный пакет Kaspersky Password Manager будет загружен на ваш компьютер. Для установки Kaspersky Password Manager следуйте стандартной процедуре установки приложений на компьютер.

Как запустить Kaspersky Password Manager из окна приложения Kaspersky

Чтобы запустить Kaspersky Password Manager, если он уже установлен:

1. Откройте главное окно Kaspersky.
2. Перейдите в раздел **Приватность**.
3. В блоке **Менеджер паролей** нажмите на кнопку **Запустить**.

   Откроется окно приложения для защиты паролей Kaspersky Password Manager.

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

Как проверить надежность ваших паролей

Ваши интернет-аккаунты подвергаются большому риску, если у них одинаковые или слабые пароли (например, qwerty или 12345), а также, если эти пароли основаны на информации, которую легко угадать или получить (например, имена родственников или даты рождения).

Kaspersky поможет вам быстро проверить, насколько сложные пароли вы используете и повторяется ли один пароль в нескольких аккаунтах.

Чтобы проверить надежность паролей:

1. Откройте главное окно приложения.
2. Выберите раздел **Приватность**.
3. В блоке **Безопасность паролей** нажмите на кнопку **Открыть**.
4.

Настройка безопасности паролей

Чтобы изменить настройки безопасности паролей:

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

   Откроется окно **Настройка**.
3. В разделе **Настройки приватности** выберите подраздел **Защита ввода данных**.
4. Установите флажок **Показывать в браузере надежность создаваемого пароля**, если вы хотите, чтобы приложение Kaspersky проверяло надежность пароля, который вы создаете на сайте, и уведомлял вас об этом.

   Если у вас установлен Kaspersky Password Manager, в уведомлении вам будет предложен надежный пароль. Если Kaspersky Password Manager не установлен, мы рекомендуем скачать и установить его, чтобы всегда создавать надежные пароли.
5. Установите флажок **Предупреждать об использовании одинаковых паролей на сайтах**, если вы хотите, чтобы приложение Kaspersky проверяло, 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, приложение Kaspersky проверяет, использовали ли вы этот пароль на сайтах банков и платежных систем.
   - **Социальные сети**. Когда вы создаете или вводите пароль в интернете, приложение Kaspersky проверяет, использовали ли вы этот пароль в социальных сетях.

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

Безопасные платежи

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

О защите финансовых операций и покупок в интернете

Для защиты конфиденциальных данных, которые вы вводите на сайтах банков и платежных систем (например, номера банковской карты, пароли для доступа к интернет-банкам), а также для предотвращения кражи платежных средств при проведении платежей онлайн, приложение Kaspersky 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 приложения не могли внедриться в процесс Защищенного браузера. Приложение Kaspersky создает специальные профили браузеров Mozilla Firefox и Google Chrome, чтобы установленные сторонние расширения не могли повлиять на работу Защищенного браузера. Приложение 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, приложение 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 приложения.

Запуск Защищенного браузера невозможен при следующих условиях:

- снят флажок **Включить самозащиту** в окне **Потребление ресурсов компьютера** в разделе настроек **Настройки производительности**;
- в браузере выключено выполнение JavaScript.

Запуск Защищенного браузера в Яндекс.Браузере

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

Возможности Защищенного браузера

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

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

  Приложение может обнаружить следующие угрозы и проблемы безопасности:

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

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

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

О защите данных буфера обмена

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

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

Если Защищенный браузер запущен на операционной системе Microsoft Windows 10, приложение Kaspersky блокирует работу приложений универсальной платформы Windows с буфером обмена.

Как изменить настройки Безопасных платежей

Чтобы настроить Безопасные платежи:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки приватности**.

4. Нажмите на кнопку **Безопасные платежи**.

   В окне отобразятся настройки компонента Безопасные платежи.

5. Включите компонент Безопасные платежи с помощью переключателя в верхней части окна.

6. В блоке **При первом обращении к сайтам банков или платежных систем** выберите действие, которое будет выполнять приложение, когда вы впервые открываете в браузере сайт банка или платежной системы:

   - Выберите **Запускать Защищенный браузер**, если хотите, чтобы приложение открывало сайт в Защищенном браузере.

   - Выберите **Спрашивать пользователя**, если хотите, чтобы при обращении к сайту приложение спрашивало у вас, открывать сайт в Защищенном браузере или нет.

   - Выберите **Не запускать Защищенный браузер**, если хотите, чтобы приложение не открывало сайт в Защищенном браузере.

7. В блоке **Дополнительно** в раскрывающемся списке **Для перехода к сайтам из окна Безопасных платежей использовать** выберите браузер, который приложение 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:

1. Откройте главное окно приложения.

2. Перейдите в раздел **Приватность**.

3. Выберите блок **Безопасные платежи** и нажмите на кнопку **Посмотреть сайты**.

   Откроется окно **Безопасные платежи**.

4. По ссылке **Добавить сайт в Безопасные платежи** откройте поля для добавления информации о сайте.

5. 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.

6. 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 приложение Kaspersky запрашивало, 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**.

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

8. Нажмите на кнопку **Добавить**.

Сайт отобразится в списке.

Как отправить отзыв о работе Безопасных платежей

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

Как отправить отзыв

Чтобы отправить отзыв о работе с Безопасными платежами:

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

   Откроется окно **Безопасные платежи**.
4. По ссылке **Оставить отзыв** откройте окно, в котором вы можете написать отзыв о работе с Безопасными платежами.
5. Оцените работу Безопасных платежей по 5-балльной шкале, выбрав от 1 до 5 звезд.

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

7. Нажмите на кнопку **Отправить**.

Как сообщить о проблеме

Чтобы сообщить о проблеме при работе с Защищенным браузером:

1. Нажмите на ссылку **Сообщить о проблеме** в окне всплывающего сообщения 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 не удается отправить отзыв (например, отсутствует соединение с интернетом), приложение Kaspersky 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 веб-камеры

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

Доступно только в Kaspersky Standard, Kaspersky Plus и Kaspersky Premium.

О доступе приложений 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 приложениям доступ к веб-камере**, приложение Kaspersky блокирует доступ к веб-камере всем приложениям и показывает уведомление о том, что доступ заблокирован.

Если флажок **Запретить всем приложениям доступ к веб-камере** снят, приложение Kaspersky контролирует доступ к веб-камере в зависимости от того, в какую группу доверия входит приложение, запрашивающее доступ. Приложение Kaspersky блокирует доступ к веб-камере приложениям, которые входят в группы доверия "Сильные ограничения" и "Недоверенные".

Вы можете разрешить доступ к веб-камере приложениям, входящим в группы "Сильные ограничения" и "Недоверенные", в окне настройки Предотвращения вторжений. Если к веб-камере пытается подключиться приложение, входящее в группу доверия "Слабые ограничения", приложение Kaspersky показывает уведомление и предлагает вам самостоятельно принять решение о том, предоставлять этому приложению доступ к веб-камере или нет.

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

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

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

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

- Приложение Kaspersky контролирует видео и статические изображения, полученные в результате обработки данных веб-камеры.
- Приложение Kaspersky контролирует аудиосигнал, если он является частью видеопотока, получаемого с веб-камеры.
- Приложение Kaspersky 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 Предотвращение вторжений.

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

Как изменить настройки доступа приложений к веб-камере

Чтобы изменить настройки доступа приложений к веб-камере:

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

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

   - Если вы хотите запретить доступ всех приложений к веб-камере, установите флажок **Запретить всем приложениям доступ к веб-камере**.
   - Если вы хотите получать уведомление о том, что веб-камеру использует приложение, которому это разрешено, установите флажок **Показывать уведомление, когда веб-камеру использует приложение, которому это разрешено**.

Как разрешить доступ приложения к веб-камере

Чтобы разрешить доступ приложения к веб-камере:

1. Откройте главное окно приложения.
2. Выберите раздел **Безопасность**.
3. В блоке **Предотвращение вторжений** нажмите на кнопку **Управлять приложениями**.

   Откроется окно **Управление приложениями**.
4. Двойным щелчком мыши по названию приложения откройте окно **Правила приложения**.
5. В окне **Правила приложения** перейдите на закладку **Права**.
6. В списке категорий прав выберите пункт **Изменение операционной системы** → **Подозрительные изменения в операционной системе** → **Доступ к веб-камере**.

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

8. Нажмите на кнопку **Сохранить**.

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

Если флажок **Запретить всем приложениям доступ к веб-камере** установлен, приложение Kaspersky блокирует доступ приложения к веб-камере независимо от группы доверия и настроенного вручную разрешения.

Сталкерские приложения

Некоторые легальные приложения могут использоваться злоумышленниками для кражи ваших данных и слежки за вами. Большинство этих приложений являются полезными, и многие пользователи применяют их. Среди таких приложений – IRC-клиенты, приложения автодозвона, приложения для загрузки файлов, мониторы активности компьютерных систем, утилиты для работы с паролями, интернет-серверы служб FTP, HTTP или Telnet.

Однако если злоумышленники получат доступ к таким приложениям или внедрят их на вашем компьютере, они смогут использовать некоторые их функции для кражи персональных данных и совершения других противоправных действий.

Ниже вы можете ознакомиться с разными типами сталкерских приложений.

Тип	Название	Описание
Client-IRC	Клиенты интернет-чатов	Пользователи устанавливают эти приложения, чтобы общаться в ретранслируемых интернет-чатах (Internet Relay Chats). Злоумышленники используют их для распространения вредоносных приложений.
Dialer	Приложения автодозвона	Могут устанавливать телефонные соединения через модем в скрытом режиме.
Downloader	Приложения-загрузчики	Могут загружать файлы с веб-страниц в скрытом режиме.
Monitor	Приложения-мониторы	Позволяют наблюдать за активностью на компьютере, на котором установлены (видеть, какие приложения работают, и как они обмениваются данными с приложениями на других компьютерах).

PSWTool	Восстановители паролей	Позволяют просматривать и восстанавливать забытые пароли. С этой же целью их скрыто внедряют на компьютеры пользователей злоумышленники.
RemoteAdmin	Приложения удаленного администрирования	Широко используются системными администраторами; позволяют получать доступ к интерфейсу удаленного компьютера, чтобы наблюдать за ним и управлять им. С этой же целью злоумышленники скрыто внедряют их на компьютеры пользователей для наблюдения за удаленными компьютерами и управления ими. Легальные приложения удаленного администрирования отличаются от троянских приложений удаленного администрирования Backdoor. Троянские приложения обладают функциями, которые позволяют им самостоятельно проникать в систему и устанавливать себя; легальные приложения этих функций не имеют.
Server-FTP	FTP-серверы	Выполняют функции FTP-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу FTP.
Server-Proxy	Прокси-серверы	Выполняют функции прокси-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы от его имени рассылать спам.
Server-Telnet	Telnet-серверы	Выполняют функции Telnet-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу Telnet.
Server-Web	Веб-серверы	Выполняют функции веб-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу HTTP.
RiskTool	Инструменты для работы на локальном компьютере	Дают пользователю дополнительные возможности при работе на своем компьютере (позволяют скрывать на своем компьютере файлы или окна активных приложений, закрывать активные процессы).

NetTool	Сетевые инструменты	Дают пользователю компьютера, на котором установлены, дополнительные возможности при работе с другими компьютерами в сети (позволяют перезагружать их, находить открытые порты, запускать установленные на них приложения).
Client-P2P	Клиенты пиринговых сетей	Позволяют работать в пиринговых (Peer-to-Peer) сетях. Могут использоваться злоумышленниками для распространения вредоносных приложений.
Client-SMTP	SMTP-клиенты	Отправляют сообщения электронной почты в скрытом режиме. Злоумышленники внедряют их на компьютер пользователя, чтобы от его имени рассылать спам.
WebToolbar	Веб-панели инструментов	Добавляют в интерфейс других приложений панели инструментов для использования поисковых систем.
FraudTool	Псевдоприложения	Выдают себя за другие приложения. Например, существуют псевдоантивирусы, которые выводят на экран сообщения об обнаружении вредоносных приложений, но на самом деле ничего не находят и не лечат.

Включите защиту от сталкерских приложений, и мы предупредим вас о попытках получить доступ к вашему местоположению, переписке и другим персональным данным.

Также вы можете включить защиту от сталкерских приложений в окне **Настройки угроз и исключений**, установив флажок **Обнаруживать другие приложения, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя**.

Анти-Баннер

Этот раздел содержит информацию о том, как с помощью приложения Kaspersky защитить вас от рекламных баннеров в интернете.

Об Анти-Баннере

Доступно только в Kaspersky Standard, Kaspersky Plus и Kaspersky Premium.

Для защиты от баннеров в интернете предназначен компонент Анти-Баннер. Анти-Баннер блокирует отображение баннеров на просматриваемых вами сайтах и в интерфейсе некоторых компьютерных приложений. Анти-Баннер блокирует баннеры из списка известных баннеров, который входит в состав баз приложения Kaspersky. Вы можете управлять блокировкой баннеров через интерфейс приложения Kaspersky 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 приложение Kaspersky не блокирует такой баннер и не отображает информацию о нем.

- Если веб-страницу, на которой расположен баннер, удалось определить, но не удалось сопоставить ни с одной веб-страницей, открытой в браузере, то приложение Kaspersky запрещает или разрешает отображение баннера с учетом информации о веб-странице, которую удалось определить. Приложение отображает информацию о баннере в отчетах, но не включает эту информацию в статистику Анти-Баннера, отображаемую в браузере.

- В статистике Анти-Баннера, отображаемой в браузере, могут учитываться баннеры, заблокированные при предыдущих загрузках веб-страницы, в том числе баннеры, заблокированные ранее и загруженные повторно.

- В статистике Анти-Баннера, отображаемой в браузере, не учитываются баннеры, заблокированные в динамическом содержимом страницы после загрузки сайта.

Как включить компонент Анти-Баннер

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

Как включить Анти-Баннер в приложении Kaspersky

Чтобы включить компонент Анти-Баннер в приложении Kaspersky:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки приватности**.
4. Выберите компонент Анти-Баннер.

   Откроется окно **Настройки Анти-Баннера**.
5. Включите компонент с помощью переключателя в верхней части окна.

Как включить Анти-Баннер в окне браузера

Чтобы включить компонент Анти-Баннер в окне браузера:

1. Нажмите на кнопку **Kaspersky Protection** в панели инструментов браузера.
2. В раскрывшемся меню в блоке **Анти-Баннер** нажмите на кнопку **Включить**.

После включения или выключения Анти-Баннера необходимо перезагрузить веб-страницу в браузере, чтобы изменения вступили в силу.

Запрет баннеров

Анти-Баннер блокирует на сайтах баннеры из списка известных баннеров, который входит в состав баз приложения Kaspersky. Если баннер на веб-странице отображается, несмотря на работающий Анти-Баннер, это может означать, что баннер не входит в список известных баннеров. Вы можете самостоятельно запретить отображение этого баннера.

Чтобы запретить баннер, нужно добавить его в список запрещенных баннеров. Вы можете сделать это непосредственно на веб-странице или в приложении Kaspersky.

Если баннер находится на сайте из списка сайтов с разрешенными баннерами, вы не можете запретить отображение этого баннера.

Как запретить баннер, находясь на веб-странице

Чтобы запретить баннер, находясь на веб-странице:

1. Убедитесь, что в браузере установлено и включено расширение Kaspersky Protection.
2. Если Анти-Баннер выключен, включите его:
   a. Нажмите на кнопку **Kaspersky Protection** в панели инструментов браузера.
   b. В раскрывшемся меню в блоке **Анти-Баннер** нажмите на кнопку **Включить**.
3. Наведите курсор мыши на баннер, который вы хотите запретить, и нажмите на правую клавишу мыши.
4. В появившемся контекстном меню выберите пункт **Добавить в Анти-Баннер**.
   Откроется окно **Добавление запрещенного баннера**.
5. В окне **Добавление запрещенного баннера** нажмите на кнопку **Добавить**.
   Адрес баннера будет добавлен в список запрещенных баннеров.
6. Обновите веб-страницу в браузере, чтобы баннер перестал отображаться.

При последующих переходах на эту веб-страницу баннер не будет отображаться.

Как запретить баннер в приложении Kaspersky

Чтобы запретить баннер в приложении Kaspersky:

1. Откройте главное окно приложения.
2. Нажмите на кнопку в нижней части главного окна.
   Откроется окно **Настройка**.
3. Выберите раздел **Настройки приватности**.
4. Выберите компонент Анти-Баннер.
   Откроется окно **Настройки Анти-Баннера**.
5. Включите компонент Анти-Баннер с помощью переключателя в верхней части окна.

6. В окне **Настройки Анти-Баннера** по ссылке **Запрещенные баннеры** 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**.

Приложение Kaspersky будет блокировать указанный баннер.

Разрешение баннеров

Вы можете разрешить как отдельный баннер, так и все баннеры на указанном вами сайте.

Как разрешить отдельный баннер

Чтобы разрешить отдельный баннер:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки приватности**.
4. Выберите компонент Анти-Баннер.

   Откроется окно **Настройки Анти-Баннера**.
5. Включите компонент Анти-Баннер с помощью переключателя в верхней части окна.
6. В окне **Настройки Анти-Баннера** по ссылке **Сайты с разрешенными баннерами** откройте окно **Сайты с разрешенными баннерами**.
7. В окне **Сайты с разрешенными баннерами** 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**.

    Приложение не будет блокировать указанный баннер.

    > Если баннер добавлен в список разрешенных баннеров, но на сайте баннер находится внутри рекламного блока, свойства которого приводят к его блокировке Анти-Баннером, такой баннер будет заблокирован вместе с рекламным блоком.

[Как разрешить все баннеры на сайте]

Чтобы разрешить все баннеры на сайте:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки приватности**.
4. Выберите компонент Анти-Баннер.

   Откроется окно **Настройки Анти-Баннера**.
5. Включите компонент Анти-Баннер с помощью переключателя в верхней части окна.
6. В окне **Настройки Анти-Баннера** по ссылке **Сайты с разрешенными баннерами** 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 не блокирует баннеры на сайтах из этого списка, даже если баннер добавлен в список запрещенных баннеров.

Как настроить фильтры Анти-Баннера

Чтобы настроить фильтры Анти-Баннера:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки приватности**.
4. Выберите компонент Анти-Баннер.

   Откроется окно **Настройки Анти-Баннера**.
5. Включите компонент Анти-Баннер с помощью переключателя в верхней части окна.
6. По ссылке **Список фильтров** 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. Приложение будет блокировать баннеры на сайтах указанного языка.

Как управлять Анти-Баннером в браузере

Вы можете управлять компонентом Анти-Баннер непосредственно в браузере с помощью расширения Kaspersky Protection.

Расширение Kaspersky Protection позволяет выполнять следующие действия:

- включать и выключать компонент;
- просматривать статистику заблокированных баннеров;

- переходить в окно настройки Анти-Баннера;
- просматривать информацию о том, запрещены или разрешены баннеры на сайте, открытом в браузере, и управлять отображением баннеров на сайте.

Как управлять компонентом Анти-Баннер через расширение Kaspersky Protection

Чтобы получить доступ к управлению компонентом Анти-Баннер через расширение Kaspersky Protection,

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

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

Блокировщик скрытых установок

Бывает, что вы устанавливаете приложение, а потом обнаруживаете, что вместе с этим приложением установились еще несколько дополнительных приложений, которые вы не запрашивали. Знакомая ситуация? Такие приложения устанавливаются незаметно и могут спамить вас рекламой и даже изменять браузер по умолчанию.

Включите **Блокировщик скрытых установок** в разделе **Безопасность**, чтобы навсегда забыть об этой проблеме. Блокировщик скрытых установок будет сам снимать флажки с приложений, предлагаемых к дополнительной установке, чтобы вам не приходилось делать это вручную.

Также вы можете включить Блокировщик скрытых установок в окне настройки Менеджера приложений.

Для этого установите флажок **Во время установки приложений автоматически снимать флажки установки дополнительных приложений. Предупреждать при попытке установить дополнительные приложения.**

Блокировщик скрытых установок поддерживает не все приложения для установки. Если приложение для установки не поддерживается, заблокировать установку дополнительных приложений будет невозможно. Список поддерживаемых приложений для установки пополняется нашими специалистами.

Как изменить настройки Менеджера приложений

Доступно только в Kaspersky Standard, Kaspersky Plus и Kaspersky Premium.

Чтобы изменить настройки Менеджера приложений:

1. Откройте главное окно приложения.
2. Выберите раздел **Приватность**.
3. В блоке **Блокировщик скрытых установок** нажмите на кнопку  .

   Будет выполнен переход в окно **Настройки Менеджера приложений**.
4. В блоке настроек **Блокировщик скрытых установок** установите флажок **Во время установки приложений автоматически снимать флажки установки дополнительных приложений. Предупреждать при попытке установить дополнительные приложения**, чтобы запретить установку дополнительного программного обеспечения при установке новых приложений. Если при установке нового приложения будут предотвращены нежелательные действия, приложение Kaspersky уведомит вас об этом.

   Если флажок **Во время установки приложений автоматически снимать флажки установки дополнительных приложений. Предупреждать при попытке установить дополнительные приложения** снят после того, как вы уже запустили установку какого-либо приложения, блокировщик скрытых установок продолжит свою работу в рамках текущей установки. Флажки напротив приложений, предлагаемых к дополнительной установке, будут сняты, а сами дополнительные приложения не будут устанавливаться. При последующей установке приложений эта функциональность работать не будет. Дополнительные приложения будут устанавливаться совместно с основным.
5. Установите флажок **Не отображать шаги установки, которые могут содержать рекламу или предложения об установке дополнительных приложений**, чтобы запретить показ шагов установки, содержащих рекламу, во время установки на компьютер новых приложений. Если такие шаги установки будут удалены, приложение Kaspersky уведомит вас об этом.

Удалять рекламные приложения

Раздражает реклама? Приложение Kaspersky удаляет с вашего компьютера приложения, которые показывают рекламу в браузерах и на рабочем столе. Помимо рекламы мы также удалим за вас приложения автодозвона и подозрительные упаковщики, которые могут содержать вирусы и другие угрозы. Включите функциональность **Удалять рекламные приложения**, чтобы никогда больше не видеть навязчивую рекламу.

Чтобы удалить рекламные приложения:

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

3. Включите функциональность **Удалять рекламные приложения**.

Секретная папка

Этот раздел содержит информацию о том, как вы можете защитить данные с помощью секретных папок.

О секретной папке

Доступно только в Kaspersky Plus и Kaspersky Premium.

Для защиты ваших конфиденциальных данных от несанкционированного доступа предназначены секретные папки. *Секретная папка* – это хранилище данных на вашем компьютере, которое вы можете открывать или закрывать с помощью известного только вам пароля. Для изменения файлов, хранящихся в секретной папке, требуется ввести пароль. Если вы ввели неверный пароль 10 раз подряд, доступ к секретной папке блокируется на один час.

Если вы потеряете или забудете пароль, восстановить данные будет невозможно.

Для создания секретной папки в приложении Kaspersky используется алгоритм шифрования данных AES XTS с эффективной длиной ключа 56 бит.

> Если на вашем компьютере используется файловая система FAT32, вы можете создавать секретные папки объемом не более 4 ГБ.

Как поместить файлы в секретную папку

Чтобы поместить файлы в секретную папку:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Приватность**.
3. В блоке **Секретная папка** выполните одно из следующих действий:

Если у вас еще нет секретной папки

1. Нажмите на кнопку **Создать папку**.
2. В окне **Секретная папка** нажмите на кнопку **Добавить** и выберите файлы в Проводнике или перетащите файлы в окно приложения Kaspersky.

Выбранные файлы отобразятся в окне **Секретная папка**.

3. Нажмите на кнопку **Продолжить**.
4. Введите название секретной папки и укажите ее расположение или используйте значения этих настроек по умолчанию.
5. Укажите размер секретной папки.
6. Для получения быстрого доступа к секретной папке установите флажок **Создать ярлык секретной папки на рабочем столе**.
7. Нажмите на кнопку **Продолжить**.
8. Заполните поля **Пароль для доступа к секретной папке** и **Подтверждение пароля** и нажмите на кнопку **Продолжить**.
9. Выберите действие с исходными копиями файлов вне секретной папки:
   - Чтобы удалить исходные копии файлов вне секретной папки, нажмите на кнопку **Удалить**.
   - Чтобы сохранить исходные копии файлов вне секретной папки, нажмите на кнопку **Пропустить**.
10. Нажмите на кнопку **Готово**.

    В списке секретных папок отобразится созданная вами секретная папка.
11. Чтобы закрыть секретную папку, нажмите на кнопку **Закрыть**.

    Данные в закрытой секретной папке будут доступны только после ввода пароля.

Если у вас уже есть секретная папка

1. По ссылке **У меня уже есть секретная папка** перейдите в окно **Секретная папка**.
2. В окне **Секретная папка** выберите нужную секретную папку и нажмите на кнопку **Открыть**.
3. Введите пароль доступа к секретной папке и нажмите на кнопку **Открыть в Проводнике**.

   Секретная папка откроется в Проводнике.

4. Перетащите нужные файлы в секретную папку.

5. Закройте окно Проводника.

6. В приложении Kaspersky в окне **Секретная папка** нажмите на кнопку **Закрыть**.

При добавлении в секретную папку файлов с одинаковыми названиями, написанными в разных регистрах, один из таких файлов может быть недоступен при попытке открытия секретной папки Чтобы избежать потери данных, мы рекомендуем добавлять такие файлы в разные секретные папки или поменять названия файлов на полностью уникальные.

Как получить доступ к файлам, хранящимся в секретной папке

Чтобы получить доступ к файлам, хранящимся в секретной папке:

1. Откройте главное окно приложения.

2. Перейдите в раздел **Приватность**.

3. В блоке **Секретная папка** нажмите на кнопку **У меня уже есть секретная папка**.

   Откроется окно **Секретная папка**.

4. Нажмите на кнопку **Открыть** рядом с секретной папкой.

5. Введите пароль и нажмите на кнопку **Открыть в Проводнике**.

   Файлы, сохраненные в секретной папке, отобразятся в окне Проводника. Вы можете внести необходимые изменения в файлы, или добавить новые файлы, и снова закрыть секретную папку.

Если вы переименовали секретную папку, при попытке открытия такой папки может появиться ошибка. Чтобы этого избежать, мы рекомендуем открыть секретную папку, которую вы хотите переименовать, извлечь ваши данные и создать новую секретную папку с этими данными, назвав ее другим именем.

Иногда, чтобы открыть секретные папки, созданные в других приложениях "Лаборатории Касперского", может потребоваться выполнить конвертацию секретных папок старого формата в новый формат. Приложение Kaspersky само предложит вам выполнить конвертацию при попытке открыть секретную папку в приложении Kaspersky.

Конвертация секретных папок в новый формат зависит от размера секретных папок и может занимать значительное время.

> Если при удалении приложения Kaspersky в окне **Сохранить следующие данные на этом компьютере для повторного использования:** флажок **Настройки работы приложения** снят, а флажок **Секретная папка** установлен, при последующей установке текущей или новой версии приложения Kaspersky секретные папки нужно будет добавить вручную по ссылке **У меня уже есть секретная папка** в окне **Секретная папка**.

Уничтожитель файлов

Доступно только в Kaspersky Plus и Kaspersky Premium.

Дополнительная безопасность персональных данных обеспечивается защитой от несанкционированного восстановления удаленной информации злоумышленниками.

В состав приложения Kaspersky входит инструмент для удаления данных без возможности восстановления обычными программными средствами.

Приложение Kaspersky позволяет удалять данные без возможности восстановления со следующих носителей информации:

- Локальные диски. Удаление возможно, если у вас есть права на запись и удаление информации.
- Внешние диски или другие устройства, которые распознаются как внешние диски (например, дискеты, карты памяти, USB-карты или мобильные телефоны). Удаление данных с карт памяти возможно, если на них механически не включен режим защиты от записи.

Вы можете удалять те данные, доступ к которым разрешен под вашей учетной записью. Перед удалением данных требуется убедиться, что эти данные не используются работающими приложениями.

Чтобы удалить данные без возможности восстановления:

1. Откройте главное окно приложения Kaspersky.
2. Перейдите в раздел **Приватность**.
3. В блоке **Уничтожитель файлов** нажмите на кнопку **Выбрать файлы**.

   Откроется окно **Уничтожитель файлов**.

4. Нажмите на кнопку **Обзор** и в открывшемся окне **Выберите файлы для удаления** выберите папку или файл для удаления без возможности восстановления.

> Удаление системных файлов может вызвать сбои в работе операционной системы.

5. В раскрывающемся списке **Метод удаления данных** выберите нужный метод удаления данных.

> Для удаления данных с SSD- и USB-устройств рекомендуется применять методы **Быстрое удаление (рекомендуется)** или **ГОСТ Р 50739-95, Россия**. Остальные методы удаления могут нанести вред SSD- или USB-устройству.

- **Быстрое удаление (рекомендуется)**. Процесс удаления состоит из двух циклов перезаписи данных: записи нулей и псевдослучайных чисел. Основное достоинство этого алгоритма – скорость выполнения. Быстрое удаление позволяет предотвратить восстановление данных с помощью стандартных утилит восстановления.

- **ГОСТ Р 50739-95, Россия**. Алгоритм проводит один цикл перезаписи данных псевдослучайными числами и защищает от восстановления данных стандартными средствами. Этот алгоритм соответствует второму классу защищенности из шести по классификации Государственной технической комиссии.

- **Алгоритм Брюса Шнайера**. Процесс состоит из семи циклов перезаписи данных. Метод отличается от немецкого VSITR последовательностью перезаписи. Этот усовершенствованный метод удаления информации считается одним из наиболее надежных.

- **Стандарт VSITR, Германия**. Проводятся семь циклов перезаписи данных. Алгоритм считается надежным, но его выполнение занимает значительное время.

- **Стандарт NAVSO P-5239-26 (MFM), США** и **Стандарт NAVSO P-5239-26 (RLL), США**. Используются три цикла перезаписи данных. Стандарты различаются последовательностью перезаписи информации.

- **Стандарт 5250.22-M, США**. Используются три цикла перезаписи. Этот стандарт применяется Министерством обороны США.

6. Нажмите на кнопку **Удалить**.

7. В открывшемся окне подтверждения удаления нажмите на кнопку **Удалить**.

Файлы, используемые сторонним приложением, не могут быть удалены.

Удаление следов активности

Доступно только в Kaspersky Standard, Kaspersky Plus и Kaspersky Premium.

При работе на компьютере действия пользователя регистрируются в операционной системе. При этом сохраняется следующая информация:

- данные о введенных пользователем поисковых запросах и посещенных сайтах;
- сведения о запуске приложений, открытии и сохранении файлов;
- записи в системном журнале Microsoft Windows;
- другая информация о действиях пользователя.

Сведения о действиях пользователя, содержащие конфиденциальные данные, могут оказаться доступными злоумышленникам и посторонним лицам.

В состав приложения входит мастер устранения следов активности пользователя в операционной системе.

Чтобы запустить мастер устранения следов активности:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Приватность**.
3. В блоке **Удаление следов активности** нажмите на кнопку **Поиск изменений**.

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**.

Удаление следов активности

Мастер выполняет действия, выбранные на предыдущем шаге. Удаление следов активности может занять некоторое время. Для устранения некоторых следов активности может потребоваться перезагрузка компьютера, о чем мастер вас уведомит.

После устранения следов активности мастер автоматически перейдет к следующему шагу.

Завершение работы мастера

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

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 приложения Kaspersky вы можете защитить от кражи свои персональные данные:

- пароли, имена пользователя и другие регистрационные данные;

- номера счетов и банковских карт.

В состав приложения Kaspersky входят компоненты и инструменты, позволяющие защитить ваши персональные данные от кражи злоумышленниками, использующими такие методы как фишинг и перехват данных, вводимых с клавиатуры.

Для защиты от фишинга предназначен Анти-Фишинг, включенный в состав компонентов Интернет-защита 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 – приложений, регистрирующих нажатие клавиш. Экранная клавиатура позволяет избежать перехвата данных, вводимых с клавиатуры.

Многие приложения-шпионы обладают функциями снятия снимков экрана, которые автоматически передаются злоумышленнику для последующего анализа и извлечения персональных данных пользователя. Экранная клавиатура защищает вводимые персональные данные от перехвата посредством снятия снимков экрана.

Экранная клавиатура имеет следующие особенности:

- На клавиши Экранной клавиатуры нужно нажимать с помощью мыши.

- В отличие от настоящей клавиатуры, на Экранной клавиатуре невозможно одновременно нажать несколько клавиш. Поэтому, чтобы использовать комбинации клавиш (например, **ALT**+**F4**), нужно сначала нажать на первую клавишу (например, **ALT**), затем на следующую (например, **F4**), а затем повторно нажать на первую клавишу. Повторное нажатие заменяет отпускание клавиши на настоящей клавиатуре.

- На Экранной клавиатуре язык ввода переключается с помощью того же сочетания клавиш, которое установлено в настройках операционной системы для обычной клавиатуры. При этом на вторую клавишу нужно нажимать правой клавишей мыши (например, если в настройках операционной системы для переключения языка ввода задана комбинация **LEFT ALT**+**SHIFT**, то на клавишу **LEFT ALT** нужно нажимать левой клавишей мыши, а на клавишу **SHIFT** нужно нажимать правой клавишей мыши).

Для защиты данных, вводимых с помощью Экранной клавиатуры, после установки приложения Kaspersky 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.

- Приложение Kaspersky не защищает от создания снимков экрана в операционной системе Microsoft Windows 8 и 8.1 (только 64-разрядные), если открыто окно Экранной клавиатуры, но не запущен процесс Защищенного браузера.

Как открыть Экранную клавиатуру

Открыть Экранную клавиатуру можно следующими способами:

- 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 приложение Kaspersky отключает функцию автозаполнения полей ввода на сайтах.

- с помощью комбинации клавиш аппаратной клавиатуры.

Запуск Экранной клавиатуры из панели инструментов браузера

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

1. Нажмите на кнопку **Kaspersky Protection** в панели инструментов браузера.
2. В раскрывшемся меню выберите пункт **Экранная клавиатура**.

Запуск Экранной клавиатуры с помощью аппаратной клавиатуры

Чтобы открыть Экранную клавиатуру с помощью аппаратной клавиатуры,

нажмите комбинацию клавиш **CTRL+ALT+SHIFT+P**.

Экранная клавиатура не запускается при нажатии на эту комбинацию клавиш, если эта комбинация клавиш уже зарегистрирована в другом приложении, например, Microsoft Word.

Как настроить отображение значка Экранной клавиатуры

Чтобы настроить отображение значка быстрого вызова Экранной клавиатуры в полях ввода на сайтах:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки приватности**.
4. В окне **Настройки приватности** нажмите на кнопку **Защита ввода данных**.

   В окне отобразятся настройки защиты ввода данных.

5. В блоке **Экранная клавиатура** установите флажок **Открывать Экранную клавиатуру по комбинации клавиш CTRL+ALT+SHIFT+P**.

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

7. Если вы хотите, чтобы значок вызова Экранной клавиатуры отображался только при открытии сайтов определенных категорий, установите флажки для категорий сайтов, на которых нужно отображать значок вызова Экранной клавиатуры в полях ввода.

   Значок вызова Экранной клавиатуры будет отображаться при открытии сайта, относящегося к какой-либо из выбранных категорий.

8. Если вы хотите включить или выключить отображение значка вызова Экранной клавиатуры на определенном сайте, выполните следующие действия:

   a. В блоке **Экранная клавиатура** по ссылке **Настройка исключений** 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".

Ограничения защиты ввода данных

Защита ввода данных в приложении Kaspersky имеет следующие ограничения:

- Защита ввода данных с аппаратной клавиатуры не работает в браузерах, запущенных в приложении Sandboxie.
- Защита ввода данных с аппаратной клавиатуры не может защитить ваши персональные данные в случае взлома сайта, требующего ввода таких данных, поскольку в этом случае информация попадет непосредственно в руки злоумышленников. Защита работает только в браузерах Microsoft Edge на 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 приложения установлен флажок **Поля ввода паролей на всех сайтах**.
  - Чтобы проверить, установлен ли флажок, перейдите в раздел **Настройки приватности** → **Настройки Защиты ввода данных** → блок **Защита ввода данных с аппаратной клавиатуры**.
- Защита работает только для полей, удовлетворяющих условиям:
  - Поле ввода однострочное, соответствует HTML-тегу <input>.
  - Поле ввода не скрытое: значение атрибута type не равно hidden, в CSS-стилях у поля display не установлено значение none.
  - Поля ввода не являются полями типа submit, radio, checkbox, button, image.

- Поле ввода не должно быть только для чтения (readOnly).
- Поле ввода должно быть доступно для ввода (получать фокус).
- Если поле имеет атрибут максимальной длины (maxlength), минимальное количество вводимых символов должно быть больше трех.

- Защита не работает в следующих случаях:
  - Ввод осуществляется с применением технологии IME.
  - Поле ввода не является полем ввода пароля.

После установки приложения Kaspersky и до первой перезагрузки компьютера приложение не перехватывает первый введенный пользователем символ (в любом приложении).

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:

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

   Откроется окно **Настройка**.
3. Перейдите в раздел **Настройки приватности**.
4. Нажмите на кнопку **Защита ввода данных**.

   Откроется окно **Настройки защиты ввода данных**.
5. В нижней части окна в блоке **Защита ввода данных с аппаратной клавиатуры** установите флажок **Защищать ввод данных с аппаратной клавиатуры**.
6. Установите флажки для категорий сайтов, на которых нужно защищать 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

Приложение Kaspersky 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 приложение Kaspersky отображает один из следующих значков:

– если веб-страница, которая открывается по ссылке, безопасна по данным "Лаборатории Касперского";

– если нет информации о безопасности веб-страницы, которая открывается по ссылке;

– если веб-страница, которая открывается по ссылке, по данным "Лаборатории Касперского" может быть использована злоумышленниками для нанесения вреда компьютеру или вашим данным;

– если веб-страница, которая открывается по ссылке, по данным "Лаборатории Касперского" может быть заражена или взломана;

– если веб-страница, которая открывается по ссылке, опасна по данным "Лаборатории Касперского".

При наведении курсора мыши на значок отображается всплывающее окно с более подробным описанием ссылки.

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

Чтобы настроить проверку ссылок на сайтах:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки безопасности**.
4. Нажмите на кнопку **Интернет-защита**.

   Откроется окно **Настройки Интернет-защиты**.
5. По ссылке **Расширенная настройка** раскройте блок дополнительных настроек Интернет-защиты.
6. В блоке **Проверка ссылок** установите флажок **Проверять ссылки**.
7. Чтобы приложение Kaspersky проверяло содержимое всех сайтов, выберите вариант **На всех сайтах, кроме указанных**.
8. Если необходимо, укажите веб-страницы, которым вы доверяете, в окне **Исключения**. Окно открывается по ссылке **Настроить исключения**. приложение Kaspersky не будет проверять содержимое указанных веб-страниц.
9. Чтобы приложение Kaspersky проверяло 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* – приложение Kaspersky проверяет содержимое веб-страницы).

   f. Нажмите на кнопку **Добавить**.

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

10. Если вы хотите указать дополнительные настройки проверки ссылок, в окне **Дополнительные настройки Интернет-защиты** в блоке **Проверка ссылок** по ссылке **Настроить проверку ссылок** разверните блок настроек **Проверяемые ссылки**.

11. Чтобы приложение Kaspersky предупреждало о безопасности ссылок на всех веб-страницах, в блоке **Проверяемые ссылки** выберите вариант **Любые ссылки**.

12. Чтобы приложение Kaspersky отображало 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.

Приложение Kaspersky 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 приложение Kaspersky выполняет проверку таких соединений по запросу компонентов защиты, таких как Почтовый Антивирус, Анти-Спам, Безопасные платежи, Проверка ссылок, Защита от сбора данных в интернете, Интернет-защита и Анти-Баннер.

Чтобы изменить настройки защищенных соединений:

1. Откройте главное окно приложения.

2. Нажмите на кнопку  в нижней части главного окна.

   Откроется окно **Настройка**.

3. Перейдите в раздел **Настройки безопасности**.

4. В блоке **Расширенные настройки** нажмите на кнопку **Настройки сети**.

5. В окне **Настройки сети** перейдите в раздел **Проверка защищенных соединений**.

6. Выберите вариант действия при подключении к сайтам по защищенному соединению:

   - **Не проверять защищенные соединения**. Приложение Kaspersky не проверяет защищенные соединения.

- **Проверять защищенные соединения по запросу компонентов защиты**. Приложение Kaspersky проверяет защищенные соединения, только если на это будет запрос от компонента Проверка ссылок. Этот вариант действия выбран по умолчанию.

- **Всегда проверять защищенные соединения**. Приложение Kaspersky всегда проверяет защищенные соединения.

По ссылке **Показать сертификаты** открывается окно со списком доверенных сертификатов, которые используются популярными сайтами. Сертификаты добавляются в этот список, если при посещении какого-либо сайта вы нажимаете на кнопку **Добавить в доверенные и продолжить** в уведомлении приложения Kaspersky. После добавления сертификата в список, сайт будет считаться доверенным. Вы можете добавить или удалить сертификаты в окне **Доверенные корневые сертификаты** с помощью кнопок **Добавить** или **Удалить**.

Если у вас на компьютере несколько учетных записей, и один из пользователей принял новый сертификат, для других пользователей он также будет добавлен в список доверенных сертификатов.

7. Выберите вариант действия, если возникают ошибки при проверке защищенных соединений:

   - **Игнорировать**. Если выбран этот вариант, приложение Kaspersky разрывает соединение с сайтом, на котором возникла ошибка проверки защищенного соединения.

   - **Спрашивать**. Если выбран этот вариант, при возникновении ошибки проверки защищенного соединения с сайтом, приложение Kaspersky показывает уведомление, в котором вы можете выбрать вариант действия:

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

     - **Добавить домен в исключения**. Если выбран этот вариант, приложение Kaspersky добавляет адрес сайта в список доверенных адресов. Приложение Kaspersky не проверяет защищенные соединения на сайтах, которые входят в список доверенных адресов. Такие сайты можно посмотреть по ссылке **Доверенные адреса**.

     Этот вариант выбран по умолчанию.

   - **Добавить домен в исключения**. Если выбран этот вариант, приложение Kaspersky добавляет сайт в список доверенных адресов. Приложение Kaspersky не проверяет защищенные соединения на сайтах, которые входят в список доверенных адресов. Такие сайты отображаются в окне **Доверенные адреса**, которое можно открыть по ссылке **Доверенные адреса**.

8. По ссылке **Доверенные адреса** откройте окно **Доверенные адреса** и выполните следующие действия:

    a. Нажмите на кнопку **Добавить**, чтобы добавить сайт в список исключений из проверки защищенных соединений.

    b. Укажите доменное имя сайта в поле **Доменное имя**.

    c. Нажмите на кнопку **Добавить**.

    Приложение Kaspersky не будет проверять защищенное соединение с этим сайтом. Обратите внимание, что добавление сайта в список доверенных адресов означает, что функциональность проверки этого сайта такими компонентами, как Безопасные платежи, Проверка ссылок, Защита от сбора данных в интернете, Интернет-защита и Анти-Баннер, может быть ограничена.

О безопасном подключении к сетям Wi-Fi

Доступно только в Kaspersky Plus и Kaspersky Premium.

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

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

Чтобы использовать компонент Безопасное VPN-соединение, вам нужно запустить приложение Kaspersky Secure Connection. Kaspersky Secure Connection устанавливается совместно с приложением Kaspersky в плане Kaspersky Plus.

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 или города 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.

Настройка уведомлений об уязвимостях сети Wi-Fi

Если на вашем компьютере не установлен Kaspersky Secure Connection, приложение Kaspersky 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 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 приложении Kaspersky Secure Connection .

Чтобы настроить уведомления об уязвимостях сети Wi-Fi:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Настройки безопасности**.
4. Выберите компонент **Сетевой экран**.

   В окне отобразятся настройки компонента Сетевой экран.

5. Установите флажок **Уведомлять об уязвимостях при подключении к сети Wi-Fi**, если вы хотите получать уведомления при подключении к уязвимым сетям Wi-Fi. Если вы не хотите получать уведомления, снимите этот флажок. Флажок доступен для изменения, если на компьютере не установлено приложение Kaspersky Secure Connection.

6. По ссылке **Выбрать категории** укажите типы уязвимостей сетей Wi-Fi, При подключении к сети Wi-Fi с указанной уязвимостью приложение Kaspersky предупредит вас об этом.

7. Если флажок **Уведомлять об уязвимостях при подключении к сети Wi-Fi** установлен, вы можете настроить дополнительные настройки отображения уведомлений:

    - Установите флажок **Запрещать передачу пароля в интернете в незащищенном виде и показывать уведомление**, чтобы блокировать передачу пароля в незащищенном текстовом виде при заполнении поля **Пароль** в интернете.

    - По ссылке **Включить** восстановите значения настроек отображения уведомлений о передаче пароля в незащищенном виде. Если ранее вы заблокировали отображение уведомлений о передаче пароля в незащищенном виде, эти уведомления снова будут отображаться.

При подключении к защищенным сетям Wi-Fi, приложение показывает уведомление, в котором спрашивает вас, доверять или нет новой сети. Вы можете выбрать один из вариантов действия:

- **Нет, запретить доступ к компьютеру извне**. Будут блокироваться все внешние соединения этой сети, кроме соединений, инициированных с вашего устройства. Вы сможете пользоваться интернетом и заходить на любые сайты. Другие пользователи данной сети не смогут подключаться к ресурсам вашего компьютера (например не получат доступ к содержимому дисков, включая общие папки).

- **Ограничить, разрешив общий доступ**. Вы сможете пользоваться интернетом и заходить на любые сайты. Другим пользователям этой сети будет заблокирован доступ к ресурсам вашего компьютера, кроме ресурсов, отмеченных как общие (например, общие папки).

- **Да, разрешить любую сетевую активность**. Любые соединения этой сети будут разрешены. Вы сможете пользоваться интернетом и заходить на любые сайты. Другие пользователи сети смогут подключаться к вашему компьютеру без ограничений (например, получать доступ к содержимому дисков).

Премиальные функции

В этом разделе вы можете прочитать, какие функции вам доступны, если вы используете Kaspersky Premium.

Премиальная техническая поддержка

Премиальная техническая поддержка по телефону доступна не во всех регионах.

Помощь наших специалистов в установке приложения

Если у вас возникли проблемы с установкой приложения на компьютер, вы можете позвонить нам и специалисты "Лаборатории Касперского" удаленно:

- запустят установку приложения;
- убедятся, что установка приложения прошла без ошибок;
- расскажут о функциональности и настройках приложения;
- ответят на любые ваши вопросы о приложении и его установке;
- выполнят настройку приложения исходя из ваших потребностей;
- убедятся, что приложение установлено, настроено и корректно работает.

Обращение в Службу технической поддержки без очереди

Вы можете обратиться без очереди к сотруднику Службы технической поддержки по телефону или в чате. Ваш звонок будет обработан с высоким приоритетом. Также вы можете написать сотруднику Службы технической поддержки в чат-приложение, с помощью которого специалисты "Лаборатории Касперского" могут помочь вам удаленно.

Удаленная поддержка

В один клик вы можете связаться со специалистом "Лаборатории Касперского", который при необходимости подключится к вашему компьютеру и поможет решить вашу проблему удаленно!

Поиск и удаление вирусов

Профессиональная помощь в поиске и удалении вирусов и приложений-шпионов с компьютера, на котором установлено приложение "Лаборатории Касперского".

Проверка исправности компьютера

Наши специалисты проведут тщательный анализ вашего устройства, чтобы гарантировать его высокую производительность и безопасность.

Чтобы воспользоваться премиальной технической поддержкой, позвоните по номеру телефона в регионе, в котором вы приобрели подписку на приложение Kaspersky Premuim.

Безопасное хранение документов

Если вы храните на компьютере важные документы, например сканы паспортов, справки, договора и так далее, мы рекомендуем вам добавить эти документы в безопасное хранилище. Хранилище – это зашифрованный файл, доскуп к которому предоставляемся только после ввода мастер-пароля. Это гарантирует безопасность ваших персональных данных, так как постороние люди не смогут получить доступ к этим документам.

О мастер-пароле

Мастер-пароль – это единый пароль, который приложение Kaspersky использует для шифрования ваших данных в хранилище. Мы рекомендуем использовать мастер-пароль из восьми или более символов, содержащий прописные и строчные буквы, а также цифры и специальные символы.

Для обеспечения безопасности приложение Kaspersky не хранит мастер-пароль на ваших устройствах и не передает его в облачное хранилище. Мы рекомендуем запомнить или записать мастер-пароль и хранить его в безопасном месте, так как восстановить забытый пароль невозможно.

О шифровании

Приложение Kaspersky шифрует данные, используя алгоритм симметричного шифрования, основанный на стандарте Advanced Encryption Standard (AES). Ключ высчитывается из вашего мастер-пароля на основании Password-Based Key Derivation Function 2 (PBKDF2). Алгоритм AES используется по всему миру для защиты секретных данных. Этот алгоритм обладает минимальными требованиями к оперативной памяти, поэтому ваши данные зашифровываются и расшифровываются за секунды.

Чтобы добавить документы в хранилище:

Защита от кражи личных данных

Подписка Kaspersky Premuim включает защиту от кражи личных данных, предоставляемую международной компанией Iris Powered by Generali, специализирующейся на кибербезопасности и защите от кражи личных данных.

> Проверьте, доступна ли защита от кражи личных данных в вашем регионе.

Услуги по защите от кражи личных данных

> Обращение по телефону доступно не во всех регионах.

Специалисты колл-центра по защите от кражи личных данных работают круглосуточно, чтобы помочь вам восстановить украденные личные данные и предотвратить дальнейший ущерб от такой кражи.

- Помощь в случае кражи или потери бумажника. Мы свяжемся с вашим банком, чтобы заблокировать и / или перевыпустить ваши банковские карты, а в случае утери водительского удостоверения, карточки социального страхования или паспорта мы обратимся от вашего лица в органы власти, выдавшие эти документы, чтобы начать процесс их замены.

- Сокращение количества предложений о кредитовании. Мы поможем вам защитить свои личные данные, сократив количество поступающим вам предложений о выпуске одобренной кредитной карты, которые могут рассылаться мошенниками с целью кражи ваших личных данных.

- Удаление из списков рекламных рассылок. Мы поможем сократить количество писем с предложением оформить кредитную карту и поступающих вам телефонных звонков с рекламными предложениями. Такие предложения могут являться попытками мошенников украсть ваши личные данные.

- Защита от мошенничества при оформлении кредита. Если ваши личные данные были похищены, вы можете подать онлайн-заявку о проверке на мошенничество при оформлении любого кредита на ваше имя в течение года. Таким образом мошенники не смогут оформить кредит на ваше имя, воспользовавшись вашими личными данными.

- Полное восстановление утраченных документов. Если вы или ваши близкие, включенные в страховку, станут жертвой кражи личных данных или мошенничества, специально выделенный сотрудник поможет вам восстановить ваши личные данные (после составления полицейского протокола, оформления доверенности на имя страховой компании, а также заполнения заявления о краже личных данных). Внимание: доступность этой услуги зависит от региона и местного законодательства.

- Решение споров с кредиторами, уведомление и поддержка. В тех регионах, где есть такая возможность, мы свяжемся со специалистами отдела по борьбе с мошенничеством вашего банка и направим им детальный отчет по каждому эпизоду мошенничества. Мы будем следить за ходом каждого такого дела и регулярно уведомлять вас о результатах разбирательства с помощью специальных статус-отчетов.

- Уведомление полиции и органов власти. Мы поможем вам обратиться в полицию и органы власти в случае мошенничества с личными данными, а также направим отчет о мошеннических действиях вашим кредиторам.

- Помощь при краже данных медицинского страхования. В тех регионах, где есть такая возможность, в случае кражи ваших данных медицинского страхования, мы поможем решить вопрос, если на ваше имя будет незаконно выставлен счет за оказание медицинских услуг или если кто-либо незаконно получит медицинскую помощь, воспользовавшись вашей медицинской страховкой. Также мы убедимся, что ваши медицинские счета и записи о прохождении лечения были исправлены, при необходимости привлекая для этого наших собственных медицинских работников.

- Помощь во время дальних поездок. Если кража личных данных произошла во время дальней поездки (более 100 миль от места проживания), мы окажем вам помощь в покупке авиабилетов, бронировании гостиниц и аренде автомобиля.

- Аванс наличными в случае непредвиденных обстоятельств. Если кража личных данных произошла на расстоянии более 100 миль от места вашего постоянного проживания, мы предоставим вам аванс наличными в размере 500 долларов. Все траты в рамках этой суммы вы совершаете на свое усмотрение. Эта услуга предоставляется при наличии действующей кредитной карты. В случае, если вы не предоставили действующую кредитную карту и получили такой аванс, эта сумма будет взыскана со счета вашей кредитной организации в пользу страховой компании в течение 30 дней с даты выдачи вам аванса, при этом вы обязуетесь погасить долг перед кредитной организацией в течение 45 дней, начиная с даты получения вами аванса. По истечении этого срока в случае непогашения долга вы должны будете заплатить процент с этой суммы по ставке 1,5% в месяц. Страховая компания сохраняет за собой право не предоставлять вам аванс наличными если у вас отсутствует действующая кредитная карта.

> Наличие вышеперечисленных услуг зависит от региона вашего местонахождения.

Страхование от кражи личных данных

Воспользовавшись страховкой от кражи личных данных, вы можете защитить себя от финансовых трат, связанных с восстановлением личных данных. Позвольте себе спать спокойно, зная, что в случае кражи или потери личных данных вы получите 1 миллион долларов на восстановление украденных личных данных и покрытие издержек.

Страховка от кражи личных данных предоставляется в рамках единого контракта группового страхования, выпущенного компанией Generali US Branch в пользу Generali Global Assistance, Inc. Перечисленные здесь условия служат для целей информирования и не включают все пункты, условия и исключения договора страхования. Страховое покрытие предоставляется не во всех юрисдикциях. Участники программы страхования должны уточнять подробную информацию об условиях страхования и о положенных им выплатах непосредственно в договоре страхования. Компания Generali US Branch (New York, NY; NAIC # 11231) работает под следующими названиями: Generali Assicurazioni Generali S.P.A. (U.S. Branch) в Калифорнии, Assicurazioni Generali – U.S. Branch в Колорадо, Generali U.S. Branch DBA The General Insurance Company of Trieste & Venice в Орегоне, и The General Insurance Company of Trieste and Venice – U.S. Branch в Вирджинии. Generali US Branch имеет лицензию на операционную деятельность во всех Соединенных Штатах и в Округе Колумбия.

Доступность вышеперечисленных функций зависит от региона.

Помощь в предотвращении мошенничества

Мошенники используют различные методы для кражи ваших денег. Они могут отправлять вам фальшивые счета на оплату или попросить оплатить поддельный онлайн-заказ. Если вы сомневаетесь, является ли какое-либо предложение действительным, вы можете позвонить нам, и мы проверим это предложение.

Предотвращение мошенничества и поддержка включают:

- ScamAssist. Если вы получили сообщение или предложение, которое выглядит подозрительно или звучит слишком хорошо, чтобы быть правдой, специалисты ScamAssist проанализируют такое сообщение или предложение и предупредят вас в случае, если оно является мошенническим, предотвратив таким образом кражу ваших денег и личных данных.

Поставщик услуги страхования не отвечает за наличие, безопасность, точность и эффективность конкретных способов, продуктов, инструментов или ресурсов, которые используются в рамках услуги Предотвращение мошенничества и поддержка. Вы берете на себя ответственность за использование услуги Предотвращение мошенничества и поддержка.

Как удалить несовместимые приложения

Приложение Kaspersky регулярно проверяет ваш компьютер на наличие несовместимых приложений. Такие приложения добавляются в список несовместимых приложений. Вы можете просмотреть этот список и принять решение, как поступить с несовместимыми приложениями.

Рекомендуется удалять с компьютера несовместимые приложения, иначе приложение Kaspersky не сможет защитить ваш компьютер в полной мере.

Причины несовместимости стороннего приложения с приложением Kaspersky могут быть следующие:

- Приложение конфликтует с Файловым Антивирусом.
- Приложение конфликтует с Сетевым экраном.
- Приложение конфликтует с Анти-Спамом.
- Приложение препятствует защите сетевого трафика.
- Приложение конфликтует с Секретной папкой.
- Приложение конфликтует с Kaspersky Password Manager.

Как удалить несовместимые приложения

Чтобы удалить несовместимые приложения:

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

   Откроется окно **Центр уведомлений**.
3. В разделе **Советы** в строке с сообщением о найденных несовместимых приложениях нажмите на кнопку **Показать**.

   Откроется окно **Несовместимое программное обеспечение** со списком найденных несовместимых приложений.
4. Оставьте флажки напротив названий несовместимых приложений, которые нужно удалить, и нажмите **Удалить**. Удаление выполняется с помощью средств удаления, предоставляемых этими приложениями. В процессе удаления от вас может потребоваться согласие на удаление или изменение настроек, связанных с удалением приложений.
5. Если на компьютере остались несовместимые приложения, которые невозможно удалить автоматически, откроется окно со списком таких приложений. Чтобы

удалить несовместимые приложения вручную, нажмите **Удалить вручную**. Откроется стандартное окно операционной системы со списком установленных приложений. Удалите несовместимые приложения в соответствии с инструкциями для вашей операционной системы.

6. После удаления несовместимых приложений перезагрузите компьютер.

Работа с приложением из командной строки

Вы можете работать с приложением Kaspersky с помощью командной строки.

Синтаксис командной строки:

```
avp.com <команда> [параметры]
```

Для просмотра справочной информации о синтаксисе командной строки предусмотрена команда:

```
avp.com [ /? | HELP ]
```

Эта команда позволяет получить полный список команд, доступных для работы с приложением Kaspersky через командную строку.

Для получения справочной информации о синтаксисе конкретной команды вы можете воспользоваться одной из следующих команд:

```
avp.com <команда> /?
avp.com HELP <команда>
```

Обращаться к приложению через командную строку следует из папки установки приложения либо с указанием полного пути к avp.com.

Вы можете включать и выключать запись событий приложения (создание файлов трассировки) через командную строку, если ранее вы установили пароль на защиту доступа к управлению приложением Kaspersky в окне настройки приложения.

Если вы не установили пароль в окне настройки приложения, вы не сможете создать пароль и включить запись событий из командной строки.

Некоторые команды можно выполнить только под учетной записью администратора.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или в других источниках информации о приложении, рекомендуется обратиться в Службу технической поддержки. Посетите сайт Службы технической поддержки, чтобы связаться с нашими экспертами, которые ответят на ваши вопросы об установке и использовании приложения.

> Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

Техническая поддержка предоставляется только пользователям, которые приобрели подписку на использование приложения. Пользователям бесплатных версий техническая поддержка не предоставляется.

Сбор информации для Службы технической поддержки

После того как вы проинформируете специалистов Службы технической поддержки о возникшей проблеме, они могут попросить вас сформировать отчет с информацией об операционной системе и отправить его в Службу технической поддержки. Также специалисты Службы технической поддержки могут попросить вас создать файл трассировки. Файл трассировки позволяет отследить процесс пошагового выполнения команд приложения и обнаружить, на каком этапе работы приложения возникает ошибка.

Для более эффективного оказания поддержки в случае возникновения вопросов по работе приложения специалисты Службы технической поддержки могут попросить вас в отладочных целях на время проведения работ по диагностике изменить настройки приложения. Для этого может потребоваться выполнение следующих действий:

- Собрать расширенную диагностическую информацию.
- Выполнить более тонкую настройку работы отдельных компонентов приложения, недоступную через стандартные средства пользовательского интерфейса.
- Изменить настройки хранения и отправки собираемой диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

Вся необходимая для выполнения перечисленных действий информация (описание последовательности шагов, изменяемые настройки, конфигурационные файлы, скрипты, дополнительные возможности командной строки, отладочные модули, специализированные утилиты и т. д.), а также состав собираемых в отладочных целях данных будут сообщены вам специалистами Службы технической поддержки. Собранная расширенная диагностическая информация сохраняется на компьютере пользователя. Автоматическая пересылка собранных данных в "Лабораторию Касперского" не выполняется.

Перечисленные выше действия должны выполняться только под руководством специалистов Службы технической поддержки по полученным от них инструкциям. Самостоятельное изменение настроек работы приложения способами, не описанными в справке или в рекомендациях специалистов Службы технической поддержки, может привести к замедлению и сбоям в работе операционной системы, снижению уровня защиты компьютера, а также к нарушению доступности и целостности обрабатываемой информации.

О составе и хранении служебных файлов данных

Файлы трассировки и дампов хранятся на вашем компьютере в открытом виде в течение семи дней с момента выключения записи данных. По истечении семи дней файлы трассировки и дампов безвозвратно удаляются.

Файлы трассировки хранятся в папке ProgramData\Kaspersky Lab.

Файлы трассировки имеют следующие названия: `KAV<номер версии_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 приложения и трассировку производительности:

1. Откройте главное окно приложения.

2. Нажмите на кнопку в нижней части окна.

   Откроется окно **Поддержка**.

3. По ссылке **Мониторинг проблем** откройте окно **Мониторинг проблем**.

4. Включите и настройте трассировку приложения и трассировку производительности в соответствии с инструкциями специалиста Службы технической поддержки "Лаборатории Касперского".

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Ограничения и предупреждения

Приложение Kaspersky имеет ряд некритичных для работы 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 модулей приложения. Также в автоматическом режиме обновляются правила Сетевого экрана, Защиты веб-камеры, Менеджера приложений, Предотвращения вторжений.

Если проверка устройства запускается с My Kaspersky, файлы будут обработаны в автоматическом режиме по правилам, заданным в приложении. 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 приложение может обращаться за информацией в Kaspersky Security Network. Если данные из Kaspersky Security Network получить не удалось, приложение принимает решения на основании локальных антивирусных баз.

Ограничения функциональности Мониторинга активности

Функциональность противодействия приложениям-шифровальщикам (шифрование файлов пользователя вредоносным приложением) имеет следующие ограничения:

- Для обеспечения функциональности используется системная папка Temp. Если на системном диске, на котором расположена папка Temp, недостаточно свободного места для создания временных файлов, защита от приложений-шифровальщиков не предоставляется. При этом уведомление о невыполнении копирования (непредоставлении защиты) не выводится.

- Временные файлы удаляются автоматически при завершении работы приложения Kaspersky или отключении компонента Мониторинг активности.

- В случае нештатного завершения работы приложения Kaspersky временные файлы автоматически не удаляются. Чтобы удалить временные файлы, необходимо вручную очистить папку Temp. Для этого откройте окно **Выполнить** и в поле **Открыть** введите `%TEMP%`. Нажмите на кнопку **OK**.

- Защита от приложений-шифровальщиков выполняется только для файлов, расположенных на носителях информации, отформатированных в файловой системе NTFS.

- Количество подлежащих восстановлению файлов не должно превышать 50 на один процесс шифрования.

- Суммарный объем изменений в файлах не должен превышать 100 МБ. Файлы, изменения в которых превышают этот лимит, не подлежат восстановлению.

- Не контролируются изменения файлов, инициированные через сетевой интерфейс.

- Не поддерживаются файлы, зашифрованные системой EFS.

- Для включения защиты от приложений-шифровальщиков после установки приложения Kaspersky требуется перезагрузить компьютер.

Ограничения функциональности проверки защищенных соединений

В связи с техническими ограничениями реализации алгоритмов проверки проверка защищенных соединений не поддерживает некоторые расширения протокола TLS 1.0 и выше (в частности NPN и ALPN). Подключение по этим протоколам может быть ограничено. Браузеры с поддержкой протокола SPDY используют вместо SPDY протокол HTTP поверх TLS, даже если сервер, к которому выполняется подключение, поддерживает SPDY. При этом уровень защиты соединения не снижается. Если сервер поддерживает только протокол SPDY, и возможность установить соединение с помощью протокола HTTPS отсутствует, приложение не будет контролировать установленное соединение.

Приложение Kaspersky не поддерживает обработку трафика, передаваемого через HTTPS/2 Proxy. Также приложение не обрабатывает трафик, передаваемый через расширения протокола HTTP/2.

Приложение Kaspersky препятствует обмену данными по протоколу QUIC. Браузеры используют стандартный транспортный протокол (TLS или SSL) независимо от того, включена в браузере поддержка протокола QUIC или нет.

Приложение Kaspersky контролирует только те защищенные соединения, которые оно может расшифровать. Приложение не контролирует соединения, добавленные в список исключений (ссылка **Сайты** в окне **Настройки сети**).

Проверка и расшифровка зашифрованного трафика по умолчанию выполняется следующими компонентами:

- Интернет-защита;
- Безопасные платежи;
- Проверка ссылок.

Приложение Kaspersky расшифровывает зашифрованный трафик при работе пользователя в браузере Google Chrome, если в этом браузере отсутствует или выключено расширение Kaspersky Protection.

Приложение Kaspersky 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, приложение Kaspersky определяет сертификат, использующийся для установления HTTPS-соединения этого клиента с сервером, как недоверенный. Чтобы этого не происходило, настройте почтовый клиент The Bat на работу с локальным хранилищем сертификатов Windows (Windows Certificate Store).

Ограничения исключений из проверки защищенных соединений

При проверке защищенных соединений с сайтами, добавленными в исключения, некоторые компоненты, в частности Анти-Баннер, Проверка ссылок и Защита от сбора данных в интернете, могут продолжать проверять защищенные соединения. Компоненты Безопасные платежи и Интернет-защита не проверяют сайты, добавленные в исключения.

Ограничения Резервного копирования

Резервное копирование имеет следующие ограничения:

- Онлайн-хранилище резервных копий становится недоступным при смене жесткого диска или при переходе на новый компьютер. Информацию о том, как восстановить подключение к Онлайн-хранилищу при смене оборудования, смотрите на сайте Службы технической поддержки "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 приложение выполняет резервное копирование через системную службу теневого копирования, автономный файл данных Outlook (OST) не попадает в резервную копию, так как он не предназначен для резервного копирования.

Ограничение функциональности Секретная папка

При создании секретной папки в файловой системе FAT32 размер файла секретной папки на диске не должен превышать 4 ГБ.

Особенности проверки памяти ядра на наличие руткитов во время работы в Защищенном браузере

В случае обнаружения недоверенного модуля во время работы Защищенного браузера открывается новая вкладка браузера с уведомлением о том, что была обнаружена вредоносное приложение. В этом случае рекомендуется закрыть браузер и выполнить полную проверку компьютера.

Особенности защиты данных буфера обмена

Приложение Kaspersky разрешает приложению обращаться к буферу обмена в следующих случаях:

- Приложение с активным окном пытается поместить данные в буфер обмена. Активным считается окно, с которым вы работаете в настоящий момент.

- Защищенный процесс приложения пытается поместить данные в буфер обмена.

- Защищенный процесс приложения или процесс с активным окном пытается получить данные из буфера обмена.

- Данные из буфера обмена пытается получить процесс приложения, который ранее сам поместил эти данные в буфер обмена.

Особенности обработки зараженных файлов компонентами приложения

Приложение по умолчанию может удалять зараженные файлы, если их лечение невозможно. Удаление по умолчанию может выполняться при обработке файлов такими компонентами, как Предотвращение вторжений, Почтовый Антивирус, Файловый Антивирус, при выполнении задач проверки, а также при обнаружении опасной активности приложений компонентом Мониторинг активности.

Ограничения работы некоторых компонентов при совместной установке приложения с Kaspersky Fraud Prevention for Endpoints

Работа следующих компонентов приложения Kaspersky ограничивается в Защищенном браузере, если приложение установлено совместно с Kaspersky Fraud Prevention for Endpoints:

- Интернет-защита, 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 приложения Kaspersky при включенном режиме Device Guard на Microsoft Windows 10 RS4

Частично ограничена работа следующей функциональности:

- защита буфера обмена;
- защита браузера от приложений эмуляции ввода с клавиатуры и мыши (подмен вводимых данных);
- защита от приложений удаленного управления;

- защита браузера (управление через API, защита от атак при помощи опасных сообщений окнам браузера, защита от управления очередью сообщений);

- эвристический анализ (эмуляция запуска вредоносных приложений).

Если в операционной системе Windows включен режим работы UMCI, приложение Kaspersky не обнаруживает приложения блокировки экрана.

О записи событий, касающихся Лицензионного соглашения и Kaspersky Security Network, в журнал событий Windows

События принятия или отказа от условий Лицензионного соглашения, а также принятия или отказа от участия в Kaspersky Security Network записываются в журнал Windows.

Ограничения проверки репутации локальных адресов в Kaspersky Security Network

Ссылки, ведущие на локальные ресурсы, не проверяются в Kaspersky Security Network.

Предупреждение о приложениях сбора информации

Если у вас на компьютере установлено приложение, выполняющее сбор и отправку информации на обработку, приложение Kaspersky может классифицировать такое приложение как вредоносное. Чтобы избежать этого, вы можете исключить приложение из проверки, настроив приложение Kaspersky способом, описанным в этом документе.

Предупреждение о создании отчета об установке приложения

При установке приложения на компьютер создается файл отчета об установке. Если установка приложения завершилась с ошибкой, файл отчета об установке сохраняется, и вы можете отправить его в Службу поддержки "Лаборатории Касперского". Вы можете ознакомиться с содержимым файла отчета об установке по ссылке из окна приложения. В случае успешной установки приложения, файл отчета об установке сразу же удаляется с вашего компьютера.

Ограничения контроля веб-камеры на операционной системе Microsoft Windows 10 Anniversary Update (RedStone 1)

После установки приложения на операционной системе Microsoft Windows 10 Anniversary Update (RedStone 1) контроль доступа к веб-камере не гарантируется до перезагрузки компьютера.

Ограничение резервного копирования и восстановления данных из резервных копий

Невозможно одновременное выполнение задачи резервного копирования в приложении Kaspersky и задачи восстановления данных в утилите Kaspersky Restore Utility на одном компьютере.

Ограничения работы Сетевого экрана

Сетевой экран не контролирует локальные подключения, которые устанавливают контролируемые приложения.

Ограничения работы компонента Предотвращение вторжений

Если на вашем компьютере установлено приложение VeraCrypt, приложение Kaspersky может завершить работу при работе с компонентом Предотвращение вторжений. Для решения этой проблемы требуется обновить приложение VeraCrypt до версии 1.19 или выше.

Ограничение первого запуска приложения после обновления операционной системы Microsoft Windows 7 до Microsoft Windows 10

Если вы обновили операционную систему Microsoft Windows 7 до Microsoft Windows 8 / 8.1 или Microsoft Windows 10 / RS1 / RS2 / RS3, при первом запуске приложение Kaspersky работает со следующими ограничениями:

- Работает только Файловый Антивирус (постоянная защита). Остальные компоненты приложения не работают.
- Работает самозащита файлов и системного реестра. Самозащита процессов не работает.
- Интерфейс приложения недоступен до перезагрузки компьютера. Приложение показывает уведомление о том, что некоторые компоненты приложения не работают, и о том, что требуется перезагрузка компьютера после завершения адаптации к новой операционной системе.
- В контекстном меню значка в области уведомлений доступен только пункт **Выход**.
- Приложение не показывает уведомления и автоматически выбирает рекомендованное действие.

Предупреждение об ошибке адаптации драйверов приложения при обновлении операционной системы с Windows 7 до Windows 10

При обновлении Windows с версии 7 до версии 10 может произойти ошибка адаптации драйверов приложения Kaspersky. Адаптация драйверов происходит в фоновом режиме, вы не получаете оповещений о ее процессе.

В случае возникновения ошибки адаптации драйверов вы не сможете воспользоваться следующими функциями приложения:

- Сетевым экраном;
- функцией обнаружения угроз во время загрузки операционной системы;
- функцией защиты процессов приложения с помощью технологии Protected Process Light (PPL) от Microsoft.

Вы можете воспользоваться следующими способами исправления ошибки:

- перезагрузить компьютер и повторить адаптацию приложения из оповещения в Центре уведомлений;
- удалить и заново установить приложение.

Ограничения 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 приложение не проверяет трафик, передаваемый по протоколу HTTPS, если изменение настроек браузера защищено Основным паролем. При обнаружении Основного пароля в браузере, приложение показывает уведомление, в котором содержится ссылка на статью в Базе знаний. Статья содержит инструкцию для решения этой проблемы.

Если трафик, передаваемый по протоколу HTTPS, не контролируется, ограничена работа следующих компонентов:

- Интернет-защита;

- Анти-Фишинг;
- Родительский контроль;
- Защита приватности;
- Анти-Баннер;
- Защита ввода данных;
- Безопасные платежи.

Ограничения работы расширения Kaspersky Protection в браузерах Google Chrome и Mozilla Firefox

Расширение Kaspersky Protection не работает в браузерах Google Chrome и Mozilla Firefox, если на вашем компьютере установлено приложение Malwarebytes for Windows.

Особенности установки приложения на операционной системе Microsoft Windows 7 Service Pack 0 и Service Pack 1

При установке приложения на операционные системы, которые не поддерживают сертификаты с цифровой подписью SHA256, приложение устанавливает свой доверенный сертификат.

Об автоматическом тестировании функциональности приложений "Лаборатории Касперского"

В приложениях "Лаборатории Касперского", включая приложение Kaspersky, предусмотрен специальный API (application programming interface – интерфейс прикладного программирования) для автоматического тестирования функциональности приложения. Этот API предназначен исключительно для использования разработчиками "Лаборатории Касперского".

Другие источники информации о приложении

Страница приложения Kaspersky в Базе знаний

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

На странице приложения Kaspersky в Базе знаний вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании приложения.

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

Поддержка приложений "Лаборатории Касперского" на нашем Форуме

Вы можете получить поддержку от пользователей и экспертов "Лаборатории Касперского" на нашем Форуме.

На Форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения и получения помощи.

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.

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 приложение Kaspersky помещает приложение или процесс в зависимости от наличия электронной цифровой подписи приложения, репутации приложения в Kaspersky Security Network, доверия к источнику приложения и потенциальной опасности действий, которые выполняет приложение или процесс. На основании принадлежности приложения к группе доверия Kaspersky может накладывать ограничения на действия этого приложения в операционной системе.

В Kaspersky 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 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, 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.

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 антивирусных 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").

Секретная папка

Специальное хранилище данных, в котором файлы хранятся в зашифрованном виде. Для получения доступа к таким файлам требуется ввод пароля. Секретные папки служат для предотвращения несанкционированного доступа к данным пользователей.

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 приложения.

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 и Safari – товарные знаки Apple Inc., зарегистрированные в США и других странах.

Dropbox – товарный знак Dropbox, Inc.

Google, Google Chrome, Google Play, Chromium, SPDY, YouTube, 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.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

LogMeIn Pro и Remotely Anywhere – товарные знаки компании LogMeIn, Inc.

Mail.ru – зарегистрированный товарный знак, правообладателем которого является ООО "Мэйл.Ру".

Microsoft, Windows, Windows Mail, Internet Explorer, Outlook, PowerShell, Bing, 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.

Список сервисов, в которые передается пароль при сканировании QR-кода

При сканировании QR-кода на Android одноразовый пароль для активации приложения на вашем смартфоне будет передан в Google Play и AppsFlyer.

Окно Расширение защиты

Развернуть всё | Свернуть всё

Пробная версия

По ссылке запускается переход на пробную подписку.

Купить код активации

Кнопка, при нажатии на которую открывается окно браузера на странице интернет-магазина, в котором вы можете приобрести подписку.

Ввести код активации

По ссылке запускается мастер активации приложения.

Окно Расширение защиты

Развернуть всё | Свернуть всё

Купить код активации

По ссылке открывается окно браузера на странице интернет-магазина, в котором вы можете приобрести подписку приложения, на которое осуществляется переход.

Ввести код активации

По ссылке запускается мастер активации приложения.

Пробная версия

При нажатии на кнопку запускается переход на пробную версию другого приложения.

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 приложение было активировано ранее, на другом компьютере.

По ссылке **Отмена** вы можете отменить активацию приложения.

Отмена

По ссылке вы можете отменить применение резервного кода активации и вернуться к окну **Лицензирование**.

Окно Ввод кода активации

Развернуть всё | Свернуть всё

Поля для ввода кода активации

Вы могли получить код активации по электронной почте или в оффлайн-магазине. Код активации состоит из четырех групп символов (например, **ABA9C-CDEFG-ABCBC-ABC2D**).

Восстановить подписку из аккаунта My Kaspersky

По ссылке открывается окно с формой подключения устройства к аккаунту My Kaspersky для активации подписки, которая хранится в аккаунте.

Где найти код активации

По ссылке **Где найти код активации?** открывается окно браузера с подробной информацией об активации приложения с помощью кода активации.

Купить подписку

По ссылке открывается окно браузера на странице интернет-магазина, в котором вы можете приобрести подписку.

Активировать

По кнопке запускается активация приложения с помощью введенного кода активации.

Код активации соответствует другому приложению

Развернуть всё | Свернуть всё

Это окно отображается, если введенный код активации соответствует другому приложению. Вы можете перейти к использованию этого приложения сейчас или после истечения срока действия подписки на приложение Kaspersky.

Отмена

По ссылке вы можете отменить активацию приложения.

Продолжить

При нажатии на кнопку запускается установка и активация приложения, которому соответствует введенный вами код активации.

Информация о категориях сайтов

Развернуть всё | Свернуть всё

По ссылке вы можете ознакомиться с описанием категорий веб-сайтов .

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.

Приложение Kaspersky автоматически получает данные о том, какой DoH-сервер используется в браузере Mozilla Firefox. Если вы добавили DoH-сервер в приложении Kaspersky вручную и хотите, чтобы данные DNS передавались через этот DoH-сервер, вам нужно добавить этот сервер в настройках браузера Mozilla Firefox. Информацию о настройке DoH-сервера смотрите в справке Mozilla Firefox.

Добавление DoH-сервера

Чтобы добавить DoH-сервер:

1. Откройте главное окно приложения.

2. Нажмите на кнопку  в нижней части главного окна.

   Откроется окно **Настройка**.

3. В разделе **Дополнительно** выберите подраздел **Сеть**.

   Откроется окно **Настройки сети**.

4. В блоке **Обработка трафика** по ссылке **Управлять DoH-серверами** 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 <приложение>

При выборе этого варианта работа мастера активации завершается. Приложение будет работать по обнаруженной действующей подписке. Если обнаружена подписка на Kaspersky Standard или Kaspersky Plus, будет запущен мастер миграции.

Нет, продолжить работу мастера и ввести новый код активации

При выборе этого варианта мастер активации продолжает работу и активирует приложение. Вам потребуется ввести новый код активации, соответствующий этому приложению.

Окно Регистрация

В этом окне нужно указать регистрационные данные, которые понадобятся в случае обращения в Службу технической поддержки.

Отсутствует соединение с интернетом

Развернуть всё | Свернуть всё

Это окно отображается, если попытка активировать приложение не удалась из-за проблем с подключением к интернету.

Повторить попытку

По ссылке мастер активации пытается активировать приложение повторно. Если проблемы с интернетом краткосрочные, то повторная попытка может оказаться успешной.

Раздел Выбор папки для восстановленных файлов

Развернуть всё | Свернуть всё

В исходную папку

При выборе этого варианта приложение помещает восстановленные файлы в папку, в которой находились исходные файлы в момент создания резервной копии.

В указанную папку

При выборе этого варианта приложение 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 должно выполнять приложение, если в папке, куда требуется поместить восстановленный файл, уже находится файл с таким же именем:

- **спрашивать** – приложение при совпадении имен файлов предлагает выбрать один из вариантов: заменить файл резервной копией, сохранить оба файла или не восстанавливать этот файл.
- **заменить файл резервной копией** – Приложение Kaspersky удаляет существующий файл и помещает на его место файл, восстановленный из резервной копии.
- **сохранить оба файла** – Приложение Kaspersky оставляет существующий файл без изменений и сохраняет файл, восстановленный из резервной копии, под новым именем в этой же папке.
- **не восстанавливать этот файл** – Приложение Kaspersky 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 приложение. По ссылке **Причины и возможные решения** вы можете просмотреть информацию о проблеме в базе знаний.

Причины и возможные решения

По ссылке вы можете перейти к статье базы знаний с информацией о причинах ошибки и возможных решениях.

Для некоторых ошибок ссылка на статью в базе знаний может отсутствовать.

Отмена

По ссылке вы можете отменить активацию приложения.

Переход к использованию другого приложения

Развернуть всё | Свернуть всё

После нажатия на кнопку **Далее** будет запущен мастер миграции. В результате работы мастера миграции будет установлено приложение, соответствующая введенному коду активации (Kaspersky Standard или Kaspersky Plus).

Если срок действия подписки на Kaspersky еще не истек, вы можете применить код активации Kaspersky на другом компьютере.

По ссылке **Отмена** вы можете отменить переход на Kaspersky Standard или Kaspersky Plus.

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 приложения по подписке. Оплата за использование приложения по подписке взимается с момента оформления подписки. Если вы оформили подписку на приложение Kaspersky, откажитесь от использования приложения по действующей лицензии и активируйте приложение с помощью кода активации для подписки.

Вы можете применить код активации, с помощью которого приложение было активировано ранее, на другом компьютере до истечения срока действия лицензии.

Окно Последовательность запуска

Развернуть всё | Свернуть всё

Последовательность запуска приложений

В списке содержится информация о приложениях, запущенных выбранным приложением (дочерних приложениях). По умолчанию дочерние приложения отсортированы по времени запуска, начиная с самого раннего.

Запуск

В графе отображается время запуска дочернего приложения.

ID процесса

В графе отображается идентификатор процесса дочернего приложения.

Приложение

В графе отображается название дочернего приложения.

Группа доверия

В графе отображается группа доверия, в которую входит приложение:

- **Доверенные**. Приложение работает без ограничений, но контролируется компонентом Файловый Антивирус.
- **Слабые ограничения**. Приложению запрещено обращаться к конфиденциальным данным и настройкам пользователя, изменять публичные данные. При попытке изменения системных данных и выполнения привилегированных операций запрашивается разрешение пользователя. Сетевая активность такого приложения ограничена.
- **Сильные ограничения**. Приложению запрещено обращаться к конфиденциальным данным и настройкам пользователя, публичным и системным данным. При попытке выполнения привилегированных операций запрашивается разрешение пользователя. Сетевая активность такого приложения заблокирована.
- **Недоверенные**. Работа такого приложения полностью блокируется.

Закладка Работающие

Развернуть всё | Свернуть всё

Список работающих приложений

В списке отображаются приложения и процессы, выполняемые на вашем компьютере в настоящее время.

По правой клавише мыши можно открыть контекстное меню заголовка любой графы. С помощью контекстного меню можно настроить отображение граф с дополнительной информацией о приложениях и процессах:

- название исполняемого файла приложения или процесса;
- сведения о производителе приложениях;
- идентификатор процесса;
- расположение исполняемого файла приложения;
- имя пользователя, запустившего приложение или процесс;

- время создания и запуска приложения или процесса;
- настройки автозапуска приложения.

С помощью пункта **Упорядочить столбцы по умолчанию** можно восстановить исходный вид таблицы.

По правой клавише мыши на строке приложения или процесса открывается контекстное меню. Из контекстного меню можно выполнить следующие действия:

- открыть окно **Правила приложения**, в котором можно настроить правила для контроля действий приложения;
- отобразить последовательность запуска процессов в окне **Последовательность запуска**;
- переместить приложение в другую группу доверия;
- установить для приложения настройки контроля активности, предусмотренные по умолчанию;
- завершить процесс;
- открыть папку, в которой расположен исполняемый файл приложения.

Вид

В раскрывающемся списке можно включить отображение системных процессов и процессов Kaspersky:

- **Показывать системные процессы**. При выборе этого элемента в общем списке приложений и процессов отображаются процессы, необходимые для работы операционной системы.
- **Показывать процессы Kaspersky**. При выборе этого элемента в общем списке приложений и процессов отображаются процессы, запущенные Kaspersky.

В раскрывающемся списке также можно выбрать способ отображения приложений и процессов:

- **Показывать как список**. При выборе этого варианта приложения / процессы отображаются в виде списка.
- **Показывать как дерево**. При выборе этого варианта приложения / процессы отображаются в виде иерархической структуры в соответствии с последовательностью вызова процессов.

Приложение

В графе отображается название приложения или процесса.

Цифровая подпись

В графе отображается информация о наличии цифровой подписи у приложения и владельце цифровой подписи.

Группа доверия

В графе отображается группа доверия, в которую помещено приложение. В зависимости от группы доверия приложения в графе отображаются следующие значки:

- Красный значок означает, что приложение находится в группе "Недоверенные".
- Розовый значок означает, что приложение находится в группе "Сильные ограничения".
- Желтый значок означает, что приложение находится в группе "Слабые ограничения".
- Зеленый значок означает, что приложение находится в группе "Доверенные".
- Некоторые специализированные системные процессы (например, System или MemCompression) не распределяются по группам доверия и не контролируются приложением Kaspersky. Такие процессы отображаются в виде серого значка с отметкой "Неизвестные".

Популярность

В графе отображается уровень популярности приложения среди участников Kaspersky Security Network (KSN). Уровень популярности соответствует числу участников KSN, использующих приложение.

Процессор

В графе отображается текущее потребление ресурсов центрального процессора приложением / процессом.

Память

В графе отображается текущее потребление оперативной памяти приложением / процессом.

Диск

В графе отображается суммарная скорость чтения и записи данных на диск приложением или процессом.

Сеть

В графе отображается суммарная скорость приема и передачи данных приложением через сетевой интерфейс.

Завершить процесс

При нажатии на кнопку завершается работа приложения, выбранного в списке.

Закладка Запускаемые при старте

Развернуть всё | Свернуть всё

Список приложений, запускаемых при старте

Список содержит приложения, которые запускаются при старте операционной системы.

По правой клавише мыши можно открыть контекстное меню заголовка любой графы. С помощью контекстного меню можно настроить отображение граф в таблице. С помощью пункта **Упорядочить столбцы по умолчанию** можно восстановить исходный вид таблицы.

По правой клавише мыши на строке приложения или процесса открывается контекстное меню. Из контекстного меню можно выполнить следующие действия:

- открыть окно **Правила приложения**, в котором можно настроить правила для контроля действий приложения;
- переместить приложение в другую группу доверия;
- установить для приложения настройки контроля активности, предусмотренные по умолчанию;
- открыть папку, в которой расположен исполняемый файл приложения.

Приложение

В графе отображается название приложения, запускаемого при старте операционной системы.

Статус

В графе отображается состояние приложения: *Выполняется* или *Остановлено*.

Цифровая подпись

В графе отображается информация о наличии цифровой подписи у приложения и владельце цифровой подписи.

Группа доверия

В графе отображается группа доверия, в которую помещено приложение. В зависимости от группы доверия приложения в графе отображаются следующие значки:

- Красный значок означает, что приложение находится в группе "Недоверенные".
- Розовый значок означает, что приложение находится в группе "Сильные ограничения".
- Желтый значок означает, что приложение находится в группе "Слабые ограничения".
- Зеленый значок означает, что приложение находится в группе "Доверенные".
- Некоторые специализированные системные процессы (например, System или MemCompression) не распределяются по группам доверия и не контролируются приложением Kaspersky. Такие процессы отображаются в виде серого значка с отметкой "Неизвестные".

Популярность

В графе отображается уровень популярности приложения среди участников Kaspersky Security Network (KSN). Уровень популярности соответствует числу участников KSN, использующих приложение.

Последний запуск

В графе отображается время последнего запуска приложения.

Закладка Все приложения

Развернуть всё | Свернуть всё

Список приложений

В списке содержатся приложения, установленные на вашем компьютере. Для каждого приложения в списке отображается информация о статусе, цифровой подписи, группе доверия, популярности приложения среди пользователей KSN и времени последнего запуска.

По двойному щелчку мышью на строке приложения или процесса открывается окно **Правила приложения**. В окне можно настроить правила для контроля действий приложения.

По правой клавише мыши на строке приложения открывается контекстное меню. В контекстном меню можно выполнить следующие действия:

- открыть окно **Правила приложения**, в котором можно настроить разрешения для действий приложения;
- разрешить или запретить запуск приложения;
- переместить приложение в другую группу доверия;
- установить для приложения настройки контроля активности, предусмотренные по умолчанию (сбросить настройки приложения);
- удалить приложение из списка;
- открыть папку, содержащую исполняемый файл приложения.

Приложения в списке объединены в группы и подгруппы. По правой клавише мыши на строке группы открывается контекстное меню. В контекстном меню можно выполнить следующие действия:

- открыть окно **Правила группы**, в котором можно настроить разрешения для действий приложения из этой группы, используемые по умолчанию;
- создать подгруппу внутри группы; по умолчанию к подгруппе применяются правила, указанные для группы, в которую она входит;

- добавить приложение в группу; по умолчанию к приложению применяются правила, указанные для группы, в которую она входит;
- установить для группы и всех входящих в нее подгрупп и приложений настройки контроля активности, предусмотренные по умолчанию (сбросить настройки группы);
- установить для подгрупп и приложений, входящих в группу, настройки контроля активности, предусмотренные по умолчанию, оставив настройки группы без изменений (сбросить настройки подгрупп и приложений);
- удалить входящие в группу подгруппы и приложения.

Приложение

В графе отображается название приложения.

Статус

В графе отображается состояние приложения: *Выполняется* или *Остановлено*.

Цифровая подпись

В графе отображается информация о наличии цифровой подписи у приложения и владельце цифровой подписи.

Группа доверия

В графе отображается группа доверия, в которую помещено приложение. Группа доверия определяет правила использования приложения на компьютере: запрет или разрешение запуска, доступ приложения к файлам и системному реестру, ограничения сетевой активности приложения.

Популярность

В графе отображается уровень популярности приложения среди участников Kaspersky Security Network (KSN). Уровень популярности соответствует числу участников KSN, использующих приложение.

Последний запуск

В графе отображается время последнего запуска приложения.

Окно 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 приложению не удается отправить отзыв (например, отсутствует соединение с интернетом), приложение сохраняет отзыв на вашем компьютере. Отзывы хранятся в открытом виде в течение 30 дней.

Об использовании приложения ребенком

Если на вашем компьютере установлено и используется приложение Kaspersky Safe Kids, ребенок может выключить Kaspersky Safe Kids средствами приложения Kaspersky. Чтобы этого не произошло, рекомендуется установить пароль на изменение настроек Kaspersky.

Если вы вошли в операционную систему под учетной записью, которая привязана к профилю ребенка в приложении Kaspersky Safe Kids, приложение Kaspersky 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 **Настройка → Интерфейс**.

Разрешения

Пароль защищает от изменения пользователем или группой пользователей следующие настройки приложений. Если флажок установлен напротив какого-либо действия, это означает, что выбранное действие разрешено пользователю или группе пользователей.

Настройка приложения	Изменение настроек приложения в главном окне, окне **Настройка**, в Центре уведомлений и в самих уведомлениях. Включение и выключение трассировки приложения.
Управление резервным	Создание, изменение, удаление задач резервного копирования, а также задач восстановления данных из резервных копий.

копированием	
Управление защитой детей	Возможность запретить запуск приложения Kaspersky Safe Kids с помощью компонента Предотвращение вторжений, возможность завершить работу приложения Kaspersky или настроить приложение Kaspersky таким образом, чтобы защита не работала. При попытке загрузить, установить или запустить Kaspersky Safe Kids пароль не запрашивается.
Завершение работы приложения	Выход из приложения.
Удаление / изменение / восстановление приложения	Удаление, изменение или восстановление приложения.
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.

Окно Информация о подписке

В окне содержится информация о подписке на приложение:

- Статус подписки.
- Количество дней, оставшихся до окончания срока действия подписки.
- Количество устройств, 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:

1. Откройте главное окно приложения.
2. В главном окне приложения 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 должно выполнить приложение, когда вы заходите на этот сайт:
   - **Включать безопасное VPN-соединение**. Приложение включает безопасное VPN-соединение, когда вы посещаете указанный сайт. Например, вы можете указать, что приложение должно включать безопасное VPN-соединение, когда вы посещаете сайт вашего банка. Настройка действует, даже если в окне **Правила подключения к сайтам** в блоке **При посещении незащищенных банковских сайтов**: выбран вариант **Не реагировать**.

     a. В раскрывающемся списке **Выбирать сервер** выберите регион и город, 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 или города для включения безопасного VPN-соединения, подключение к сайту происходит через тот регион или город, 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**. Приложение не включает безопасное VPN-соединение, когда вы посещаете указанный сайт.

9. Нажмите на кнопку **Добавить**.

Приложение не включает безопасное VPN-соединение, если подключение к сайту выполняется по протоколу HTTPS.

Вернуться в справку Kaspersky Secure Connection.

Как настроить безопасное VPN-соединение для категорий сайтов

По умолчанию приложение Kaspersky Secure Connection не устанавливает безопасное VPN-соединение, когда вы открываете сайты в браузере. Вы можете настроить включение безопасного VPN-соединения для разных категорий сайтов, если на вашем компьютере установлено и активировано приложение Kaspersky Plus или Kaspersky Premium. Например, вы можете указать, что безопасное VPN-соединение должно включаться, когда вы посещаете сайты платежных систем или социальных сетей.

Чтобы настроить безопасное VPN-соединение для категорий сайтов:

1. Откройте главное окно приложения.
2. В главном окне приложения нажмите на кнопку ☰.
3. Выберите пункт **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**. Приложение будет включать безопасное VPN-соединение при посещении сайтов выбранной категории.

   - **Спрашивать**. При посещении какого-либо сайта из выбранной категории приложение будет спрашивать вас, нужно ли включать безопасное VPN-соединение для этого сайта. В окне браузера выберите нужное действие и установите флажок **Запомнить выбор для этого сайта**. Приложение будет выполнять выбранное вами действие каждый раз при посещении этого сайта. Если флажок не установлен, приложение запоминает ваш выбор на один час.

   - **Не реагировать**. Приложение не будет включать безопасное VPN-соединение при посещении сайтов выбранной категории.

7. Если выбран вариант **Включать безопасное VPN-соединение**, в раскрывающемся списке **Выбирать сервер** укажите регион и город, 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 .

Предотвращение вторжений

Развернуть всё | Свернуть всё

В блоке **Приложения** отображается информация о количестве приложений, которые контролирует приложение Kaspersky.

Управление приложениями

По ссылке открывается окно **Управление приложениями**. В этом окне можно указать группы доверия приложений, разрешить или запретить запуск приложений, а также перейти к настройке разрешений для отдельного приложения.

В блоке **Текущая активность** отображается информация о количестве приложений и процессов, запущенных в данный момент. В графическом виде представлена информация о загрузке центрального процессора, объеме оперативной памяти и дискового пространства, а также о сетевой активности.

Показать всю активность

По ссылке открывается окно **Активность приложений** на закладке **Работающие**. В этом окне можно просмотреть информацию о потреблении ресурсов компьютера каждым приложением, запущенным в текущий момент, а также перейти к настройке разрешений для отдельного приложения.

Предотвращение вторжений. Исключения

Развернуть всё | Свернуть всё

Исключения

Содержит ресурсы с персональными данными, исключаемые из области защиты Предотвращения вторжений. Ресурсом может быть файл, папка или ключ реестра.

Ресурс

Графа, в которой указывается название ресурса.

Путь

Графа, в которой указывается расположение ресурса. Путь может содержать маску.

Статус

В графе отображается раскрывающийся список со статусом ресурса:

- **Включить контроль**. Если выбран этот вариант, приложение контролирует действия с этим ресурсом.
- **Выключить контроль**. Если выбран этот вариант, приложение не контролирует действия с этим ресурсом.

Нажав левой клавишей мыши на значок статуса, в раскрывающемся списке вы можете включить или выключить контроль ресурса.

Добавить

При нажатии на кнопку открывается окно, в котором можно указать ресурс с персональными данными, добавляемыми в список.

Изменить

Кнопка, при нажатии на которую открывается окно **Изменение файла или папки** / **Изменение ключа реестра**. В окне можно изменить настройки выбранного ресурса.

Ресурсы, добавленные в список по умолчанию, не подлежат изменению.

Удалить

Кнопка, при нажатии на которую выбранный ресурс удаляется из списка.

Ресурсы, добавленные в список по умолчанию, не подлежат удалению.

Закладка Общие

Развернуть всё | Свернуть всё

Закладка Общие

Описание выбранной группы приложений.

Закладка Ресурсы

Развернуть всё | Свернуть всё

На этой закладке можно выбрать системные ресурсы или ресурсы пользователя и изменить права доступа приложений к этим ресурсам.

Кнопка 

С помощью кнопки-переключателя можно открывать или скрывать панель настройки правил.

Вид

В раскрывающемся списке можно выбрать два варианта фильтрации ресурсов:

- **Скрывать системные приложения**. Если выбран этот вариант, в списке ресурсов не отображаются ресурсы системных приложений.
- **Скрывать Kaspersky**. Если выбран этот вариант, в списке не отображаются ресурсы приложения Kaspersky.

Операционная система

Содержит настройки и ресурсы операционной системы выбранной категории. Ресурсом может быть файл или папка, ключ реестра, сетевой сервис или IP-адрес. Предотвращение вторжений контролирует доступ других приложений к ресурсам из списка.

По умолчанию в список **Операционная система** входят следующие объекты:

- ключи реестра, содержащие настройки автозапуска;
- ключи реестра, содержащие настройки работы в интернете;
- ключи реестра, влияющие на безопасность операционной системы;
- ключи реестра, содержащие настройки системных служб;
- системные файлы и папки;
- папки автозапуска.

Персональные данные

Содержит персональные данные пользователя, распределенные по ресурсам и категориям. Ресурсом может быть файл или папка. Предотвращение вторжений анализирует действия других приложений над ресурсами из списка.

По умолчанию в список персональных данных входят следующие объекты:

- файлы пользователя (папка "Мои документы", файлы cookies, данные об активности пользователя);
- файлы, папки и ключи реестра, содержащие настройки работы и важные данные наиболее часто используемых приложений: браузеров, файловых менеджеров, почтовых клиентов, IM-клиентов и электронных кошельков.

Ресурс

Графа, в которой содержится название ресурса операционной системы, защищаемого Предотвращением вторжений.

Путь

Графа, в которой указывается расположение ресурса. Путь может содержать маску.

Статус

В графе отображается раскрывающийся список со статусом ресурса:

- **Включить контроль**. Если выбран этот вариант, приложение контролирует действия с этим ресурсом.
- **Выключить контроль**. Если выбран этот вариант, приложение не контролирует действия с этим ресурсом.

Нажав левой клавишей мыши на значок статуса, в раскрывающемся списке вы можете включить или выключить контроль ресурса.

Добавить

В раскрывающемся списке можно добавить категорию ресурсов, файл или папку с ресурсами или ключ системного реестра.

Изменить

По ссылке открывается окно, в котором можно изменить название выбранного ресурса и путь к нему.

Удалить

По ссылке можно удалить из списка выбранную категорию ресурсов, файл или папку с ресурсами или ключ системного реестра. Предотвращение вторжений не будет контролировать доступ других приложений к этому ресурсу.

Восстановить

В раскрывающемся списке можно выбрать варианты действия:

- **настройки категории**. Если выбран этот вариант, настройки выбранной категории получат значения по умолчанию.

- **настройки подгрупп и ресурсов**. Если выбран этот вариант, настройки входящих в категорию подгрупп и ресурсов получат значения по умолчанию.

Список приложений

В списке отображаются группы доверия и приложения, входящие в эти группы доверия. В графах **Чтение**, **Запись**, **Создание**, **Удаление** указаны права доступа приложения или группы приложений к выбранному ресурсу.

В таблице ниже приведено описание действий Kaspersky, если приложение или группа приложений пытается получить доступ к ресурсу.

Описание действий Kaspersky

Действие	Описание
Наследовать	Приложение или группа приложений наследует реакцию из вышестоящей группы.
Разрешить	Приложение Kaspersky разрешает приложением, входящим в выбранную группу, доступ к ресурсу.
Запретить	Приложение Kaspersky запрещает приложениям, входящим в выбранную группу, доступ к ресурсу.
Спрашивать пользователя	Если в разделе **Настройки** → **Настройки производительности** → **Потребление ресурсов компьютера** установлен флажок **Автоматически выполнять рекомендуемые действия**, приложение Kaspersky автоматически выбирает действие с этим ресурсом по правилам, созданным специалистами "Лаборатории Касперского". По сноске вы можете прочитать, какое именно действие будет выбрано. Если флажок снят, приложение Kaspersky спрашивает пользователя, разрешать этому приложению доступ к ресурсу или нет.
Записывать в отчет	Помимо заданной реакции приложение Kaspersky записывает в отчет информацию о попытке доступа приложения к ресурсу.

Окно Лицензионное соглашение

Развернуть всё | Свернуть всё

Окно содержит текст Лицензионного соглашения. Для просмотра Лицензионного соглашения вы можете воспользоваться полосой прокрутки.

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 приложения 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 приложения.

Кнопка отображается, если возникшие проблемы с лицензией можно решить обновлением баз (например, дата выпуска баз не соответствует сроку действия лицензии).

Причины и возможные решения

Кнопка, при нажатии на которую открывается окно браузера на сайте Службы технической поддержки с информацией о возникшей проблеме.

Кнопка отображается, если возникли проблемы с действующей подпиской.

Обновить статус

Кнопка, при нажатии на которую с сервера поставщика услуг скачивается актуальная информация о статусе подписки.

Кнопка отображается, если приложение используется по подписке.

Найдены другие несовместимые приложения

Развернуть всё | Свернуть всё

Список несовместимых приложений

В списке перечислены приложения, несовместимые с устанавливаемым приложением. Для корректной работы устанавливаемого приложения нужно удалить несовместимые с ним приложения.

Удалить вручную

Кнопка, при нажатии на которую открывается окно со списком приложений, установленных на компьютере. В этом списке можно выбрать приложения, несовместимые с устанавливаемым приложением, чтобы удалить их с компьютера.

Продолжить

Кнопка, при нажатии на которую несовместимые приложения, представленные в списке, остаются на компьютере, а мастер продолжает работу.

Одновременное использование приложений, несовместимых с устанавливаемым приложением, может привести к некорректной работе устанавливаемого приложения и существенному ослаблению защиты вашего компьютера.

Найдены несовместимые приложения

Развернуть всё | Свернуть всё

Список несовместимых приложений

В списке перечислены приложения, несовместимые с устанавливаемым приложением. Для корректной работы устанавливаемого приложения нужно удалить несовместимые с ним приложения.

Удалить

Кнопка, при нажатии на которую несовместимые приложения, представленные в списке, удаляются с компьютера, а мастер продолжает работу.

Оставить

Кнопка, при нажатии на которую несовместимые приложения, представленные в списке, остаются на компьютере, а мастер продолжает работу.

Одновременное использование приложений, несовместимых с устанавливаемым приложением, может привести к некорректной работе устанавливаемого приложения и существенному ослаблению защиты вашего компьютера.

Необходимо перезагрузить компьютер

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.

Приложение Kaspersky 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 приложение Kaspersky 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 (приложения, службы, сервера), который использует порт;
- идентификатор процесса;
- локальный IP-адрес процесса;
- протокол, по которому выполняется соединение через порт.

По двойному щелчку на строке списка открывается окно **Правила приложения** на закладке **Сетевые правила**. В этом окне вы можете настроить сетевые правила для приложения, которое использует выбранный порт.

По правой клавише мыши на элементе списка открывается контекстное меню, из которого можно перейти к настройке сетевых правил.

Меню содержит следующие пункты:

- **Сетевые правила приложения**. При выборе этого пункта меню открывается окно **Правила приложения** на закладке **Сетевые правила**. В окне вы можете настроить сетевое правило для приложения, которое использует порт, выбранный в списке.

- **Все сетевые правила**. При выборе этого пункта меню открывается окно **Пакетные правила**. В окне вы можете настроить пакетные правила для приложения, которое использует порт, выбранный в списке.

Раздел Сетевая активность

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** – в списке отображается информация о соединениях, установленных приложением Kaspersky.

Сетевая активность

Содержит активные сетевые соединения, установленные на вашем компьютере в данный момент.

Для каждого соединения указана следующая информация:

- название процесса (приложения, службы, сервера), который инициировал соединение;
- направление соединения (входящее / исходящее);
- протокол, по которому выполняется соединение;
- настройки соединения (удаленный порт и IP-адрес);
- объем переданной / принятой информации в килобайтах.

По правой клавише мыши на элементе списка открывается контекстное меню, из которого можно перейти к настройке сетевых правил.

Меню содержит следующие пункты:

- **Сетевые правила приложений**. При выборе этого пункта меню открывается окно **Правила приложения** на закладке **Сетевые правила**. В этом окне вы можете настроить сетевое правило для приложения, выбранного в списке.
- **Все сетевые правила**. При выборе этого пункта меню открывается окно **Пакетные правила**. В этом окне вы можете настроить пакетные правила для приложения,

выбранного в списке.

Блокировать любую сетевую активность

По ссылке Сетевой экран запрещает сетевую активность всем процессам.

В нижней части окна отображается график объема входящего и исходящего трафика для процесса, выбранного в списке. График показывает объем трафика в режиме реального времени. Объем трафика указывается в килобайтах.

Особенности добавления правила для сетевого адаптера

Когда вы создаете разрешающее правило для сетевого адаптера и / или правило с указанием TTL, это правило может конфликтовать с запрещающим правилом для приложений. Например, если приложение находится в группе "Сильные ограничения", ей будет запрещен сетевой доступ, даже если вы создали разрешающее пакетное правило для сетевого адаптера (а также для TTL).

Чтобы разрешающее правило работало для всех приложений, которые будут пытаться подключаться к сети через этот сетевой адаптер, необходимо создать следующие правила в порядке приоритета от наиболее приоритетного к наименее приоритетному (в общем списке пакетных правил приоритет считается сверху вниз от самого приоритетного к наименее приоритетному).

1. Разрешающее правило для выбранного сетевого адаптера.
2. Запрещающие правила для всех остальных сетевых адаптеров.
3. Разрешающее правило без указания сетевого адаптера.

Чтобы работало разрешающее правило для сетевого адаптера с использованием TTL, необходимо создать следующие правила в порядке приоритета от наиболее приоритетного к наименее приоритетному:

1. Разрешающее правило для конкретного значения TTL.
2. Запрещающее правило для TTL со значением равным 255.
3. Разрешающее правило без указания конкретного значения TTL.

Раздел Сетевой трафик

Период

Список содержит интервалы времени для просмотра распределения сетевого трафика.

Возможные значения:

- **За день**. В списке отображается распределение сетевого трафика за текущие сутки.
- **За вчера**. В списке отображается распределение сетевого трафика за вчерашние сутки.
- **За месяц**. В списке отображается распределение сетевого трафика за текущий месяц.
- **За год**. В списке отображается распределение сетевого трафика за текущий год.

Сетевой трафик

Содержит информацию обо всех входящих и исходящих соединениях между вашим компьютером и другими компьютерами.

Для каждого приложения (компьютера, службы, сервера, процесса) указан объем входящего и исходящего трафика.

По двойному щелчку на приложении в списке открывается окно **Правила приложения** на закладке **Сетевые правила**. В этом окне вы можете настроить сетевые правила для выбранного приложения.

По правой клавише мыши на элементе списка открывается контекстное меню, из которого можно перейти к настройке сетевых правил.

Меню содержит следующие пункты:

- **Сетевые правила приложений**. При выборе этого пункта открывается окно **Правила приложения** на закладке **Сетевые правила**, на которой вы можете настроить сетевое правило для выбранного приложения.
- **Все сетевые правила**. При выборе этого пункта открывается окно **Пакетные правила**, в котором вы можете настроить пакетные правила для выбранного приложения.

В нижней части окна отображается диаграмма распределения трафика выбранного приложения по времени за выбранный период.

Разрыв сетевых соединений

Если в момент завершения работы на компьютере или приостановки защиты были установлены сетевые соединения, контролируемые приложением, на экран будет выведено уведомление о разрыве этих соединений. Это необходимо для корректного завершения работы приложения. Разрыв происходит автоматически по истечении 10 секунд либо при нажатии на кнопку **Да**. Большинство прерванных соединений восстанавливается через некоторое время.

> Если во время разрыва соединения вы скачиваете файл без использования менеджера загрузки, передача данных будет прервана. Для получения файла вам потребуется повторно инициировать его загрузку.

Вы можете отменить разрыв соединений. Для этого в окне уведомления нажмите на кнопку **Нет**. При этом приложение продолжит свою работу.

О дополнительных возможностях безопасного VPN-соединения

Дополнительные возможности безопасного VPN-соединения доступны, если на вашем устройстве установлено приложение Kaspersky Plus или Kaspersky Premium.

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 и города. Если вы указали в настройках безопасного VPN-соединения разные регионы или города при подключении к сайтам разных категорий, вы можете указать, надо ли менять регион или город, 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

Развернуть всё | Свернуть всё

Устранить

При нажатии на кнопку приложение Kaspersky 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

Уведомления приложения, появляющиеся в области уведомлений панели задач, информируют о событиях, происходящих в процессе работы приложения и требующих вашего внимания.

При появлении на экране уведомления следует выбрать один из предложенных в уведомлении вариантов действия. Оптимальный вариант – тот, который рекомендован специалистами "Лаборатории Касперского" по умолчанию.

Об облачной защите

В этом окне вы можете ознакомиться с информацией о Kaspersky Security Network.

Окно Активация

Развернуть всё | Свернуть всё

В этом окне отображается процесс активации приложения.

Отмена

При нажатии на кнопку можно отменить активацию приложения.

Регистрация и авторизация

Развернуть всё | Свернуть всё

Адрес электронной почты

Поле для ввода адреса электронной почты для подключения к существующему аккаунту My Kaspersky или создания нового аккаунта.

Войти с помощью Google

При нажатии на кнопку выполняется переход к форме входа в аккаунт Google в браузере по умолчанию (доступно не во всех регионах).

Войти с помощью Facebook

При нажатии на кнопку выполняется переход к форме входа в аккаунт Facebook в браузере по умолчанию (доступно не во всех регионах).

Войти с помощью Apple

При нажатии на кнопку выполняется переход к форме входа в аккаунт Apple в браузере по умолчанию.

У меня есть код активации

При нажатии на ссылку открывается форма ввода кода активации.

Продолжить

При нажатии на кнопку выполняется переход в форму ввода пароля от существующего аккаунта My Kaspersky или начинается процесс создания нового аккаунта.

При входе в существующий аккаунт My Kaspersky в окне отображается следующее:

Пароль

Поле для ввода пароля от аккаунта My Kaspersky.

Забыли пароль?

Переход к окну восстановления пароля от аккаунта My Kaspersky, если вы его забыли.

Ввести другой email

При нажатии на кнопку происходит возврат в форму ввода адреса электронной почты.

Войти

При нажатии на кнопку происходит подключение устройства к аккаунту My Kaspersky.

В процессе создания аккаунта My Kaspersky в окне отображается следующее:

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.

Регион

По ссылке открывается окно выбора региона. От выбранного региона зависит, какие приложения и какие способы оплаты вы сможете использовать.

Ввести другой email

При нажатии на кнопку происходит возврат в форму ввода адреса электронной почты.

Создать

При нажатии на кнопку выполняется регистрация аккаунта My Kaspersky. На указанный вами адрес электронной почты придет письмо, содержащее ссылку для создания пароля от аккаунта My Kaspersky.

Подробнее об аккаунте My Kaspersky

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 секретной папки

Развернуть всё | Свернуть всё

В этом окне можно выбрать место хранения создаваемой секретной папки.

Выбрать

При нажатии на кнопку можно подтвердить, что указанный путь верный.

Окно Выбор файла или папки

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 приложений

Развернуть всё | Свернуть всё

В этом окне отображаются приложения, которые не удалось распределить по другим группам. Вы можете выбрать группу доверия из списка и нажать на кнопку **Сохранить**. Приложения, которые не удалось распределить по другим группам, будут попадать в указанную вами группу доверия.

По умолчанию такие приложения помещаются в группу **Слабые ограничения**.

Окно Группа доверия для приложений, запущенных до начала работы Kaspersky

Развернуть всё | Свернуть всё

В этом окне можно выбрать группу доверия для неизвестных приложений, запущенных до начала работы приложения Kaspersky.

Список групп доверия

В списке можно указать группу доверия, в которую нужно помещать приложения, запущенные до начала работы приложения Kaspersky. Сетевая активность таких приложений будет ограничиваться в соответствии с правилами выбранной группы доверия. По умолчанию сетевая активность приложений, запущенных до начала работы приложения Kaspersky, ограничивается в соответствии с правилами, заданными специалистами "Лаборатории Касперского".

Выбрать группу доверия автоматически

Если выбран этот вариант, компонент Предотвращение вторжений помещает приложения, запущенные до начала работы приложения Kaspersky, в одну из групп доверия на основании правил, заданных специалистами "Лаборатории Касперского".

Выбрать группу доверия вручную

Если выбран этот вариант, вы можете самостоятельно выбрать группу доверия, в которую необходимо помещать приложения, запущенные до начала работы приложения Kaspersky.

Окно Добавление / изменение исключения Защиты от сбора данных в интернете

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 приложений должен анализировать и контролировать компонент Предотвращение вторжений.

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 компонент Предотвращение вторжений.

Название

В поле можно указать название ресурса с ключом реестра.

Путь к ключу

В поле можно указать путь к ключу реестра.

Защитить значение ключа

Если флажок установлен, от изменения защищается только значение ключа, указанное в поле **Значение ключа**.

Если флажок снят, то защищаются все значения этого ключа реестра.

Если в поле **Значение ключа** не указано никакого значения, то защищается значение ключа реестра по умолчанию.

Флажок автоматически устанавливается при выборе ключа реестра.

Значение ключа

В поле можно указать значение ключа реестра, которое компонент Предотвращение вторжений должен защищать от изменения.

Поле доступно, если установлен флажок **Защитить значение ключа**.

Добавить

При нажатии на кнопку ключ реестра добавляется в список ресурсов.

Окно Добавление / Изменение 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

Развернуть всё | Свернуть всё

Название

В поле можно указать название ресурса с файлом или папкой, доступ к которым должно контролировать Предотвращение вторжений.

Путь

В поле вы можете вручную указать путь к файлу или папке.

При вводе пути вручную вы можете использовать маску.

Маска `\*` позволяет указать, что нужно контролировать доступ ко всем файлам в выбранной папке.

Маска `\*<расширение>` позволяет указать, что нужно контролировать доступ ко всем файлам с определенным расширением в выбранной папке.

Также вы можете контролировать доступ приложений к файловым ресурсам, расположенным на удаленном компьютере. Для этого укажите путь к сетевому ресурсу в UNC-формате согласно правилу `\\Server\Share\Относительный путь`, в котором:

- Server – доменное имя компьютера или IP-адрес в формате IPv4 или IPv6 (обязательно для ввода).
- Share – сетевое имя общей папки (обязательно для ввода).
- Относительный путь – путь к папке или файлу из общей папки (необязательно для ввода).

  Примеры путей:

- `\\Server1\ShareFolder1\test\example.exe`
- `\\Server1\ShareFolder1\test\*.docx`
- `\\Server1\ShareFolder1\*`

  Приложение не контролирует доступ к файловому ресурсу, если заданный в правиле путь отличается от пути, по которому выполняется обращение.

Выбрать

При нажатии на кнопку открывается окно, где вы можете выбрать файл или папку.

Добавить

При нажатии на кнопку папка или файл добавляется в список ресурсов.

Окно завершения активации

Развернуть всё | Свернуть всё

Это окно открывается, если приложение активировано успешно.

Готово

При нажатии на кнопку завершается процедура активации приложения. Выполняется переход в окно лицензирования.

Окно Запрещенные и разрешенные приложения

Развернуть всё | Свернуть всё

В этом окне отображается список приложений, которым разрешено или запрещено изменять настройки операционной системы. Пустой список означает, что вы еще не разрешали и не запрещали приложениям изменять настройки операционной системы.

Список приложений

Список приложений содержит следующую информацию:

- **Приложение**. В графе отображается название приложения.
- **Имя файла**. В графе отображается название исполняемого файла приложения.
- **Путь**. В графе отображается путь к исполняемому файлу приложения на жестком диске вашего компьютера.
- **Издатель**. В графе отображается цифровая подпись издателя приложения.
- **Изменения**. В графе отображается, запрещено или разрешено приложению изменять настройки операционной системы, браузеров, а также настройки сети.

Окно Защита приватности

В этом окне вы можете включать и выключать следующие компоненты:

Защита веб-камеры

Поиск утечки данных

Защита от сбора данных в интернете

Обновление приложений. Исключения

Развернуть всё | Свернуть всё

Исключения

В список **Исключения** попадают пропущенные вами обновления установленных приложений. Вы можете пропустить как отдельное обновление, так и все обновления для приложения, установленного на компьютере.

Список **Исключения** состоит из следующих граф:

- **Приложение** – в графе отображается название приложения.
- **Пропускать** – графа может содержать следующие значения:
  - **Версия обновления** – отображается, если вы пропустили отдельное обновление для установленного приложения.
  - **Все обновления** – отображается, если вы решили не обновлять приложение.

Удалить из списка

При нажатии на кнопку выбранные приложения удаляются из списка исключений. Кнопка доступна, если приложение выбрано в списке.

Приложение Kaspersky будет сообщать о наличии обновлений для приложений, удаленных из списка.

Окно Исключения Защиты от сбора данных в интернете

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 в интернете обнаруживает попытки сбора данных, но не блокирует их, даже если в настройках компонента указано блокировать сбор данных этими категориями сервисов отслеживания.

Вы можете добавить в список веб-адрес или маску веб-адреса.

Изменить

Открывает окно, в котором можно изменить выбранный веб-адрес / маску веб-адреса.

Удалить

Удаляет из списка выбранный веб-адрес / маску веб-адреса.

Добавить

Открывает окно, в котором можно добавить веб-адрес / маску веб-адреса.

Окно Использование приложений

Развернуть всё | Свернуть всё

Приложение

В графе отображаются приложения и группы приложений, использование которых вы можете ограничить.

Использование

В графе указано, разрешено или запрещено пользователю работать с приложением или группой приложений:

- **Разрешено** – пользователь может работать с этим приложением или группой приложений.
- **Заблокировано** – пользователю запрещено работать с этим приложением или группой приложений.
- **Ограничено** – пользователь может работать с этим приложением или группой приложений ограниченное количество времени.

Вы можете разрешить, запретить или ограничить использование приложения или группы приложений для выбранного пользователя, выбрав нужный пункт раскрывающегося списка.

Путь

В графе отображается путь к исполняемому файлу приложения.

Правила

По кнопке открывается окно, где вы можете ограничить использование выбранного приложения по времени.

Удалить

Нажатие на кнопку удаляет выбранное приложение из списка. После удаления приложения из списка приложение Kaspersky перестает контролировать использование приложения, пользователь может работать с этим приложением без ограничений.

Добавить приложение

По кнопке открывается окно, в котором вы можете выбрать исполняемый файл приложения для добавления в список. Родительский контроль помещает приложение 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 приложение Kaspersky возвращает файл, выбранный в списке, в папку, в которой он находился до помещения на карантин.

Удалить

Кнопка, при нажатии на которую приложение Kaspersky удаляет файл, выбранный в списке.

Удалить все

При нажатии на кнопку приложение Kaspersky удаляет все резервные копии файлов, помещенные на карантин.

Приложение Kaspersky 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 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

Развернуть всё | Свернуть всё

В этом окне представлен список нецензурных слов. По наличию этих слов приложение Kaspersky 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**. Приложение проверяет наличие этого слова в сообщениях.
- **Неактивно**. Приложение 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 приложений

Развернуть всё | Свернуть всё

Включить / выключить Менеджер приложений

Включение Менеджера приложений. Если переключатель включен, приложение Kaspersky контролирует установку и удаление дополнительных приложений, а также показ шагов установки, содержащих рекламу.

Во время установки приложений автоматически снимать флажки установки дополнительных приложений. Предупреждать при попытке установить дополнительные приложения

Если флажок установлен, при установке приложений на ваш компьютер, приложение Kaspersky блокирует установку дополнительных приложений.

Если флажок снят после того, как вы уже запустили установку какого-либо приложения, Блокировщик скрытых установок продолжит свою работу в рамках текущей установки. Флажки напротив приложений, предлагаемых к дополнительной установке, будут сняты, а сами дополнительные приложения не будут устанавливаться. При последующей установке приложений эта функциональность работать не будет. Дополнительные приложения будут устанавливаться совместно с основным.

Не отображать шаги установки, которые могут содержать рекламу или предложения об установке дополнительных приложений

Если флажок установлен, при установке приложений на ваш компьютер приложение Kaspersky блокирует показ рекламы или предложений об установке дополнительных приложений.

Окно Настройки обновления приложений

Развернуть всё | Свернуть всё

Включить поиск обновлений для приложений

Если флажок установлен, приложение Kaspersky ищет обновления для установленных приложений и предлагает скачать и установить их.

Задать режим поиска обновлений

По ссылке открывается окно, в котором вы можете задать режим поиска обновлений для приложений, установленных на вашем компьютере.

Автоматически скачивать и устанавливать обновления, если не требуется принимать новое лицензионное соглашение

Если флажок установлен, приложение Kaspersky автоматически ищет обновления для установленных приложений, а также скачивает и устанавливает найденные обновления, если для этого от вас не требуется принять новое лицензионное соглашение.

Искать обновления для приложений

В настройке требуется выбрать, какие обновления приложений будут устанавливаться:

- **Важные обновления, которые повышают безопасность компьютера** – будет установлены только важные обновления, которые устраняют уязвимости и повышают безопасность вашего компьютера.
- **Все обновления для известных приложений** – будут установлены все обновления.

Исключения

По ссылке открывается окно **Исключения** со списком исключений. В список исключений попадают пропущенные вами обновления установленных приложений. Вы можете пропустить как отдельное обновление, так и все обновления для приложения, установленного на компьютере.

Режим поиска обновлений / Расписание

В таблице описаны настройки, применимые к расписанию работы следующих компонентов: Обновление приложений, Менеджер приложений.

Настройка	Описание
Режим поиска обновлений (Обновление приложений) **Выполнять анализ** (Менеджер приложений)	**Автоматически**. Приложение Kaspersky выполняет задачу один раз в сутки согласно внутренним настройкам. **По минутам** / **По часам** / **По дням** / **Еженедельно** / **Каждый месяц** / **В указанное время**. Приложение Kaspersky выполняет задачу по сформированному вами расписанию, которое можно уточнить до минут. При выборе одного из этих вариантов доступен список **Отложить запуск после старта приложений на N минут**. **После запуска приложения**. Приложение Kaspersky выполняет задачу после своего запуска, спустя столько минут, сколько указано в поле **Запускать через N минут**.

	После каждого обновления. Приложение Kaspersky выполняет задачу после загрузки и установки нового пакета обновлений.
Запускать поиск обновлений на следующий день, если компьютер был выключен (Обновление приложений) **Выполнять анализ объектов на следующий день, если компьютер был выключен** (Менеджер приложений)	Если запланированный по расписанию поиск обновлений для приложений или анализ объектов пропущен из-за того, что компьютер был выключен, приложение Kaspersky 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 приложений только в случае, когда компьютер заблокирован или включена экранная заставка (Обновление приложений) **Выполнять анализ объектов только в случае, когда компьютер заблокирован или включена экранная заставка** (Менеджер приложений)	Приложение Kaspersky запускает задачу тогда, когда вы закончили работу на компьютере. Таким образом, задача не будет занимать ресурсы компьютера во время работы. Флажок отображается, если выбран режим запуска **После каждого обновления**.

Настройки обновления

Настройка	Описание
Расписание обновления	По ссылке открывается окно **Расписание обновления баз**, в котором можно выбрать один из режимов запуска обновлений баз:

баз	**Автоматически**. Режим запуска задачи обновления, при котором приложение Kaspersky проверяет наличие пакета обновлений в источнике обновлений с определенной периодичностью. Частота проверки наличия пакета обновлений увеличивается во время вирусных эпидемий и сокращается при их отсутствии. Обнаружив свежий пакет обновлений, приложение Kaspersky 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 приложения**. Режим запуска задачи обновления, при котором приложение Kaspersky выполняет задачу обновления по сформированному вами расписанию. Если выбран этот режим запуска задачи обновления, вы также можете запускать задачу обновления приложения Kaspersky вручную.
Настроить источники обновлений	По ссылке открывается окно со списком источников обновлений. *Источник обновлений* – это HTTP- или FTP-сервер или папка общего доступа (локальная или сетевая), откуда приложение может загрузить обновления баз и модулей. По умолчанию список источников обновлений содержит серверы обновлений "Лаборатории Касперского". Вы можете добавлять в список другие источники обновлений. Если в списке выбрано несколько источников обновлений, приложение Kaspersky обращается к ним по очереди, пока не скачает пакет обновлений с первого доступного источника обновлений.
Запускать обновление баз с правами	По ссылке открывается окно, в котором вы можете выбрать, от имени какого пользователя запускать обновление баз. По умолчанию задача обновления приложения Kaspersky запускается от имени пользователя, с правами которого вы зарегистрированы в операционной системе. Однако обновление приложения Kaspersky может производиться из источника обновления, к которому у пользователя нет прав доступа (например, из папки общего доступа, содержащей пакет обновлений) или для которого не настроено использование аутентификации на прокси-сервере. Вы можете указать пользователя, обладающего этими правами, в параметрах приложения и запускать задачу обновления приложения Kaspersky от имени этого пользователя.

Окно Поиск уязвимостей в приложениях

Развернуть всё | Свернуть всё

Начать поиск

Кнопка, при нажатии на которую запускается поиск уязвимостей в приложениях.

Остановить

Кнопка, при нажатии на которую поиск уязвимостей в приложениях останавливается.

Кнопка отображается, если запущен поиск уязвимостей в приложениях.

<N> уязвимых приложений

По ссылке открывается окно **Уязвимые приложения** со списком уязвимых приложений, обнаруженных при проверке. Ссылка отображается, если был запущен поиск уязвимостей в приложениях.

Окно Приостановка защиты

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 приложения

Режим возобновления работы компонентов защиты, при котором защита включается после перезапуска приложения или перезагрузки операционной системы (при условии, что включен автоматический запуск приложения).

Приостановить

Режим возобновления работы компонентов защиты, при котором защита включится только тогда, когда вы сами решите возобновить ее.

Окно Проверка пароля

Развернуть всё | Свернуть всё

Пароль

Пароль, ограничивающий доступ к управлению приложением Kaspersky.

Запомнить пароль на эту сессию

Если флажок установлен, приложение Kaspersky запоминает введенный пароль и больше не запрашивает его во время текущего сеанса работы.

Окно Приложения, которым запрещен доступ к веб-камере

Развернуть всё | Свернуть всё

В окне отображаются приложения, которым вы запретили доступ к веб-камере.

Разрешить доступ к веб-камере

При нажатии на кнопку приложению, выбранному в списке, разрешается доступ к веб-камере.

Окно Рекомендуемая настройка

Развернуть всё | Свернуть всё

Включить защиту от рекламных предложений, чтобы устанавливать только нужные приложения и блокировать дополнительные установки

Если флажок установлен, приложение Kaspersky блокирует показ рекламы во время установки на компьютер какого-либо программного обеспечения. При этом блокируется также установка предлагаемых в рекламе дополнительных приложений.

Готово

При нажатии на кнопку вы переходите в главное окно приложения.

Окно Отчеты

Для удобства работы с отчетами вы можете использовать следующие возможности:

- фильтрация по дате;
- фильтрация по значению в любой из ячеек;
- поиск по тексту записи о событии;
- сортировка списка по каждой графе отчета;
- изменение порядка и набора граф, отображаемых в отчете.

В отчетах применяются следующие уровни важности событий:

Информационные сообщения. События справочного характера, как правило, не несущие важной информации.

Предупреждения. События, на которые нужно обратить внимание, поскольку они отражают важные ситуации в работе приложения Kaspersky.

Критические события. События критической важности, указывающие на проблемы в работе приложения Kaspersky 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 обновление баз с правами

Выбор учетной записи, с правами которой приложение Kaspersky будет запускать задачи обновления. Функция доступна для запуска задачи обновления приложения Kaspersky 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 приложением всех команд, а также информация о состоянии приложения.

По ссылке **<количество файлов>**, **<объем данных>** рядом с флажком открывается окно **Полученные для анализа данные**. В окне отображаются список файлов и суммарный объем информации, которая будет передана на сервер Службы технической поддержки.

Сохранить отчет 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 приложение Kaspersky включает в отчет, отсылаемый на сервер Службы технической поддержки. В состав списка входят файлы трассировок и дампов. В этих файлах сохранена история выполнения приложением всех команд, а также информация о состоянии приложения.

Если флажок в строке файла установлен, то файл будет загружен на сервер Службы технической поддержки. Перед загрузкой подготовленные файлы данных будут упакованы в архив.

Если флажок в строке файла снят, то файл не будет загружен на сервер Службы технической поддержки.

Файл

Графа, в которой указывается название файла, готового для отправки на сервер Службы технической поддержки.

Размер

Объем информации, который будет передан на сервер Службы технической поддержки, если указанный файл включен в состав отчета. Приложение помещает файл в отчет, если установлен флажок в строке этого файла.

Запуск скрипта

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 приложения

Развернуть всё | Свернуть всё

Уязвимые приложения

Содержит найденные в приложениях уязвимости.

Из-за особенностей работы службы обновлений уязвимости некоторых приложений могут быть обнаружены повторно.

Для каждой найденной уязвимости доступны следующие кнопки:

- **Подробнее**

Кнопка, при нажатии на которую открывается сайт Службы технической поддержки с описанием угрозы. На сайте вы можете скачать нужное обновление для вашей версии приложения и установить его.

- **Добавить в исключения**

Кнопка, при нажатии на которую приложение будет добавлено в доверенную зону.

Выберите zip-файл или папку

Применение альтернативных тем оформления доступно не во всех регионах.

При выборе темы оформления учитывайте следующие ограничения:

- Приложение Kaspersky не сможет использовать выбранную тему оформления в следующих случаях:
  - Если внутри архива файлы отличаются наименованием или имеют иное расположение в структуре папок, чем в стандартной теме.
  - Если внутри архива повреждены файлы, отвечающие за тексты на окнах приложения.
- Темы оформления предназначены для определенной версии приложения Kaspersky и не применимы к другим версиям и другим приложениям. При обновлении приложения до новой версии или установки поверх нее другого приложения тема оформления меняется на стандартную.

Если в результате выбора альтернативной темы оформления вы столкнулись с проблемами и не можете установить стандартную тему оформления предусмотренным для этого способом (например, не можете снять флажок **Использовать альтернативную тему оформления** в окне **Настройки интерфейса** из-за того, что шрифт сливается с фоном и нужные элементы управления неразличимы), рекомендуется переустановить приложение Kaspersky.

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 приложение Kaspersky защищать ввод данных с аппаратной клавиатуры для выбранного сайта или веб-страницы.

Защищать

Приложение Kaspersky защищает ввод данных с аппаратной клавиатуры для выбранного сайта или веб-страницы.

Не защищать

Приложение Kaspersky 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, должно ли приложение показывать значок Экранной клавиатуры на страницах, соответствующих заданной маске веб-адреса.

Показывать значок в окне браузера

Приложение Kaspersky отображает значок быстрого вызова Экранной клавиатуры в полях ввода.

Не показывать значок в окне браузера

Приложение Kaspersky 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

Флажок включает / выключает функцию ограничения срока хранения отчетов. Срок хранения может составлять один день, одну неделю, один или шесть месяцев или один год.

При достижении указанного значения приложение удаляет все записи в отчете старше, чем указанное количество дней, минус 10 %. Если вы указали значение в тридцать дней, при появлении в отчете события старше тридцати дней, из отчета удаляются все события, которые хранятся дольше 27 дней.

Если флажок снят, срок хранения отчетов не ограничен.

Ограничить размер файла отчетов до

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. Удаление происходит при достижении половины от указанного размера. При этом удаляется 10 % от фактического размера файла отчета. Если указанное значение составляет 1024 МБ, то удаление более старых записей в файле отчета начнется при достижении размера файла отчета 512 МБ, при этом размер файла отчета будет сокращен на 10 % от фактического размера за счет удаления наиболее старых записей.

Если флажок снят, то размер файла отчета не ограничен.

Очистить

При нажатии на кнопку Kaspersky удаляет данные из папки отчетов.

По умолчанию Kaspersky удаляет отчеты задач проверки, отчеты задачи обновления, отчеты обработки правил Сетевого экрана.

В блоке **Карантин** вы можете изменить настройки карантина.

Хранить объекты не более

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 приложения Kaspersky от изменения или удаления собственных файлов на диске, процессов в памяти, записей в системном реестре.

Если флажок установлен, также отключается возможность внешнего управления системной службой. Если отключено внешнее управление системной службой, приложение Kaspersky блокирует любую попытку удаленного управления сервисами приложений. При попытке удаленного управления появляется уведомление над значком Kaspersky в области уведомлений панели задач Microsoft Windows (если уведомления не отключены).

Разрешить управление настройками Kaspersky через приложения удаленного управления

Если флажок установлен, доверенные приложения удаленного администрирования (такие как TeamViewer, LogMeIn Pro и Remotely Anywhere) могут изменять настройки приложения Kaspersky.

Недоверенным приложениям удаленного администрирования изменение настроек приложения Kaspersky 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. Приложение Kaspersky использует подключение к интернету в работе некоторых компонентов защиты, а также для обновления баз и модулей приложения.

Автоматически определять настройки прокси-сервера

Приложение Kaspersky 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 использует настройки прокси-сервера, указанные в браузере Microsoft Edge на базе Chromium. Kaspersky не учитывает настройки прокси-серверов, указанные для других браузеров, установленных на компьютере пользователя.

Использовать указанные настройки прокси-сервера

Приложение Kaspersky использует прокси-сервер, отличный от заданного в настройках соединения браузера.

Адрес

Содержит IP-адрес или символьное имя (URL) прокси-сервера.

Поле доступно, если выбрана настройка **Использовать указанные настройки прокси-сервера** (например, IP-адрес 192.168.0.1).

Порт

Порт прокси-сервера.

Поле доступно, если выбрана настройка **Использовать указанные настройки прокси-сервера**.

Использовать аутентификацию на прокси-сервере

Аутентификация – это проверка регистрационных данных пользователя.

Флажок включает / выключает использование аутентификации на прокси-сервере.

Если флажок установлен, то приложение Kaspersky попытается выполнить NTLM-, а затем BASIC-аутентификацию.

Если флажок не установлен или настройки прокси-сервера не указаны, то приложение Kaspersky попытается выполнить NTLM-аутентификацию с использованием учетной записи, от имени которой запущена задача (например, задача обновления).

Если аутентификация на прокси-сервере необходима, а вы не указали имя пользователя и пароль, или указанные данные по каким-либо причинам не были приняты прокси-сервером, откроется окно запроса имени пользователя и пароля. Если аутентификация пройдет успешно, приложение Kaspersky будет использовать в дальнейшем указанные имя пользователя и пароль. В противном случае приложение Kaspersky повторно запросит настройки аутентификации.

Имя пользователя

Имя пользователя, которое используется при аутентификации на прокси-сервере.

Пароль

Пароль для введенного имени пользователя.

Не использовать прокси-сервер для локальных адресов

Если флажок установлен, приложение Kaspersky не использует прокси-сервер при обновлении баз и модулей приложения из локальной или сетевой папки.

Если флажок снят, приложение Kaspersky использует прокси-сервер при обновлении баз и модулей приложения из локальной или сетевой папки.

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 приложениям доступ к веб-камере

Если флажок установлен, то запрет на доступ к веб-камере распространяется на все установленные на вашем компьютере приложения.

Если флажок снят, то приложение Kaspersky контролирует доступ приложений к веб-камере на основе принадлежности приложения к группе доверия:

- **Доверенные** – доступ к веб-камере разрешен.
- **Слабые ограничения** – при попытке доступа к веб-камере приложение Kaspersky выводит на экран окно с запросом разрешения на доступ этого приложения к веб-камере.
- **Сильные ограничения** и **Недоверенные** – доступ к веб-камере запрещен.

Показывать уведомление, когда веб-камеру использует приложение, которому это разрешено

Если флажок установлен, приложение Kaspersky выводит на экран уведомление при доступе к веб-камере приложения, которому доступ разрешен. С помощью уведомления вы можете изменить настройки доступа приложения к веб-камере, а также отказаться от дальнейшего отображения уведомлений.

Если флажок снят, уведомление не выводится.

Флажок доступен, если снят флажок **Запретить всем приложениям доступ к веб-камере**.

Обнаружено подозрительное перенаправление

Развернуть всё | Свернуть всё

Удалить записи

Приложение Kaspersky удаляет все подозрительные записи из файла hosts.

Пропустить

Приложение Kaspersky не удаляет из файла hosts подозрительные записи, представленные в списке.

Список подозрительных записей

Список содержит адреса вредоносных или неизвестных веб-серверов, на которые производится перенаправление при обращении приложения к серверам "Лаборатории Касперского".

Рекомендуется удалять подозрительные записи из файла hosts.

Окно Ввод пароля

Развернуть всё | Свернуть всё

Текущий пароль

Текущий пароль, который используется для доступа к управлению приложением Kaspersky.

Запомнить пароль на эту сессию

Если флажок установлен, приложение Kaspersky 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 приложения Kaspersky 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 приложением Kaspersky.

Подтверждение пароля

Повторный ввод пароля, введенного в поле **Новый пароль**.

В блоке **Область действия пароля** вы можете указать, какие функции управления приложением нужно защитить паролем.

Настройка приложения

Флажок включает / выключает запрос пароля при попытке пользователя сохранить изменения настроек приложения.

Управление Резервным копированием

Флажок включает / выключает запрос пароля при попытке пользователя открыть окно **Резервное копирование**.

Завершение работы приложения

Флажок включает / выключает запрос пароля при попытке пользователя завершить работу приложения.

Удаление приложения

Флажок включает / выключает запрос пароля при попытке пользователя удалить приложение.

Настройки проверки

В таблице описаны настройки, применимые к следующим видам проверки: полная проверка, быстрая проверка, выборочная проверка, проверка из контекстного меню.

Настройка	Описание
Уровень безопасности	Для проверки приложение Kaspersky применяет разные наборы настроек. Наборы настроек, сохраненные в приложении, называются *уровнями безопасности*. • **Предельный**. Приложение Kaspersky проверяет файлы всех типов. Во время проверки составных файлов приложение дополнительно проверяет файлы почтовых форматов. • **Оптимальный**. Приложение Kaspersky проверяет только файлы определенных форматов на всех жестких, сменных и сетевых дисках компьютера, а также вложенные OLE-объекты. Приложение не проверяет архивы и установочные пакеты.

	• **Низкий**. Приложение Kaspersky проверяет только новые и измененные файлы с определенными расширениями на всех жестких, сменных и сетевых дисках компьютера. Приложение не проверяет составные файлы.

Действие при обнаружении угрозы	• **Спрашивать пользователя**. Если во время проверки приложение Kaspersky обнаруживает зараженный или возможно зараженный объект, оно сразу уведомляет вас об этом и запрашивает действие над обнаруженным объектом.
	
	Этот вариант доступен, если в разделе **Настройки → Настройки производительности → Потребление ресурсов компьютера** снят флажок **Автоматически выполнять рекомендуемые действия**.
	
	• **Выбирать действие автоматически**. При обнаружении зараженных или возможно зараженных объектов приложение Kaspersky выполняет действие, рекомендуемое специалистами "Лаборатории Касперского":
	
	  • Зараженный объект приложение Kaspersky сначала пытается вылечить и, если это не удается - удаляет.
	
	  • Возможно зараженный объект приложение Kaspersky удаляет, если установлен флажок **Удалять вредоносные утилиты, рекламные приложения, приложения автодозвона и подозрительные упаковщики**. Если флажок снят, приложение не удаляет возможно зараженный объект; уведомление об обнаружении такого объекта отображается в центре уведомлений (открывается по кнопке **Подробнее** в главном окне приложения).
	
	Этот вариант доступен, если в разделе **Настройки → Настройки производительности → Потребление ресурсов компьютера** установлен флажок **Автоматически выполнять рекомендуемые действия**.
	
	• **Лечить; удалять, если лечение невозможно** Если выбран этот вариант действия, то приложение автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то приложение их удаляет.
	
	• **Лечить; блокировать, если лечение невозможно**. Если выбран этот вариант действия, то приложение Kaspersky автоматически пытается вылечить все обнаруженные

зараженные файлы. Если лечение невозможно, то приложение добавляет информацию об обнаруженных зараженных файлах в список обнаруженных объектов.

- **Информировать**. Если выбран этот вариант действия, то при обнаружении зараженных файлов приложение Kaspersky добавляет информацию об этих файлах в список обнаруженных объектов.

Перед лечением или удалением зараженного файла приложение формирует его резервную копию на тот случай, если впоследствии понадобится восстановить файл или появится возможность его вылечить.

Изменить область проверки (нет в настройках проверки из контекстного меню)	По ссылке открывается окно со списком объектов, которые проверяет приложение Kaspersky. 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 приложение выполняет задачу проверки по сформированному вами расписанию. Если выбран этот режим запуска задачи проверки, вы также можете запускать задачу проверки вручную.
Запускать проверку с правами	По ссылке открывается окно, в котором вы можете выбрать, от имени какого пользователя запускать проверку. По умолчанию задача проверки запускается от имени пользователя, с правами которого вы зарегистрированы в операционной системе. Область защиты может включать сетевые диски или другие объекты, для доступа к которым нужны специальные права. Вы можете указать пользователя, обладающего этими правами, в параметрах приложения, и запускать задачу проверки от имени этого пользователя.
Типы файлов	

Файлы без расширения приложение Kaspersky считает исполняемыми. Приложение проверяет исполняемые файлы всегда, независимо от того, файлы какого типа вы выбрали для проверки.

Все файлы. Если выбран этот параметр, Kaspersky проверяет все файлы без исключения (любых форматов и расширений).

Файлы, проверяемые по формату. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы. Перед началом поиска вредоносного кода в файле выполняется анализ его внутреннего заголовка на предмет формата файла (например, TXT, DOC, EXE). В процессе проверки учитывается также расширение файла.

Файлы, проверяемые по расширению. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы. Формат файла определяется на основании его расширения.

Проверять только новые и измененные файлы	Проверка только новых файлов и тех файлов, которые изменились после предыдущей проверки. Это позволит сократить время выполнения проверки. Такой режим проверки распространяется как на простые, так и на составные файлы.
Пропускать файлы, если их проверка длится более N секунд	Ограничение длительности проверки одного объекта. По истечении заданного времени приложение прекращает проверку файла. Это позволит сократить время выполнения проверки.
Проверять архивы	Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату.
Проверять дистрибутивы	Флажок включает / выключает проверку дистрибутивов сторонних приложений.
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 приложение Kaspersky проверяет файлы почтовых форматов, а также почтовые базы данных.

	Приложение полностью проверяет только файлы почтовых форматов Microsoft Outlook, Windows Mail / Microsoft Outlook Express и формата EML, и только при наличии на компьютере почтового клиента Microsoft Outlook x86. Если флажок установлен, приложение Kaspersky разбирает файл почтового формата и анализирует на наличие вирусов каждый его компонент (тело письма, вложения). Если флажок снят, приложение Kaspersky проверяет файл почтового формата как единый объект.
Проверять архивы, защищенные паролем	Если флажок установлен, приложение проверяет архивы, защищенные паролем. Перед проверкой файлов, содержащихся в архиве, на экран выводится запрос пароля. Если флажок не установлен, приложение пропускает проверку защищенных паролем архивов.
Не распаковывать составные файлы большого размера **Максимальный размер файла**	Если флажок установлен, то приложение не проверяет составные файлы, размеры которых больше заданного значения. Если флажок снят, приложение проверяет составные файлы любого размера. Приложение проверяет файлы больших размеров, извлеченные из архивов, независимо от состояния флажка.
Эвристический анализ	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.
Технология iSwift	Технология, представляющая собой развитие технологии iChecker для компьютеров с файловой системой NTFS. Технология iSwift имеет ограничение: она привязана к конкретному местоположению файла в файловой системе и применима только к объектам, расположенным в файловой системе NTFS.

	При обновлении версии приложения Kaspersky, технология iSwift включается для всех типов проверки, даже если ранее она была выключена.
Технология iChecker	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз приложения Kaspersky, дату предыдущей проверки файла, а также изменение настроек проверки. Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной приложению структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

Настройки проверки внешних дисков

Настройка	Описание
Действие при подключении внешнего диска	• **Быстрая проверка**. Если выбран этот вариант, то после подключения внешнего устройства Kaspersky проверяет только файлы определенных форматов, наиболее подверженные заражению, находящиеся в корневой папке подключенного устройства. Также при быстрой проверке приложение не распаковывает и не проверяет архивы. • **Подробная проверка**. Если выбран этот вариант, то после подключения внешнего устройства Kaspersky проверяет все файлы, расположенные во всех папках внешнего устройства, а также распаковывает и проверяет архивы, кроме защищенных паролем.
Максимальный размер внешнего диска	Если флажок установлен, то Kaspersky проверяет внешние устройства, размер которых не превышает указанный максимальный размер. Если флажок снят, то Kaspersky проверяет внешние устройства любого размера.
Отображать ход проверки	Если флажок установлен, то Kaspersky отображает ход проверки внешних устройств в отдельном окне, а также в окне запуска проверки.
Запретить остановку	Если флажок установлен, то для задачи проверки внешних устройств недоступна кнопка **Остановить** в окне запуска проверки.

задачи проверки

Настройки фоновой проверки

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

Если компьютер работает от аккумулятора, приложение Kaspersky не выполняет фоновую проверку компьютера.

Настройки поиска уязвимостей в приложениях

Настройка	Описание
Изменить область проверки	По ссылке открывается окно **Область поиска уязвимостей** со списком объектов, которые проверяются при поиске уязвимостей в приложениях. Вы можете добавить в список объекты или удалить добавленные вами объекты. Чтобы исключить объект из проверки, не обязательно удалять объект из списка, достаточно снять флажок напротив названия объекта.
Расписание проверки	**Вручную**. Режим запуска, при котором вы запускаете поиск уязвимостей в приложениях вручную в удобное для вас время. **По расписанию**. Режим запуска задачи проверки, при котором приложение выполняет задачу проверки по сформированному вами расписанию. Если выбран этот режим запуска задачи проверки, вы также можете запускать задачу проверки вручную.

Настройки учетной записи

Развернуть всё | Свернуть всё

Запуск от имени

Выбор учетной записи, с правами которой приложение Kaspersky будет запускать задачи проверки. Функция доступна для запуска проверки 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 приложений. По умолчанию Анти-Баннер блокирует на сайтах баннеры из списка известных баннеров. Список входит в состав баз приложения Kaspersky.

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". Список обновляется автоматически при обновлении баз и модулей приложения.

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:

- **Предельный**. 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.

- **Оптимальный**. 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 оптимальный уровень безопасности

По ссылке приложение устанавливает уровень безопасности **Оптимальный**. 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, приложение 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, приложение отслеживает все обращения к веб-сайтам банков или платежных систем и выполняет действие, заданное по умолчанию или настроенное пользователем. По умолчанию в режиме Безопасных платежей приложение запрашивает подтверждение пользователя на запуск Защищенного браузера.

Если переключатель выключен, приложение разрешает обращение к веб-сайтам банков или платежных систем с использованием обычного браузера.

Узнать больше

По ссылке открывается окно браузера на странице с более подробной информацией о компоненте.

В блоке **При первом обращении к сайтам банков или платежных систем** вы можете выбрать действие, которое приложение выполняет при первом обращении к сайтам банков и платежных систем.

Запускать Защищенный браузер

Если приложение 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 приложение 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, приложение 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 приложение 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 Интернет-защиты

Настройка	Описание
Уровень безопасности	Для работы Интернет-защиты приложение применяет разные наборы настроек. Наборы настроек, сохраненные в приложении, называются *уровнями безопасности*. • **Предельный**. Уровень безопасности веб-трафика, при котором компонент Интернет-защита максимально проверяет веб-трафик, поступающий на компьютер по HTTP- и FTP-протоколам. Интернет-защита детально проверяет все объекты веб-трафика, используя полный набор баз приложения, а также выполняет максимально глубокий эвристический анализ. • **Оптимальный**. Уровень безопасности веб-трафика, обеспечивающий оптимальный баланс между производительностью приложения Kaspersky и безопасностью веб-трафика. Компонент Интернет-защита выполняет эвристический анализ на среднем уровне. Этот уровень безопасности веб-трафика рекомендован для использования специалистами "Лаборатории Касперского". • **Низкий**. Уровень безопасности веб-трафика, параметры которого обеспечивают максимальную скорость проверки веб-трафика. Компонент Интернет-защита выполняет эвристический анализ на поверхностном уровне.
Действие при обнаружении угрозы	• **Информировать.** Интернет-защита информирует вас об обнаружении зараженного или возможно зараженного объекта и запрашивает дальнейшее действие над ним.

Этот вариант доступен, если в разделе **Настройки** → **Настройки производительности** → **Потребление ресурсов компьютера** снят флажок **Автоматически выполнять рекомендуемые действия**.

- **Выполнять действие автоматически.** Интернет-защита выбирает действие автоматически на основе установленных настроек. Если веб-ресурс находится в списке исключений или не содержит зараженных или возможно зараженных объектов, то Интернет-защита разрешает доступ к нему. Если в результате проверки Интернет-защита обнаруживает, что веб-ресурс содержит зараженный или возможно зараженный объект, он блокирует доступ к веб-ресурсу.

  Этот вариант доступен, если в разделе **Настройки** → **Настройки производительности** → **Потребление ресурсов компьютера** установлен флажок **Автоматически выполнять рекомендуемые действия**.

- **Запрещать загрузку**. Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта компонент Интернет-защита блокирует доступ к объекту и показывает сообщение в браузере.

- **Информировать**. Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта, приложение 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 приложения и пополняется при обновлении баз приложения Kaspersky.
Проверять веб-адрес по базе веб-адресов, на которых находятся рекламные приложения	Например, приложение, которое в процессе вашей работы с интернетом перенаправляет поисковый запрос на рекламный сайт. Таким образом, вы попадаете не на тот интернет-ресурс, который наилучшим образом соответствует вашему запросу, а на рекламный сайт.
Проверять веб-адрес	Например, приложение удаленного администрирования,

по базе веб-адресов, на которых находятся легальные приложения, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или вашим данным	которое легально используют системные администраторы для диагностики и устранения неполадок. Злоумышленник может без вашего ведома установить такое приложение на ваш компьютер, получить к нему доступ и использовать в своих целях. Приложение Kaspersky разрешает скачивание таких приложений по ссылкам на веб-страницах. Исключение составляют одноразовые ссылки. По ним невозможно скачать легальные приложения, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или вашим данным.
Использовать эвристический анализ	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса. Во время проверки веб-трафика на наличие вирусов и других приложений, представляющих угрозу эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.
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 приложения и пополняется при обновлении баз приложения Kaspersky.
Анти-Фишинг **Использовать эвристический анализ**	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет обнаружить фишинг, даже если веб-адрес отсутствует в базе фишинговых веб-адресов.
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 приложение Kaspersky отображает один из следующих значков:  – если веб-страница, которая открывается по ссылке, безопасна по данным "Лаборатории Касперского";  – если нет информации о безопасности веб-страницы, которая открывается по ссылке;  – если веб-страница, которая открывается по ссылке, по данным "Лаборатории Касперского" может быть использована злоумышленниками для нанесения вреда компьютеру или вашим данным;  – если веб-страница, которая открывается по ссылке, по данным "Лаборатории Касперского" может быть заражена или взломана;  – если веб-страница, которая открывается по ссылке, опасна по данным "Лаборатории Касперского". При наведении курсора мыши на значок отображается всплывающее окно с более подробным описанием ссылки.
На всех сайтах, кроме указанных **Настроить исключения**	При выборе этого варианта приложение проверяет ссылки на всех сайтах, кроме указанных в окне **Исключения**. Окно **Исключения** открывается по ссылке **Настроить исключения**.
Только на указанных сайтах **Настроить проверяемые сайты**	При выборе этого варианта Kaspersky проверяет ссылки только на тех сайтах, которые указаны в окне **Проверяемые сайты**. Окно **Проверяемые сайты** открывается по ссылке **Настроить проверяемые сайты**.
Настроить проверку ссылок	• **Любые ссылки**. Приложение проверяет ссылки на всех типах веб-страниц. • **Только ссылки в результатах поиска**. Приложение проверяет ссылки на веб-страницах с результатами поиска при использовании поисковых систем.
Категории сайтов	Если установлен флажок **Отображать информацию о категориях содержимого сайтов**, приложение добавляет в комментарий к ссылке сведения о том, не принадлежит ли

	сайт к одной из указанных категорий (например, **Насилие** или **Для взрослых**). Вы можете снять флажки напротив категорий, о которых предупреждать не нужно.
Не проверять веб-трафик с доверенных веб-адресов	Если флажок установлен, компонент Интернет-защита не проверяет содержимое веб-страниц / веб-сайтов, адреса которых включены в список доверенных веб-адресов. Вы можете добавить в список доверенных веб-адресов как конкретный адрес веб-страницы / веб-сайта, так и маску адреса веб-страницы / веб-сайта. Список доверенных веб-адресов доступен в окне **Доверенные веб-адреса**, открывающемся по ссылке **доверенных веб-адресов**.

Окно Сайты "Лаборатории Касперского" и ее партнеров

В окне представлен список сайтов "Лаборатории Касперского" и ее партнеров.

Список составляют и обновляют специалисты "Лаборатории Касперского". Список обновляется автоматически при обновлении баз и модулей приложения.

Настройки Защиты от сетевых атак

Компонент Защита от сетевых атак (англ. IDS – Intrusion Detection System) отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на компьютер пользователя, приложение Kaspersky блокирует сетевое соединение с атакующим компьютером. Описания известных в настоящее время видов сетевых атак и методов борьбы с ними содержатся в базах приложения Kaspersky. Список сетевых атак, которые обнаруживает компонент Защита от сетевых атак, пополняется в процессе обновления баз и модулей приложения.

Настройки компонента Защита от сетевых атак

Настройка	Описание
Считать атаками сканирование портов и интенсивные сетевые запросы	*Атака типа Интенсивные сетевые запросы (англ. Network Flooding)* – атака на сетевые ресурсы организации (например, веб-серверы). Атака заключается в отправке большого количества запросов для превышения пропускной способности сетевых ресурсов. Таким образом пользователи не могут получить доступ к сетевым ресурсам организации.

	Атака типа Сканирование портов заключается в сканировании UDP- и TCP-портов, а также сетевых служб на компьютере. Атака позволяет определить степень уязвимости компьютера перед более опасными видами сетевых атак. Сканирование портов также позволяет злоумышленнику определить операционную систему на компьютере и выбрать подходящие для нее сетевые атаки. Если переключатель включен, компонент Защита от сетевых атак блокирует сканирование портов и интенсивные сетевые запросы.
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. Минимальное время, на которое атакующий компьютер можно добавить в список блокирования, составляет одну минуту. Максимальное – 32768 минут.
Настроить исключения	Список содержит IP-адреса, сетевые атаки с которых компонент Защита от сетевых атак не блокирует. Приложение не заносит в отчет информацию о сетевых атаках с IP-адресов, входящих в список исключений.

Настройки Предотвращения вторжений

Развернуть всё | Свернуть всё

Включить / выключить Предотвращение вторжений

Переключатель включает / выключает Предотвращение вторжений.

Узнать больше

По ссылке открывается окно браузера на странице с более подробной информацией о компоненте.

Доверять приложениям, имеющим цифровую подпись

Если флажок установлен, Предотвращение вторжений считает доверенными приложения, имеющие цифровую подпись. Предотвращение вторжений помещает такие приложения в группу **Доверенные** и не проверяет их активность.

Если флажок снят, Предотвращение вторжений не считает приложения с обычной цифровой подписью доверенными и проверяет их активность. Приложения доверенных поставщиков программного обеспечения (например, Microsoft) Предотвращение вторжений считает доверенными независимо от того, установлен флажок или снят.

Загружать правила для приложений из Kaspersky Security Network (KSN)

Если флажок установлен, для определения группы доверия приложения Предотвращение вторжений отправляет запрос в базу Kaspersky Security Network.

Если флажок снят, Предотвращение вторжений не ищет информацию в базе Kaspersky Security Network для определения группы доверия, к которой относится приложение.

Группа доверия для приложений, которые не удалось распределить по другим группам

По ссылке открывается окно **Группа доверия для приложений, которые не удалось распределить по другим группам**. В окне можно выбрать группу доверия, в которую будут помещаться неизвестные приложения.

Можно выбрать один из следующих вариантов:

- Доверенные;
- Слабые ограничения;
- Сильные ограничения;
- Недоверенные.

Изменить группу доверия для приложений, запущенных до начала работы Kaspersky

По ссылке открывается окно **Группа доверия для приложений, запущенных до начала работы приложения Kaspersky**. В окне можно изменить группу доверия для приложений, запущенных до начала работы приложения Kaspersky. Сетевая активность приложений, запущенных до начала работы приложения Kaspersky, будет контролироваться в соответствии с правилами выбранной вами группы доверия.

По умолчанию приложений, запущенные до начала работы приложения Kaspersky, помещаются в одну из групп доверия на основании правил, заданных специалистами "Лаборатории Касперского".

Управление приложениями

По ссылке открывается окно **Управление приложениями**. В нем вы можете отредактировать список правил для приложений.

Управление ресурсами

По ссылке открывается окно **Управление ресурсами**. В нем вы можете сформировать список персональных данных, а также список настроек и ресурсов операционной системы, доступ к которым контролирует Предотвращение вторжений.

Окно Веб-маяки

В окне представлен список веб-маяков.

Список составляют и обновляют специалисты "Лаборатории Касперского". Список обновляется автоматически при обновлении баз и модулей приложения.

Защита от сбора данных в интернете. Категории и исключения

Развернуть всё | Свернуть всё

Сервисы веб-аналитики

Если флажок установлен, компонент Защита от сбора данных в интернете блокирует сервисы веб-аналитики, использующие сбор данных с целью анализа ваших действий в интернете.

По ссылке **Показать список** открывается окно со списком сервисов веб-аналитики, использующих сбор данных с целью анализа ваших действий в интернете.

Рекламные агентства

Если флажок установлен, компонент Защита от сбора данных в интернете блокирует сбор данных о ваших действиях в интернете, который выполняют рекламные агентства в рекламных целях.

По ссылке **Показать список** открывается окно со списком рекламных агентств, выполняющих сбор данных о ваших действиях в интернете в рекламных целях.

Веб-маяки

Если флажок установлен, компонент Защита от сбора данных в интернете блокирует сбор данных о ваших действиях в интернете, выполняемый веб-маяками. Веб-маяки представляют собой невидимые пользователю объекты, внедренные в веб-страницу.

По ссылке **Показать список** открывается окно со списком веб-маяков.

Социальные сети

Если флажок установлен, компонент Защита от сбора данных в интернете блокирует сбор данных при посещении вами социальных сетей, кроме сбора данных, выполняемого самими социальными сетями. Блокирование сбора данных не мешает вам использовать функции "Мне нравится", "+1" и подобные им.

Флажки с названиями социальных сетей позволяют указать социальные сети, на сайтах которых приложение должно блокировать сбор данных.

Исключения

По ссылке открывается окно, где вы можете указать сайты, на которых разрешаете сбор данных о ваших действиях.

Окно Несовместимые сайты

В окне представлен список сайтов, о которых специалистам "Лаборатории Касперского" известно, что их работоспособность может быть нарушена в результате запрета на сбор данных.

Список составляют и обновляют специалисты "Лаборатории Касперского". Список обновляется автоматически при обновлении баз и модулей приложения.

Окно Настройки Защиты от сбора данных в интернете

Развернуть всё | Свернуть всё

Включить / выключить Защиту от сбора данных в интернете

Если переключатель включен, то, когда вы находитесь в интернете, компонент Защита от сбора данных в интернете обнаруживает попытки сбора данных сервисами отслеживания. Сервисы отслеживания используют полученную информацию для анализа ваших действий и могут применять результаты анализа, например, для показа вам соответствующей рекламной информации.

Только собирать статистику

При выборе этого варианта компонент Защита от сбора данных в интернете работает в *режиме обнаружения*, предоставляя вам возможность просмотреть отчеты об обнаруженных попытках сбора данных.

Запретить сбор данных

При выборе этого варианта компонент Защита от сбора данных в интернете работает в *режиме блокировки*, обнаруживая и блокируя попытки сбора данных. Информация о попытках сбора данных записывается в отчет.

Категории и исключения

По ссылке открывается окно, где можно указать категории сервисов отслеживания, которым вы хотите запретить или разрешить сбор данных. Из этого окна можно перейти к формированию списка сайтов, на которых вы хотите разрешить сбор данных.

Отправлять запрет на сбор данных в интернете

Если флажок установлен, то в режиме блокировки при обращении к сайту браузер отправляет на сайт HTTP-заголовок Do not track, означающий запрет на сбор данных о ваших действиях.

Разрешить сбор данных на сайтах "Лаборатории Касперского" и ее партнеров

Если флажок установлен, приложение Kaspersky 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 в интернете на несовместимых сайтах

Если флажок установлен, приложение Kaspersky разрешает сбор данных на сайтах, работоспособность которых может быть нарушена в результате запрета на сбор данных.

Несовместимые сайты

По ссылке открывается окно со списком сайтов, работоспособность которых может быть нарушена в результате запрета на сбор данных.

Окно Рекламные агентства

В окне представлен список рекламных агентств, выполняющих сбор данных о ваших действиях в интернете в рекламных целях.

Список составляют и обновляют специалисты "Лаборатории Касперского". Список обновляется автоматически при обновлении баз и модулей приложения.

Окно Сервисы веб-аналитики

В окне представлен список сервисов веб-аналитики, использующих сбор данных с целью анализа ваших действий в интернете.

Список составляют и обновляют специалисты "Лаборатории Касперского". Список обновляется автоматически при обновлении баз и модулей приложения.

Настройки Почтового Антивируса

Настройка	Описание
Уровень безопасности	Для работы Почтового Антивируса приложение Kaspersky применяет разные наборы настроек. Наборы настроек, сохраненные в приложении, называются *уровнями безопасности*. • **Предельный**. Уровень безопасности почты, при котором компонент Почтовый Антивирус максимально контролирует сообщения. Компонент Почтовый Антивирус проверяет входящие и исходящие сообщения электронной почты, а также выполняет глубокий эвристический анализ. Высокий уровень безопасности почты рекомендуется применять для работы в опасной среде. Примером опасной среды может служить подключение к одному из бесплатных почтовых сервисов из домашней сети, не обеспечивающей централизованной защиты почты. • **Оптимальный**. Уровень безопасности почты, обеспечивающий оптимальный баланс между производительностью приложения Kaspersky 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. Низкий уровень безопасности почты рекомендуется применять для работы в хорошо защищенной среде. Примером такой среды может служить локальная сеть организации с централизованным обеспечением безопасности почты.

Действие при обнаружении угрозы

- **Спрашивать пользователя**. Почтовый Антивирус сообщает вам об обнаружении зараженного или возможно зараженного объекта и запрашивает дальнейшее действие над ним.

  Этот вариант доступен, если в разделе **Настройки → Настройки производительности → Потребление ресурсов компьютера** 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 → Настройки производительности → Потребление ресурсов компьютера** установлен флажок **Автоматически выполнять рекомендуемые действия**.

- **Лечить; удалять, если лечение невозможно**. При обнаружении зараженного объекта во входящем или исходящем сообщении приложение Kaspersky пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение Kaspersky удаляет зараженный объект. Приложение Kaspersky добавит информацию о выполненном действии в тему сообщения, например, *[Сообщение было обработано] <тема сообщения>*.

- **Лечить; блокировать, если лечение невозможно**. При обнаружении зараженного объекта во входящем сообщении приложение Kaspersky пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение Kaspersky добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение Kaspersky пытается вылечить обнаруженный объект. Если вылечить объект не удалось, приложение Kaspersky блокирует отправку сообщения, почтовый клиент показывает ошибку.

- **Блокировать**. При обнаружении зараженного объекта во входящем сообщении приложение Kaspersky добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение Kaspersky 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 приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.
Проверять вложенные файлы форматов Microsoft Office	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты.
Проверять вложенные архивы	Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату.
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 приложения (в том числе приложений-вымогателей) и восстановить состояние операционной системы до установки этого приложения (отменить последствия вредоносной или другой активности приложения). В некоторых случаях отменить последствия действий приложения невозможно, например, если приложение было обнаружено компонентом Предотвращение вторжений.

Мониторинг активности собирает данные из разных источников, в том числе и от других компонентов приложения Kaspersky. Мониторинг активности анализирует активность приложений и предоставляет собранную информацию о событиях другим компонентам приложения Kaspersky.

В блоке **Защита от эксплойтов** вы можете настроить действия при запуске исполняемых файлов из уязвимых приложений.

Контролировать попытки выполнить несанкционированные операции

Флажок включает / выключает функцию защиты от эксплойтов.

Если флажок установлен, приложение Kaspersky отслеживает исполняемые файлы, запускаемые уязвимыми приложениями. Если приложение Kaspersky обнаруживает, что попытка запустить исполняемый файл из уязвимого приложения не была инициирована пользователем, то он выполняет действие, выбранное в раскрывающемся списке **При обнаружении угрозы**.

При обнаружении угрозы

В раскрывающемся списке можно выбрать действие, которое должен выполнять Мониторинг активности в случае запуска исполняемых файлов из контролируемых уязвимых приложений.

Список содержит следующие варианты действий:

- **Спрашивать пользователя**. Мониторинг активности запрашивает действие у пользователя. Этот вариант доступен, если в разделе **Настройки** → **Общие** снят флажок **Автоматически выполнять рекомендуемые действия**.
- **Выбирать действие автоматически**. Мониторинг активности автоматически выполняет действие, указанное в настройках приложения Kaspersky и добавляет информацию о выбранном действии в отчет. Этот вариант доступен, если в разделе **Настройки** → **Настройки производительности** → **Потребление ресурсов компьютера** установлен флажок **Автоматически выполнять рекомендуемые действия**.
- **Разрешать действие**. Мониторинг активности разрешает запуск исполняемого файла.
- **Запрещать действие**. Мониторинг активности блокирует запуск исполняемого файла.

При обнаружении вредоносной или другой активности приложения

В раскрывающемся списке можно выбрать действие, которое должен выполнять Мониторинг активности, если в результате анализа активности была замечена вредоносная или другая активность приложения.

- **Спрашивать пользователя**. Мониторинг активности запрашивает действие у пользователя. Этот вариант доступен, если в разделе **Настройки** → **Настройки производительности** → **Потребление ресурсов компьютера** снят флажок **Автоматически выполнять рекомендуемые действия**.
- **Выбирать действие автоматически**. Мониторинг активности автоматически выполняет действие, рекомендуемое специалистами "Лаборатории Касперского".

Этот вариант доступен, если в разделе **Настройки** → **Настройки производительности** → **Потребление ресурсов компьютера** установлен флажок **Автоматически выполнять рекомендуемые действия**.

- **Выбирать действие автоматически**. Мониторинг активности автоматически выполняет действие, рекомендуемое специалистами "Лаборатории Касперского".
- **Удалять приложение**. Мониторинг активности удаляет приложение.
- **Завершать работу приложения**. Мониторинг активности завершает все процессы приложения.
- **Пропускать**. Мониторинг активности не предпринимает никаких действий с приложением.

При возможности отменить последствия вредоносной или другой активности приложения

В раскрывающемся списке можно выбрать действие, которое Мониторинг активности должен выполнять при наличии возможности отменить последствия вредоносной или другой активности приложения.

- **Спрашивать пользователя**. Если в результате работы Мониторинга активности, Файлового Антивируса или выполнения задачи проверки подтверждается необходимость отмены последствий, Мониторинг активности запрашивает действие у пользователя. Этот вариант доступен, если в разделе **Настройки** → **Настройки производительности** → **Потребление ресурсов компьютера** снят флажок **Автоматически выполнять рекомендуемые действия**.
- **Выбирать действие автоматически**. Если по результатам анализа активности приложения Мониторинг активности признает его вредоносным, то он выполняет отмену последствий активности приложения и уведомляет об этом пользователя. Этот вариант доступен, если в разделе **Настройки** → **Настройки производительности** → **Потребление ресурсов компьютера** установлен флажок **Автоматически выполнять рекомендуемые действия**.
- **Выполнять откат**. Мониторинг активности выполняет отмену последствий вредоносной или другой активности приложения.
- **Не выполнять откат**. Мониторинг активности сохраняет информацию о вредоносной или другой активности приложения, но не выполняет отмену действий приложения.

В блоке **Защита от приложений блокировки экрана** вы можете настроить действия при активизации приложений блокировки экрана. Приложения блокировки экрана – это вредоносные приложения, которые ограничивают возможность работы на компьютере, блокируя экран, клавиатуру, доступ к панели задач и ярлыкам. Приложения блокировки экрана могут требовать выкуп за возврат возможности работы с операционной системой. С помощью функции защита от приложений блокировки экрана можно завершить работу приложения блокировки экрана по нажатию определенной комбинации клавиш.

Распознавать и закрывать приложения блокировки экрана

Флажок включает / выключает использование функции защиты от приложений блокировки экрана.

Если флажок установлен, при обнаружении действий приложения блокировки экрана вы можете остановить ее работу по нажатию комбинации клавиш, указанной в раскрывающемся списке под флажком.

Для закрытия приложения блокировки экрана вручную использовать комбинацию клавиш

В раскрывающемся списке можно выбрать клавишу или комбинацию клавиш, при нажатии которой функция защиты от приложений блокировки экрана обнаруживает и удаляет приложение блокировки экрана.

По умолчанию используется следующая комбинация клавиш: CTRL+ALT+SHIFT+F4.

Настройки Файлового Антивируса

Настройка	Описание
Уровень безопасности	Для работы Файлового Антивируса приложение Kaspersky применяет разные наборы настроек. Наборы настроек, сохраненные в приложении, называются *уровнями безопасности*. • **Предельный**. Уровень безопасности файлов, при котором компонент Файловый Антивирус максимально контролирует все открываемые, сохраняемые и запускаемые файлы. Компонент Файловый Антивирус проверяет все типы файлов на всех жестких, сменных и сетевых дисках компьютера, а также архивы, установочные пакеты и вложенные OLE-объекты. • **Оптимальный**. Уровень безопасности файлов, который рекомендован для использования специалистами "Лаборатории Касперского". Компонент Файловый Антивирус проверяет только файлы определенных форматов на всех жестких, сменных и сетевых дисках компьютера, а также

	вложенные OLE-объекты, компонент Файловый Антивирус не проверяет архивы и установочные пакеты. • **Низкий**. Уровень безопасности файлов, параметры которого обеспечивают максимальную скорость проверки. Компонент Файловый Антивирус проверяет только файлы с определенными расширениями на всех жестких, сменных и сетевых дисках компьютера, компонент Файловый Антивирус не проверяет составные файлы.
Действие при обнаружении угрозы	• **Спрашивать пользователя**. Файловый Антивирус информирует вас об обнаружении зараженного или возможно зараженного объекта и запрашивает дальнейшее действие над ним. Этот вариант доступен, если в разделе **Настройки** → **Настройки производительности** → **Потребление ресурсов компьютера** 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** → **Настройки производительности** → **Потребление ресурсов компьютера** установлен флажок **Автоматически выполнять рекомендуемые действия**. • **Лечить; удалять, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то приложение их удаляет. • **Лечить; блокировать, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то приложение добавляет информацию об

обнаруженных зараженных файлах в список обнаруженных объектов.

- **Блокировать**. Если выбран этот вариант действия, то компонент Файловый Антивирус автоматически блокирует зараженные файлы без попытки их вылечить.

Перед лечением или удалением зараженного файла приложение формирует его резервную копию на тот случай, если впоследствии понадобится восстановить файл или появится возможность его вылечить.

Типы файлов	**Все файлы**. Если выбран этот параметр, приложение проверяет все файлы без исключения (любых форматов и расширений). **Файлы, проверяемые по формату**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы. Перед началом поиска вредоносного кода в файле выполняется анализ его внутреннего заголовка на предмет формата файла (например, TXT, DOC, EXE). В процессе проверки учитывается также расширение файла. **Файлы, проверяемые по расширению**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы. Формат файла определяется на основании его расширения.
Изменить область защиты	По ссылке открывается окно **Область защиты Файлового Антивируса** со списком объектов, которые проверяет Файловый Антивирус. Вы можете добавить в список объекты или удалить добавленные вами объекты. Чтобы исключить объект из проверки, не обязательно удалять объект из списка, достаточно снять флажок напротив названия объекта.
Эвристический анализ	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса.

	Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.
Проверять только новые и измененные файлы	Проверка только новых файлов и тех файлов, которые изменились после предыдущей проверки. Это позволит сократить время выполнения проверки. Такой режим проверки распространяется как на простые, так и на составные файлы.
Проверять архивы	Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату.
Проверять дистрибутивы	Флажок включает / выключает проверку дистрибутивов сторонних приложений.
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 приложение не проверяет составные файлы, размеры которых больше заданного значения. Если флажок снят, приложение проверяет составные файлы любого размера. Приложение проверяет файлы больших размеров, извлеченные из архивов, независимо от состояния флажка.
Распаковывать составные файлы в фоновом режиме **Максимальный размер файла**	Если флажок установлен, приложение предоставляет доступ к составным файлам, размер которых превышает заданное значение, до проверки этих файлов. При этом приложение Kaspersky в фоновом режиме распаковывает и проверяет составные файлы. Приложение предоставляет доступ к составным файлам, размер которых меньше данного значения, только после распаковки и проверки этих файлов. Если флажок снят, приложение предоставляет доступ к составным файлам только после распаковки и проверки файлов любого размера.
Режим проверки	**Интеллектуальный**. Режим проверки, при котором Файловый Антивирус проверяет объект на основании анализа операций,

	выполняемых над объектом. Например, при работе с документом Microsoft Office приложение Kaspersky 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. При обновлении версии приложения Kaspersky, технология iSwift включается для всех типов проверки, даже если ранее она была выключена.
Технология iChecker	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз приложения Kaspersky, дату предыдущей проверки файла, а также изменение настроек проверки. Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной приложению структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).
Исключения	Объекты, исключаемые из проверки. Указываются по ссылке **Настроить исключения**, в окне **Исключения**.
Приостановка работы Файлового Антивируса	Временная автоматическая приостановка работы Файлового Антивируса в указанное время или во время работы с указанными приложениями. Настраивается по ссылке **Приостановить работу Файлового Антивируса**.

Настройки AMSI-защиты

Настройка	Описание
Проверять архивы	Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату.
Проверять дистрибутивы	Флажок включает / выключает проверку дистрибутивов сторонних приложений.
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 приложение не проверяет составные файлы, размеры которых больше заданного значения. Если флажок снят, приложение проверяет составные файлы любого размера. Приложение проверяет файлы больших размеров, извлеченные из архивов, независимо от состояния флажка.

Окно Добавление / изменение персональных данных

Развернуть всё | Свернуть всё

Типы персональных данных

По ссылкам в поле **Название поля** подставляется соответствующий тип персональных данных.

Название поля

Описание, которое отображается в списке записей персональных данных (например, *Домашний телефон*, *Рабочий телефон*, *Почтовый индекс*).

Можно подставить описание персональных данных автоматически по нужной ссылке с типом персональных данных.

Значение

Персональные данные, пересылка которых запрещается или разрешается.

Отчет о пересылке персональных данных

Развернуть всё | Свернуть всё

В верхней части окна отображается имя учетной записи пользователя, отчет о действиях которого приводится в этом окне.

Контроль включен / выключен  /

Переключатель позволяет включать / выключать контроль действий пользователя с помощью Родительского контроля.

В зависимости от того контролирует ли действия пользователя Родительский контроль, переключатель имеет следующий вид:

 – Родительский контроль контролирует действия пользователя.

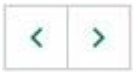
 – Родительский контроль не контролирует действия пользователя.

Контроль действий пользователя выполняется в соответствии с заданными для него настройками Родительского контроля.

В окне можно просмотреть информацию об употреблении выбранным пользователем ключевых слов и попытках пересылки персональных данных.

Сегодня

При нажатии на кнопку отображается отчет о действиях пользователя, совершенных за сегодняшний день.

Кнопки 

При нажатии на кнопки отображаются отчеты за предыдущий и следующий период.

День / Неделя / Месяц

Период, за который формируется отчет. Можно сформировать отчет за следующие периоды: день, неделя, месяц.

Кнопка

При нажатии на кнопку открывается окно настройки Родительского контроля на разделе **Контроль содержимого**. В этом разделе можно указать ограничения пересылки персональных данных.

Список заблокированных персональных данных

Содержит перечень персональных данных в отправленных и полученных выбранным пользователем сообщениях за отчетный период.

Данные

Графа содержит персональные данные, которые содержались в отправленных или полученных сообщениях.

Для заблокированных персональных данных также указывается тип информации, запрещенной к пересылке.

Ресурс

В графе отображается сайт, через который пользователь пытался отправить или получить сообщение с персональными данными, запрещенными к пересылке.

Статус

Если пересылка сообщения была заблокирована Родительским контролем, в графе отображается значение *Заблокировано*.

Дата

Графа содержит дату отправки или получения сообщения, содержащего персональные данные, запрещенные к пересылке.

Выбор профиля пользователя

Развернуть всё | Свернуть всё

Сбор статистики

При нажатии на кнопку к учетной записи выбранного пользователя применяется профиль с предустановленными по умолчанию настройками. Этот профиль предусматривает только сбор статистики о действиях выбранного пользователя. Ограничения на использование приложений и интернета не установлены.

Выборочные ограничения

К учетной записи выбранного пользователя применяются ограничения, настроенные вручную.

Ребенок (4+)

При нажатии на кнопку к учетной записи выбранного пользователя применяется профиль, предусмотренный для детей в возрасте от четырех до двенадцати лет. Этот профиль предусматривает следующие правила использования приложений и интернета:

- разрешено использование интернета;
- разрешено посещение только сайтов, относящихся к категориям "Общение в сети", "Компьютерные игры";
- запрещена загрузка файлов всех типов;
- включен контроль использования компьютера, ограничения использования не установлены;
- включен контроль использования приложений, ограничения использования не установлены;
- включен контроль использования игр, ограничения установлены в соответствии с рейтинговой системой.

Подросток (12+)

При нажатии на кнопку к учетной записи выбранного пользователя применяется профиль, предусмотренный для детей старше двенадцати лет. Этот профиль предусматривает следующие правила использования приложений и интернета:

- разрешено использование интернета;
- разрешено посещение только сайтов, относящихся к категориям "Общение в сети", "Интернет-магазины, банки и платежные системы", "Компьютерные игры";

- включен контроль использования компьютера, ограничения использования не установлены;
- включен контроль использования приложений, ограничения использования не установлены;
- включен контроль использования игр, ограничения установлены в соответствии с рейтинговой системой.

Настройки по умолчанию

При нажатии на кнопку к учетной записи выбранного пользователя применяется профиль с настройками по умолчанию. Этот профиль предусматривает следующие правила использования приложений и интернета:

- разрешено использование интернета;
- разрешено посещение только сайтов, относящихся к категориям "Общение в сети", "Интернет-магазины, банки и платежные системы", "Компьютерные игры";
- включен безопасный поиск;
- включен контроль использования компьютера, ограничения использования не установлены;
- включен контроль использования приложений, ограничения использования не установлены;
- включен контроль запуска игр, ограничения запуска не установлены;
- включен контроль защищенных SSL-соединений в браузерах.

Импорт

По ссылке открывается окно для выбора файла, содержащего настройки Родительского контроля. После выбора файла эти настройки применяются к учетной записи выбранного пользователя.

Экспорт

По ссылке открывается окно для сохранения текущих настроек Родительского контроля в файл.

Окно Добавить / Изменить маску веб-адреса

Развернуть всё | Свернуть всё

Маска веб-адреса

Адрес или маска адреса сайта, доступ к которому требуется разрешить ли запретить.

Действие

Позволяет разрешить или запретить доступ пользователя к сайту.

Можно выбрать один из следующих вариантов:

- **Разрешить**. При выборе этого варианта Родительский контроль разрешает пользователю доступ к сайту, даже если он относится к запрещенной категории или включено блокирование всех сайтов.
- **Запретить**. При выборе этого варианта Родительский контроль запрещает пользователю доступ к сайту, даже если он относится к разрешенной категории.

Тип

Позволяет указать область, на которую распространяется разрешение или запрет доступа к сайту.

Можно выбрать один из следующих вариантов:

- **Маска сайта**. При выборе этого варианта Родительский контроль разрешает или запрещает пользователю доступ ко всем веб-страницам указанного сайта.

  Например, если в поле **Маска веб-адреса** указан адрес example.com, то Родительский контроль будет разрешать или запрещать доступ ко всем веб-страницам сайта example.com: news.example.com, market.example.com, mail.example.com.

- **Указанный веб-адрес**. При выборе этого варианта Родительский контроль разрешает или запрещает пользователю доступ только к конкретной странице сайта, указанной в поле **Маска веб-адреса**.

  Например, если в поле **Маска веб-адреса** указан адрес mail.example.com/login, то Родительский контроль будет разрешать или запрещать доступ только к указанной странице авторизации для входа в почтовый ящик интернет-почты. На другие страницы сайта это правило распространяться не будет.

Применить шаблон

Позволяет применить к исключению один из существующих шаблонов с заданным набором настроек.

Вы можете выбрать один из следующих вариантов:

- **Весь сайт** – при выборе этого варианта Родительский контроль разрешает или запрещает доступ к домену, указанному в поле **Маска веб-адреса**. Например, если в поле **Маска веб-адреса** указан адрес example.com, Родительский контроль будет разрешать или запрещать доступ ко всем веб-страницам домена example.com: news.example.com, market.example.com, mail.example.com.

- **Указанная веб-страница** – при выборе этого варианта Родительский контроль разрешает или запрещает доступ к конкретной странице, указанной в поле **Маска веб-адреса**, и ко всем веб-адресам, содержащим эту страницу. Например, если в поле **Маска веб-адреса** указан адрес example.com/hl, Родительский контроль будет разрешать или запрещать доступ как к этой странице, так и к содержащим ее веб-адресам, например, example.com/hl/example1.html.

- **Указанный веб-адрес** – при выборе этого варианта Родительский контроль разрешает или запрещает доступ к конкретному веб-адресу, указанному в поле **Маска веб-адреса**. Например, если в поле **Маска веб-адреса** указан адрес mail.example.com/login, Родительский контроль будет разрешать или запрещать доступ только к указанной странице авторизации для входа в почтовый ящик интернет-почты. На другие страницы сайта это правило распространяться не будет.

Родительский контроль. Исключения

Развернуть всё | Свернуть всё

В этом окне вы можете сформировать список исключений из заданных настроек Родительского контроля. Настройки доступа к сайтам, добавленным в список исключений, действуют как при блокировке сайтов по категориям (кнопка выбора **Блокировать доступ к сайтам из выбранных категорий**), так и при блокировке всех сайтов (кнопка выбора **Блокировать доступ ко всем сайтам**).

Например, можно разрешить доступ к сайтам из категории "Общение в сети", но добавить в список исключений сайт example.com с запретом доступа. В этом случае Родительский контроль разрешает доступ ко всем социальным сетям, кроме сайта example.com. Также можно установить блокирование всех сайтов и добавить в список исключений сайт интернет-почты, доступ к которому разрешен. В этом случае Родительский контроль предоставляет пользователю доступ только к сайту интернет-почты.

Список исключений

Список содержит перечень веб-адресов, доступ к которым разрешен или запрещен вне зависимости от установленных настроек Родительского контроля.

С помощью контекстного меню веб-адреса в списке можно изменить веб-адрес или удалить его из списка, а также разрешить или запретить доступ к сайту.

Маска веб-адреса

Адрес или маска адреса сайта, доступ к которому разрешен или запрещен.

Тип

В графе указана область применения запрета или разрешения доступа к сайту.

Если в графе установлено значение *Маска сайта*, разрешение или запрет доступа применяется ко всем страницам сайта.

Если в графе установлено значение *Указанный веб-адрес*, разрешение или запрет доступа применяется только к указанной странице сайта.

Действие

В графе указано, разрешен или запрещен доступ к сайту.

Если в графе установлено значение *Разрешено*, Родительский контроль разрешает доступ к сайту.

Если в графе установлено значение *Запрещено*, Родительский контроль запрещает доступ к сайту.

Изменить

При нажатии на кнопку открывается окно **Изменить**, где вы можете изменить маску веб-адреса или адрес веб-сайта, выбранного в списке исключений, и настройки доступа к нему.

Кнопка доступна, если в списке исключений выбрана маска веб-адреса.

Удалить

При нажатии на кнопку приложение удаляет выбранную маску веб-адреса из списка исключений.

Кнопка доступна, если в списке исключений выбрана маска веб-адреса.

Добавить

При нажатии на кнопку открывается окно добавления маски веб-адреса, в котором можно добавить адрес или маску адреса веб-сайта в список исключений.

Окно Ограничения использования приложения

Развернуть всё | Свернуть всё

В этом окне можно настроить ограничения времени использования выбранного приложения.

В блоке **Рабочие дни** вы можете указать ограничения времени использования приложения по рабочим дням.

Разрешить доступ не более <N> часов в день

Флажок включает / выключает ограничение времени использования приложения в рабочие дни.

Если флажок установлен, Родительский контроль ограничивает суммарное время использования приложения для выбранного пользователя. Ограничение времени использования приложения (в часах) указывается в раскрывающемся списке рядом с флажком.

Если флажок снят, Родительский контроль не ограничивает использование приложения по рабочим дням.

В блоке **Выходные дни** вы можете указать ограничения времени использования приложения по выходным дням.

Разрешить доступ не более <N> часов в день

Флажок включает / выключает ограничение времени использования приложения в выходные дни.

Если флажок установлен, Родительский контроль ограничивает суммарное время использования приложения для выбранного пользователя. Ограничение времени использования приложения (в часах) указывается в раскрывающемся списке рядом с флажком.

Если флажок снят, Родительский контроль не ограничивает использование приложения по выходным дням.

В блоке **Перерывы в работе** вы можете настроить периодическое блокирование доступа к приложению в течение суток.

Делать перерыв каждые <N> часов в течение <N> минут

Флажок включает / выключает периодическое блокирование работы приложения с указанной длительностью, чтобы обеспечить отдых пользователя.

Если флажок установлен, Родительский контроль блокирует работу приложения с периодичностью, указанной в раскрывающемся списке **<ЧЧ:ММ>**. Доступ блокируется на промежуток времени, указанный в раскрывающемся списке **<N> минут**.

В блоке **Точное время использования** отображается таблица времени использования приложения. С помощью таблицы вы можете составить почасовое расписание использования приложения пользователем в течение недели.

Таблица времени использования приложения

С помощью таблицы можно указать дни недели и часы, когда пользователю разрешено пользоваться приложением. Строки таблицы соответствуют дням недели, графы – интервалам в один час на временной шкале. В зависимости от установленных в операционной системе региональных настроек временная шкала может иметь 24- и 12-часовое представление. Цвета ячеек таблицы отражают установленные ограничения: красный цвет означает, что использование приложения запрещено, серый – использование приложения разрешено. При нажатии на ячейку таблицы цвет ячейки изменяется. При наведении на ячейку курсора мыши под таблицей отображается временной интервал, которому соответствует ячейка.

Окно Список персональных данных

Развернуть всё | Свернуть всё

Список персональных данных

Список содержит персональные данные пользователя, пересылку которых необходимо контролировать.

Название поля

В графе отображается тип персональных данных (например, *Номер банковской карты*, *Домашний телефон*).

Значение

В графе отображаются персональные данные (например, номер банковской карты, телефон), упоминание которых необходимо отслеживать в переписке.

Изменить

При нажатии на кнопку открывается окно, в котором вы можете изменить запись с персональными данными.

Удалить

Кнопка позволяет удалить выбранную запись из списка.

Добавить

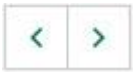
При нажатии на кнопку открывается окно, в котором вы можете добавить в список персональных данных новую запись.

Отчет о заблокированных сайтах и загрузках

Развернуть всё | Свернуть всё

Сегодня

При нажатии на кнопку отображается отчет о действиях пользователя, совершенных за сегодняшний день.

Кнопки 

При нажатии на кнопки отображаются отчеты за предыдущий и следующий период.

День / Неделя / Месяц

Период, за который формируется отчет. Можно сформировать отчет за следующие периоды: день, неделя, месяц.

Кнопка

При нажатии на кнопку открывается окно настройки Родительского контроля на разделе **Интернет**. В этом разделе можно ограничить выбранному пользователю время использования интернета и доступ к сайтам и ограничить скачивание файлов.

Заблокированные сайты и загрузки

Список содержит перечень сайтов, открытие которых было запрещено Родительским контролем, а также перечень файлов, скачивание которых было заблокировано.

Список содержит следующую информацию:

- название заблокированного сайта или файла;
- причина, по которой пользователю заблокирована попытка доступа (например, *Сайт из запрещенной категории*);
- дата открытия сайта или скачивания файла.

Отчет о запускавшихся приложениях

Развернуть всё | Свернуть всё

В верхней части окна отображается имя учетной записи пользователя, отчет о действиях которого приводится в этом окне.

Контроль включен / выключен  / 

Переключатель позволяет включать / выключать контроль действий пользователя с помощью Родительского контроля.

В зависимости от того контролирует ли действия пользователя Родительский контроль, переключатель имеет следующий вид:

 – Родительский контроль контролирует действия пользователя.

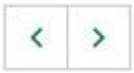
 – Родительский контроль не контролирует действия пользователя.

Контроль действий пользователя выполняется в соответствии с заданными для него настройками Родительского контроля.

В окне **Отчет о запускавшихся приложениях** вы можете получить информацию о запуске приложений за отчетный период для выбранной учетной записи.

Сегодня

При нажатии на кнопку отображается отчет о действиях пользователя, совершенных за сегодняшний день.

Кнопки 

При нажатии на кнопки отображаются отчеты за предыдущий и следующий период.

День / Неделя / Месяц

Период, за который формируется отчет. Можно сформировать отчет за следующие периоды: день, неделя, месяц.

Кнопка

При нажатии на кнопку открывается окно настройки Родительского контроля на разделе **Приложения**. В этом разделе можно указать ограничения запуска и использования приложений.

Часто используемые приложения

Содержит перечень приложений, которые запускались пользователем наиболее часто в течение отчетного периода. Также в списке отображается информация о длительности использования приложений.

Заблокированные приложения

Содержит перечень приложений, запуск которых был заблокирован Родительским контролем. Приложения отображаются в порядке их запуска, начиная с последних.

По ссылке **Еще <N>** можно перейти к просмотру других приложений, запуск которых был заблокирован.

Все используемые приложения

Содержит перечень всех приложений, которые пользователь запускал в течение отчетного периода. Также в списке отображается информация о длительности использования приложений.

Приложения сгруппированы по категориям (например, "Игры" или "IM-клиенты").

При нажатии на кнопку ⌄ можно просмотреть список приложений в категории.

При нажатии на кнопку › список приложений в категории сворачивается в одну строку.

Блокировать игры по категориям

Развернуть всё | Свернуть всё

В этом окне можно разрешить или запретить запуск игр в зависимости от их содержимого. Тип категоризации содержимого игр (набор флажков) соответствует рейтингам PEGI или ESRB. Тип категоризации игр выбирается автоматически в зависимости от вашего местоположения. При необходимости можно установить тип категоризации игр вручную в настройках компонента Родительский контроль.

Если флажок напротив категории установлен, Родительский контроль блокирует запуск игр, относящихся к этой категории.

Если флажок напротив категории снят, Родительский контроль разрешает запуск игр, относящихся к этой категории.

Запуск игры разрешен, если ее содержимое относится к категориям, каждая из которых разрешена.

Окно Область действия пароля

Развернуть всё | Свернуть всё

Управление Резервным копированием

Флажок включает / выключает запрос пароля при попытке пользователя открыть окно **Резервное копирование**.

Настройка приложения

Флажок включает / выключает запрос пароля при попытке пользователя сохранить изменения настроек приложения.

Завершение работы приложения

Флажок включает / выключает запрос пароля при попытке пользователя завершить работу приложения.

Удаление приложения

Флажок включает / выключает запрос пароля при попытке пользователя удалить приложение.

Создать пароль

Кнопка, при нажатии на которую доступ к указанным функциям приложения ограничивается паролем.

Общая статистика

Развернуть всё | Свернуть всё

В верхней части окна отображается имя учетной записи пользователя, отчет о действиях которого приводится в этом окне.

Контроль включен / выключен  / 

Переключатель позволяет включать / выключать контроль действий пользователя с помощью Родительского контроля.

В зависимости от того контролирует ли действия пользователя Родительский контроль, переключатель имеет следующий вид:

 – Родительский контроль контролирует действия пользователя.

 – Родительский контроль не контролирует действия пользователя.

Контроль действий пользователя выполняется в соответствии с заданными для него настройками Родительского контроля.

Профиль: <настройки профиля>

По ссылке можно изменить настройки Родительского контроля, которые требуется применить к текущей учетной записи.

В блоке **Компьютер** можно просмотреть информацию о времени использования компьютера выбранным пользователем, а также перейти к просмотру отчета об использовании компьютера и настройке Родительского контроля. Статистика использования компьютера отображается за период времени, указанный в отчете о времени работы за компьютером. По умолчанию отображается статистика за текущие сутки.

Подробнее

По ссылке открывается окно **Отчет об использовании компьютера**. В окне можно получить информацию об использовании компьютера выбранным пользователем.

Настройка

По ссылке открывается окно. В этом окне вы можете указать время, в течение которого выбранному пользователю можно находиться за компьютером.

В блоке **Приложения** отображается информация о приложениях, которые выбранный пользователь использовал в последнее время. Статистика использования приложений отображается за период времени, указанный в отчете о запускаемых приложений. По умолчанию отображается статистика за текущие сутки.

Подробнее

По ссылке открывается окно **Отчет о запускавшихся приложениях**. В окне вы можете получить информацию о приложениях, которые запускал выбранный пользователь, и времени их использования.

Настройка

По ссылке открывается окно. В этом окне вы можете указать приложения, с которыми выбранный пользователь может работать.

Блок **Интернет** содержит статистику посещений сайтов и отчет о времени, которое провел пользователь на этих сайтах. Также вы можете посмотреть общее количество заблокированных попыток посещения запрещенных сайтов.

Статистика посещения веб-ресурсов отображается за период времени, указанный в отчете о времени работы в интернете. По умолчанию отображается статистика за текущие сутки.

Подробнее

По ссылке открывается окно **Отчет об использовании интернета**. В окне можно получить информацию о веб-ресурсах, которые посещал выбранный пользователь.

Настройка

По ссылке открывается окно. В этом окне вы можете указать время, в течение которого выбранному пользователю можно пользоваться интернетом.

В блоке **Контроль содержимого** отображается информация об количестве заблокированных попыток передачи персональных данных.

Статистика отображается за период времени, указанный в отчете о контроле содержимого. По умолчанию отображается статистика за одну неделю.

Подробнее

По ссылке открывается окно. В окне можно получить информацию о том, какие персональные данные пытался передать выбранный пользователь, общаясь в социальных сетях.

Настройка

По ссылке открывается окно. В этом окне вы можете указать персональные данные, использование которых в переписке выбранного пользователя вы хотите контролировать.

Отчет об использовании интернета

Развернуть всё | Свернуть всё

В верхней части окна отображается имя учетной записи пользователя, отчет о действиях которого приводится в этом окне.

Контроль включен / выключен  / 

Переключатель позволяет включать / выключать контроль действий пользователя с помощью Родительского контроля.

В зависимости от того контролирует ли действия пользователя Родительский контроль, переключатель имеет следующий вид:

 – Родительский контроль контролирует действия пользователя.

– Родительский контроль не контролирует действия пользователя.

Контроль действий пользователя выполняется в соответствии с заданными для него настройками Родительского контроля.

В окне **Отчет об использовании интернета** вы можете получить информацию о сайтах, которые посещал выбранный пользователь за отчетный период.

Сегодня

При нажатии на кнопку отображается отчет о действиях пользователя, совершенных за сегодняшний день.

Кнопки 

При нажатии на кнопки отображаются отчеты за предыдущий и следующий период.

День / Неделя / Месяц

Период, за который формируется отчет. Можно сформировать отчет за следующие периоды: день, неделя, месяц.

Кнопка

При нажатии на кнопку открывается окно настройки Родительского контроля на разделе **Интернет**. В этом разделе можно ограничить выбранному пользователю время использования интернета и доступ к сайтам и ограничить скачивание файлов.

Самые посещаемые сайты

Отчет показывает список сайтов, которые пользователь часто посещал в течение отчетного периода, и количество посещений.

Потрачено

Общее время, проведенное выбранным пользователем в интернете за отчетный период.

Заблокировано веб-ресурсов

Перечень сайтов, открытие которых было запрещено Родительским контролем, а также перечень файлов, скачивание которых было заблокировано.

Показать все

По ссылке открывается окно с информацией о количестве заблокированных загрузок файлов и переходов на сайты.

Категории сайтов

Содержит перечень категорий сайтов. Для каждой категории сайтов указано количество посещений, заблокированных или разрешенных Родительским контролем:

- красным цветом отображается количество переходов на сайты, заблокированных Родительским контролем;
- серым цветом отображается количество переходов на сайты, разрешенных Родительским контролем.

Отчет об использовании компьютера

Развернуть всё | Свернуть всё

В верхней части окна отображается имя учетной записи пользователя, отчет о действиях которого приводится в этом окне.

Контроль включен / выключен /

Переключатель позволяет включать / выключать контроль действий пользователя с помощью Родительского контроля.

В зависимости от того контролирует ли действия пользователя Родительский контроль, переключатель имеет следующий вид:

– Родительский контроль контролирует действия пользователя.

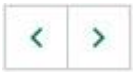
– Родительский контроль не контролирует действия пользователя.

Контроль действий пользователя выполняется в соответствии с заданными для него настройками Родительского контроля.

В окне **Отчет об использовании компьютера** вы можете получить информацию о времени использования компьютера за отчетный период для выбранной учетной записи.

Сегодня

При нажатии на кнопку отображается отчет о действиях пользователя, совершенных за сегодняшний день.

Кнопки 

При нажатии на кнопки отображаются отчеты за предыдущий и следующий период.

День / Неделя / Месяц

Период, за который формируется отчет. Можно сформировать отчет за следующие периоды: день, неделя, месяц.

Кнопка

При нажатии на кнопку открывается окно настройки Родительского контроля на разделе **Компьютер**. В этом разделе можно указать ограничения использования компьютера по времени.

Отчет об использовании компьютера

Содержит информацию о периодах и длительности использования компьютера за отчетный период.

Розовым цветом отображаются промежутки времени, в которые компьютер использовался выбранной учетной записью.

Зеленым цветом отображается текущий период времени (сутки, неделя или месяц).

Красной линией отображается текущее время сегодняшнего дня (если выбран период *День* или *Неделя*).

Окно Управление приложениями

Развернуть всё | Свернуть всё

Запуск / Ограничения

По ссылкам изменяется способ отображения приложений в списке:

- По ссылке **Запуск** список приложений в списке распределяются по двум группам: **Запретить запуск** и **Разрешить запуск**.

- По ссылке **Ограничения** приложений в списке распределяются по группам доверия. Например, доверенные приложения будут располагаться в группе **Доверенные**.

Очистка

По ссылке приложение Kaspersky удаляет из списка несуществующие приложения.

Вид

В раскрывающемся списке можно выбрать вид отображения приложений и процессов.

- **Развернуть все**. При выборе этого варианта в списке отображаются все приложения, установленные на компьютере.

- **Свернуть все**. При выборе этого варианта в списке отображаются группы доверия.

В раскрывающемся списке можно выбрать способ отображения приложений и процессов:

- **Показывать как список**. При выборе этого варианта приложения / процессы отображаются в виде списка.

- **Показывать как дерево**. При выборе этого варианта приложения / процессы отображаются в виде иерархической структуры в соответствии с последовательностью вызова процессов.

В раскрывающемся списке также можно выключить отображение системных приложений, приложений "Лаборатории Касперского" и несетевых приложений:

- **Скрывать системные приложения**. При выборе этого элемента в общем списке приложений и процессов не отображаются приложений, необходимые для работы операционной системы. По умолчанию системные приложений скрыты.

- **Скрывать Kaspersky**. При выборе этого элемента в общем списке приложений и процессов не отображаются приложения "Лаборатории Касперского". По умолчанию приложения "Лаборатории Касперского" скрыты.

- **Показывать только сетевые приложения**. При выборе этого элемента в общем списке приложений и процессов отображаются только сетевые приложения. Сетевые приложения – это приложения, предназначенные для организации совместной работы группы пользователей на разных компьютерах.

Список приложений

В списке содержатся приложения, установленные на вашем компьютере. Для каждого приложения в списке отображается информация о статусе, цифровой подписи, группе доверия, популярности приложения среди пользователей KSN и времени последнего запуска.

По двойному щелчку мышью на строке приложения или процесса открывается окно **Правила приложения**. В окне можно настроить правила для контроля действий приложения.

По правой клавише мыши на строке приложения открывается контекстное меню. В контекстном меню можно выполнить следующие действия:

- открыть окно **Правила приложения**, в котором можно настроить разрешения для действий приложения;
- разрешить или запретить запуск приложения;
- переместить приложение в другую группу доверия;
- установить для приложения настройки контроля активности, предусмотренные по умолчанию (сбросить настройки приложения);
- удалить приложение из списка;
- открыть папку, содержащую исполняемый файл приложения.

Приложения в списке объединены в группы и подгруппы. По правой клавише мыши на строке группы открывается контекстное меню. В контекстном меню можно выполнить следующие действия:

- открыть окно **Правила группы**, в котором можно настроить разрешения для действий приложения из этой группы, используемые по умолчанию;
- создать подгруппу внутри группы; по умолчанию к подгруппе применяются правила, указанные для группы, в которую она входит;
- добавить приложение в группу; по умолчанию к приложению применяются правила, указанные для группы, в которую она входит;
- установить для группы и всех входящих в нее подгрупп и приложений настройки контроля активности, предусмотренные по умолчанию (сбросить настройки группы);
- установить для подгрупп и приложений, входящих в группу, настройки контроля активности, предусмотренные по умолчанию, оставив настройки группы без

изменений (сбросить настройки подгрупп и приложений);

- удалить входящие в группу подгруппы и приложения.

Приложение

В графе отображается название приложения.

Ограничения

В графе отображается группа доверия, в которую помещено приложение. Группа доверия определяет правила использования приложения на компьютере: запрет или разрешение запуска, доступ приложения к файлам и системному реестру, ограничения сетевой активности приложения.

Популярность

В графе отображается уровень популярности приложения среди участников Kaspersky Security Network (KSN). Уровень популярности соответствует числу участников KSN, использующих приложение.

Сеть

В этой графе можно выбрать действие при попытке приложения получить доступ к сети.

В таблице ниже приведено описание действий Kaspersky, если приложение или группа приложений пытается получить доступ к сети.

Описание действий Kaspersky

Действие	Описание
Наследовать	Приложение или группа наследует реакцию из вышестоящей группы.
Разрешить	Kaspersky разрешает приложениям, входящим в выбранную группу, доступ к сети.
Запретить	Kaspersky запрещает приложениям, входящим в выбранную группу, доступ к сети.
Спрашивать пользователя	Если в разделе **Настройки** → **Настройки производительности** → **Потребление ресурсов компьютера** установлен флажок

	Автоматически выполнять рекомендуемые действия, Kaspersky автоматически выбирает действие по правилам, созданным специалистами "Лаборатории Касперского". По сноске вы можете прочитать, какое именно действие будет выбрано. Если этот флажок снят, приложение спрашивает пользователя, предоставлять этому приложению доступ к сети или нет.
Записывать в отчет	Помимо заданной реакции, Kaspersky записывает в отчет информацию о попытке доступа приложения к сети.

Запуск

В графе с помощью переключателя можно разрешить или запретить запуск выбранного приложения. По умолчанию запуск приложения разрешен или запрещен в зависимости от ограничений группы, в которую входит приложение.

О защите компьютера

Приложение Kaspersky обеспечивает комплексную защиту от вирусов, сетевых атак, фишинга, кражи персональных данных и других видов киберугроз. Для решения задач комплексной защиты в составе приложения Kaspersky предусмотрены различные функции и компоненты защиты.

Каждый тип угроз обрабатывается отдельным компонентом защиты. Вы можете включать и выключать компоненты защиты, а также настраивать их работу.

В дополнение к постоянной защите, реализуемой компонентами защиты, рекомендуется периодически выполнять проверку вашего компьютера на присутствие вирусов и других приложений, представляющих угрозу. Это необходимо делать для того, чтобы исключить возможность распространения вредоносных приложений, которые не были обнаружены компонентами защиты, например, из-за установленного низкого уровня защиты или по другим причинам.

Для поддержки приложения Kaspersky в актуальном состоянии необходимо обновление баз и модулей приложения.

Файловый Антивирус

Файловый Антивирус позволяет избежать заражения файловой системы компьютера. Компонент запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы на вашем компьютере и на всех присоединенных дисках. Приложение Kaspersky перехватывает каждое обращение к файлу и проверяет этот файл на присутствие известных вирусов и других приложений, представляющих угрозу. Дальнейшая работа с файлом возможна только в том случае, если файл не заражен или был успешно вылечен программой. Если файл по каким-либо причинам невозможно вылечить, он будет удален. При этом копия файла будет помещена на карантин. Если на место удаленного файла поместить зараженный файл с таким же именем, в карантине сохраняется только копия последнего файла. Копия предыдущего файла с таким же именем не сохраняется.

Защита от сетевых атак

Компонент Защита от сетевых атак запускается при старте операционной системы и отслеживает во входящем трафике активность, характерную для сетевых атак. Обнаружив попытку атаки на компьютер, приложение Kaspersky блокирует любую сетевую активность атакующего компьютера в отношении вашего компьютера.

Интернет-защита

Интернет-защита перехватывает и блокирует выполнение скриптов, расположенных на сайтах, если эти скрипты представляют угрозу безопасности компьютера. Интернет-защита также контролирует весь веб-трафик и блокирует доступ к опасным сайтам.

Почтовый Антивирус

Почтовый Антивирус проверяет входящие и исходящие почтовые сообщения на вашем компьютере. Письмо будет доступно адресату только в том случае, если оно не содержит опасных объектов.

Сетевой экран

Сетевой экран обеспечивает безопасность вашей работы в локальных сетях и в интернете. Компонент фильтрует всю сетевую активность согласно правилам двух типов: правилам для приложений и пакетным правилам.

Сетевой экран доступен только в планах Kaspersky Standard, Kaspersky Plus и Kaspersky Premium.

Мониторинг активности

Компонент Мониторинг активности отменяет в операционной системе изменения, вызванные вредоносной и другой активностью приложений.

Компонент защищает от вредоносных приложений, в том числе от:

- эксплойтов;
- приложения блокировки экрана;
- приложений-шифровальщиков, которые шифруют данные;
- приложений-вымогателей, которые шифруют данные или блокируют доступ к файлам или системе, а затем требуют выкуп за восстановление файлов или доступа к этим файлам.

Не рекомендуется выключать этот компонент.

Анти-Фишинг

Приложение Kaspersky защищает вас от перехода на фишинговые сайты. Фишинговый сайт – это поддельный сайт, который выглядит как сайт банка или платежной системы, или как любой другой сайт. Отличить фишинговый сайт от настоящего по внешним признакам довольно сложно. Переход на фишинговый сайт может привести к краже паролей, данных банковских карт и других персональных данных.

Удаление следов активности / Отмена изменений

В этом окне отображается процесс удаления следов вашей активности в операционной системе. Удаление может занять некоторое время. Для удаления некоторых следов активности может потребоваться перезагрузка компьютера.

Если на первом шаге был выбран вариант **Отменить внесенные ранее изменения**, мастер удаление следов активности выполняет откат действий, выбранных на предыдущем шаге.

Потребление ресурсов компьютера

Настройка	Описание
Автоматически выполнять рекомендуемые действия	Если флажок снят, основные компоненты приложения Kaspersky работают в интерактивном режиме. Это значит, что приложение Kaspersky запрашивает ваше решение при выборе действия с обнаруженными объектами и угрозами, если в настройках

	Файлового Антивируса, Интернет защиты, Почтового Антивируса, Мониторинга активности и Предотвращения вторжений выбран вариант действия **Спрашивать пользователя**. Если флажок установлен, приложение Kaspersky выбирает действие автоматически на основе правил, заданных специалистами "Лаборатории Касперского".
Удалять вредоносные утилиты, рекламные приложения, приложения автодозвона и подозрительные упаковщики	Если флажок установлен, приложение Kaspersky удаляет вредоносные утилиты, рекламные приложения, приложения автодозвона и подозрительные упаковщики в автоматическом режиме защиты. Функция доступна, если установлен флажок **Автоматически выполнять рекомендуемые действия**.
Экономия заряда батареи	Если флажок установлен, то режим экономии питания аккумулятора включен. Приложение Kaspersky откладывает выполнение задач, для которых задан запуск по расписанию. По мере необходимости вы можете самостоятельно запускать задачи проверки и обновления.
Игровой режим	Если флажок установлен, приложение Kaspersky не запускает задачи проверки и обновления, не отображает уведомления, когда вы играете или работаете с приложениями в полноэкранном режиме.
Режим "Не беспокоить"	Если флажок установлен, приложение Kaspersky не показывает уведомления о событиях во время видео-звонков и во время просмотра фильмов.
Откладывать выполнение задач проверки компьютера при высокой нагрузке на центральный процессор и дисковые системы	Когда приложение Kaspersky выполняет задачи по расписанию, может увеличиваться нагрузка на центральный процессор и дисковые подсистемы, что замедляет работу других приложений. Если флажок установлен, то при увеличении нагрузки приложение Kaspersky приостанавливает выполнение задач по расписанию и высвобождает ресурсы операционной системы для других приложений.
Выполнять поиск небезопасных настроек	Если флажок установлен, приложение Kaspersky выполняет поиск небезопасных настроек операционной системы в автоматическом режиме.

операционной системы	
Запускать Kaspersky при включении компьютера (рекомендуется)	Если флажок установлен, то приложение Kaspersky запускается после загрузки операционной системы и защищает компьютер пользователя в течение всего сеанса работы. Если флажок не установлен, то приложение Kaspersky не запускается после загрузки операционной системы до того момента, как пользователь запустит приложение 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 приложение Kaspersky предлагает провести процедуру лечения активного заражения компьютера. После подтверждения пользователем этой процедуры приложение Kaspersky устраняет угрозу. Завершив процедуру лечения активного заражения, приложение Kaspersky выполняет перезагрузку компьютера. Применение технологии лечения активного заражения требует значительных ресурсов компьютера, что может замедлить работу других приложений. Во время обнаружения приложением активного заражения некоторые функции операционной системы могут быть недоступны. Доступность операционной системы восстановится после завершения лечения активного заражения и перезагрузки компьютера.
Включить самозащиту	Если флажок установлен, то Kaspersky предотвращает изменение и удаление файлов приложения на жестком диске, процессов в памяти и записей в системном реестре.
Разрешить управление настройками Kaspersky через приложения удаленного управления	Если флажок установлен, доверенные приложения удаленного администрирования (такие как TeamViewer, LogMeIn Pro и Remotely Anywhere) могут изменять настройки Kaspersky. Недоверенным приложениям удаленного администрирования изменение настроек Kaspersky будет запрещено, даже если флажок установлен.
Включить возможность внешнего управления	Если флажок установлен, то Kaspersky разрешает управление службами приложения с удаленного компьютера. При попытке управления службами приложениями с удаленного компьютера, над значком приложения в области уведомлений панели задач

системными службами	Microsoft Windows отображается уведомление (если служба уведомлений не выключена пользователем).
Включить запись дампов	Если флажок установлен, то Kaspersky записывает дампы в случае сбоев в работе. Если флажок снят, то Kaspersky не записывает дампы. Приложение удаляет уже существующие на жестком диске компьютера файлы дампов.
Включить защиту файлов дампов и файлов трассировки	Если флажок установлен, то доступ к файлам дампов предоставляется системному и локальному администраторам, а также пользователю, включившему запись дампов. Доступ к файлам трассировки предоставляется только системному и локальному администраторам. Если флажок снят, доступ к файлам дампов и файлам трассировки имеет любой пользователь.

Угрозы и исключения

Настройка	Описание
Типы обнаруживаемых объектов	Приложение обнаруживает объекты разных типов, такие как, например, вирусы и черви, троянские приложения, рекламные приложения. Подробнее о них читайте в Энциклопедии "Касперского" . Вы можете выключить обнаружение объектов следующих типов: • Другие приложения, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя. К таким приложениям относятся, например, приложения удаленного администрирования, которые используют системные администраторы; чтобы получать доступ к интерфейсу удаленного компьютера для наблюдения и управления. • 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 приложение не

проверяет объект на вирусы и другие приложения, представляющие угрозу.

Вы можете добавлять, изменять и удалять исключения из списка.

В окне добавления или изменения исключения можно задать условия, в соответствии с которыми объекты должны исключаться из проверки (приложение не будет их проверять):

- Файл или папка, которые нужно исключить из проверки (в том числе можно исключить исполняемые файлы приложений и процессов). Вы можете использовать маски в соответствии со следующими правилами:

  - Символ `*`, 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*`, приложение исключает из проверки объекты типов `Client-IRC`, `Client-P2P` и `Client-SMTP`.

- Хеш-сумму объекта. Сверка хеш-суммы объекта с указанной в этой настройке позволяет исключить из проверки объект, если он не изменялся.

- Компоненты защиты, при работе которых действует исключение.

Вместо удаления исключения из списка можно изменить статус исключения на **Неактивно** (в окне добавления или изменения исключения), в этом случае оно не будет действовать.

Указать доверенные приложения

По ссылке открывается окно со списком доверенных приложений. Приложение Kaspersky не контролирует файловую и сетевую активность доверенных приложений (в том числе и вредоносную), а также обращения этих приложений к системному реестру.

Вы можете добавлять, изменять и удалять доверенные приложений из списка.

> Даже если приложение включено в список доверенных, приложение Kaspersky продолжает проверить исполняемый файл и процесс этого приложения на вирусы и другие угрозы. Если вы хотите, чтобы исполняемый файл и процесс доверенного приложения не проверялись, добавьте их в список исключений.

При добавлении или изменении доверенного приложения вы можете указать правила, в соответствии с которыми приложение Kaspersky контролирует активность доверенного приложения, в окне **Исключения для приложения**.

В окне **Исключения для приложения** доступны для выбора следующие правила:

- Не проверять открываемые файлы.

- Не контролировать активность приложений. Не контролируется любая активность приложения в рамках работы Предотвращения вторжений.

- Не наследовать ограничения родительского процесса (приложения). Если ограничения родительского процесса или приложения не наследуются, активность приложения контролируется по заданным вами правилам или по правилам группы доверия, в которую входит это приложение.

- Не контролировать активность дочерних приложений.

	• Не блокировать взаимодействие с интерфейсом приложения Kaspersky. Приложению разрешено управлять приложением Kaspersky, используя графический интерфейс приложения Kaspersky. Необходимость разрешить приложению управлять интерфейсом приложение Kaspersky может возникнуть при использовании приложений удаленного доступа к рабочему столу или приложения, обеспечивающего работу устройства ввода данных. К таким устройствам относятся, например, сенсорные панели (тачпады), графические планшеты. • Не проверять весь трафик (или зашифрованный трафик). В зависимости от выбранного варианта (**Не проверять весь трафик** или **Не проверять зашифрованный трафик**) приложение Kaspersky исключает из проверки весь сетевой трафик приложения или трафик, передаваемый по протоколу SSL. Значение настройки не влияет на работу Сетевого экрана: Сетевой экран проверяет трафик приложения в соответствии с установленными для него настройками. Исключения влияют на работу Почтового Антивируса, Интернет-защиты и Анти-Спама. Вы можете уточнить IP-адреса или сетевые порты, на которые должно распространяться ограничение контроля трафика. Если в окне **Исключения для приложения** изменить статус на **Неактивно**, приложение Kaspersky не относит приложение к доверенным. Таким образом можно временно исключить приложение из доверенных, не удаляя из списка.
Доверенное системное хранилище сертификатов	Если выбрано одно из доверенных системных хранилищ сертификатов, приложение Kaspersky исключает из проверки приложения, подписанные доверенной цифровой подписью. Kaspersky автоматически помещает такие приложения в группу *Доверенные*. Если выбрано **Не использовать**, то Kaspersky проверяет приложения независимо от наличия цифровой подписи. Приложение Kaspersky помещает приложение в группу доверия в зависимости от уровня опасности, которую это приложение может представлять для компьютера.

Настройки сети

Настройка	Описание
Ограничивать	Если флажок установлен, приложение ограничивает собственный

трафик при лимитном подключении	сетевой трафик в том случае, если подключение к интернету является лимитным. Приложение Kaspersky определяет высокоскоростное мобильное подключение к интернету как лимитное, а подключение по Wi-Fi – как безлимитное. Учет стоимости подключения работает на компьютерах под управлением Windows 8 и выше.
Внедрять в трафик скрипт взаимодействия с веб-страницами	Если флажок установлен, приложение Kaspersky внедряет в трафик скрипт взаимодействия с веб-страницами. Этот скрипт обеспечивает работу таких компонентов как Безопасные платежи, Защита от сбора данных в интернете, Анти-Баннер, Проверка ссылок.
Поддерживать работу DNS поверх HTTPS (DoH)	Если флажок установлен, приложение корректно обрабатывает данные DNS при передаче их по протоколу HTTPS. Мы не рекомендуем снимать этот флажок.
Управлять DoH-серверами	По ссылке открывается окно, в котором вы можете добавить вручную DoH-сервер, через который будет выполняться передача данных DNS в браузере. Здесь вы можете прочитать о том, что такое DNS поверх HTTPS (DoH) и как добавить DoH-сервер.
Контролируемые порты	**Контролировать все сетевые порты**. Режим контроля портов, при котором Почтовый Антивирус, Анти-Спам и Интернет защита контролируют все открытые порты вашего компьютера. **Контролировать только выбранные сетевые порты**. Режим контроля портов, при котором Почтовый Антивирус, Анти-Спам и Интернет защита контролируют выбранные вами порты вашего компьютера. Указать контролируемые сетевые порты можно в окне **Сетевые порты**, которое открывается по ссылке **Выбрать**. Вы также можете указать, при работе каких приложений нужно контролировать все сетевые порты, используемые этими приложениями: • **Контролировать все порты для приложений из списка, рекомендованного "Лабораторией Касперского"**. Список таких приложений задан по умолчанию и входит в комплект поставки приложения Kaspersky. Если установлен этот флажок, приложение Kaspersky контролирует все порты для следующих приложений: • 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 приложений**. Указать приложения можно в окне **Приложения**, которое открывается по ссылке **Выбрать**.

Сетевые порты

Список портов, которые обычно используются для передачи почты и веб-трафика, включен в комплект поставки приложения Kaspersky. По умолчанию приложение Kaspersky контролирует трафик, проходящий через все порты из этого списка. Вы можете добавить в список порты или удалить их из списка.

Если в графе **Статус** в строке порта установлено значение *Активно*, то приложение Kaspersky контролирует трафик, проходящий через этот порт. Если в графе **Статус** в строке порта установлено значение *Неактивно*, то приложение Kaspersky исключает этот порт из проверки, но не удаляет его из списка портов. Изменить статус и другие параметры порта можно в окне по кнопке **Изменить**.

Проверка защищенных соединений

Вы можете выбрать один из режимов проверки защищенных соединений по протоколу SSL:

- **Не проверять защищенные соединения**.
- **Проверять защищенные соединения по запросу компонентов защиты**.
- **Всегда проверять защищенные соединения**.

	Если выбрано **Проверять защищенные соединения по запросу компонентов защиты**, приложение Kaspersky использует установленный сертификат "Лаборатории Касперского" для проверки SSL-соединений, если этого требуют компоненты Интернет защита и Проверка ссылок. Если эти компоненты выключены, приложение Kaspersky не проверяет SSL-соединения. После того как приложение Kaspersky проверит SSL-соединение, в сертификатах сайтов может не отображаться название организации, на которую зарегистрирован сайт. Если вы не хотите, чтобы приложение проверяло SSL-соединение с сайтом, вы можете добавить сайт в список исключений по ссылке **Доверенные адреса**.
В случае возникновения ошибки при проверке защищенного соединения	В раскрывающемся списке вы можете выбрать действие, которое выполняет приложение, если на каком-либо сайте возникла ошибка проверки защищенных соединений. • **Игнорировать**. Приложение разрывает соединение с сайтом, на котором возникла ошибка проверки. • **Спрашивать**. Приложение показывает вам уведомление с предложением добавить адрес сайта в список сайтов, на которых возникли ошибки проверки. Адрес сайта будет проверен по базе вредоносных объектов. • **Добавить домен в исключения**. Приложение добавляет адрес сайта в список сайтов, на которых возникли ошибки проверки. Адрес сайта будет проверен по базе вредоносных объектов.
Домены с ошибками проверки	Список доменов, которые не были проверены из-за того, что при подключении к ним возникли ошибки. Адреса доменов были проверены по базе вредоносных объектов.
Доверенные адреса	По ссылке открывается окно **Доверенные адреса** со списком сайтов, которые вы добавили как исключение для компонентов Интернет защита и Проверка ссылок.
Доверенные приложения	Список приложений, активность которых приложение Kaspersky не проверяет в процессе своей работы. Вы можете выбрать виды активности приложения, которые приложение Kaspersky не будет контролировать (например, не проверять сетевой трафик). Приложение Kaspersky поддерживает переменные среды и символы `*` и `?` для ввода маски.

Блокировать соединения по протоколу SSL 2.0 (рекомендуется)	Если флажок установлен, то приложение блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0. Если флажок снят, то приложение не блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0, и не контролирует сетевой трафик, передаваемый по этим соединениям.
Расшифровывать защищенное соединение с сайтом, использующим EV-сертификат	EV-сертификаты (англ. Extended Validation Certificate) подтверждают подлинность веб-сайтов и повышают безопасность соединения. Браузеры сообщают о наличии на веб-сайте EV-сертификата с помощью значка замка в адресной строке браузера. Также браузеры могут полностью или частично окрашивать адресную строку в зеленый цвет. Если флажок установлен, приложение расшифровывает и контролирует защищенные соединения с EV-сертификатом. Если флажок снят, приложение не имеет доступа к содержанию HTTPS-трафика. Поэтому приложение контролирует HTTPS-трафик только по адресу веб-сайта, например, `https://bing.com`. Если вы впервые открываете веб-сайт с EV-сертификатом, защищенное соединение будет расшифровано независимо от того, установлен флажок или нет.
Настройка прокси-сервера	Параметры прокси-сервера для доступа пользователей клиентских компьютеров в интернет. Приложение Kaspersky использует эти параметры в работе некоторых компонентов защиты, в том числе для обновления баз и модулей приложения. Для автоматической настройки прокси-сервера приложение Kaspersky использует протокол WPAD (Web Proxy Auto-Discovery Protocol). В случае если по этому протоколу не удается определить IP-адрес прокси-сервера, приложение использует адрес прокси-сервера, указанный в параметрах браузера Microsoft Internet Explorer.
Использовать выбранное хранилище сертификатов для проверки защищенных соединений в приложениях Mozilla	Если флажок установлен, приложение проверяет зашифрованный трафик в браузере Mozilla Firefox и почтовом клиенте Thunderbird. Доступ к некоторым сайтам по протоколу HTTPS может быть заблокирован.

Для проверки трафика в браузере Mozilla Firefox и почтовом клиенте Thunderbird должна быть включена проверка защищенных соединений. Если проверка защищенных соединений выключена, приложение не проверяет трафик в браузере Mozilla Firefox и почтовом клиенте Thunderbird.

Приложение расшифровывает и анализирует зашифрованный трафик с помощью корневого сертификата "Лаборатории Касперского". Вы можете выбрать хранилище сертификатов, в котором будет находиться корневой сертификат "Лаборатории Касперского":

- **Использовать хранилище сертификатов Windows (рекомендуется)**. Это хранилище, в которое корневой сертификат "Лаборатории Касперского" добавляется при установке приложения Kaspersky.

- **Использовать хранилище сертификатов Mozilla**. Приложения 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 приложения

Настройка	Описание
Импортировать	Извлечь настройки работы приложения из файла формата CFG и применить их.
Экспортировать	Сохранить текущие настройки работы приложения в файл формата CFG.
Восстановить	Вы в любое время можете восстановить настройки приложения, рекомендуемые "Лабораторией Касперского". В результате восстановления настроек для всех компонентов защиты будет установлен уровень безопасности **Оптимальный**.

Сетевой экран

Настройка	Описание
Уведомлять об уязвимостях при подключении к сети Wi-Fi	Если флажок установлен, приложение Kaspersky показывает уведомления при обнаружении уязвимостей сети Wi-Fi. Флажок доступен для изменения, если на компьютере не установлено приложение Kaspersky Secure Connection. Если установлен флажок **Запрещать передачу пароля в интернете в незащищенном виде и показывать уведомление**, приложение Kaspersky блокирует передачу пароля в незащищенном текстовом виде при заполнении поля **Пароль** в интернете. По ссылке **Выбрать категории** открывается окно **Категории**, в котором вы можете указать типы уязвимостей сетей Wi-Fi. Приложение будет предупреждать вас о том, что сеть Wi-Fi, к которой вы подключаетесь, имеет указанную уязвимость.
Показывать устройства, подключенные к моим сетям	Если флажок установлен, компонент Устройства в моей сети включен и работает.
Разрешать подключения на случайный порт для активного режима FTP	Если флажок установлен, Сетевой экран разрешает подключение к вашему компьютеру на случайный порт, если до этого был обнаружен переход в активный режим FTP на управляющем соединении.
Не выключать Сетевой экран до полного завершения работы операционной системы	Если флажок установлен, Сетевой экран не прекращает работу до полной остановки операционной системы.
Блокировать сетевые соединения, если нет возможности запросить действие у пользователя	Если флажок установлен, работа Сетевого экрана не останавливается в то время, когда не загружен интерфейс приложения Kaspersky.
Правила приложений	По ссылке открывается окно **Сетевые правила приложений**. В окне отображается информация, связанная с контролем сетевой активности приложений и групп приложений.

Сетевую активность приложений в соответствии с сетевыми правилами приложений и групп приложений регулирует компонент Предотвращение вторжений.

Вы можете настроить разрешения на сетевую активность приложения или группы приложений через меню ячейки в графе **Сеть**. Элементы меню описаны в разделе Правила Предотвращения вторжений.

Выбрав в контекстном меню строки пункт **Подробности и правила**, вы можете перейти к настройке сетевых правил приложения или группы приложений.

Пакетные правила

По ссылке открывается окно **Пакетные правила**. По умолчанию в окне представлены предустановленные сетевые пакетные правила, которые рекомендованы специалистами "Лаборатории Касперского" для оптимальной защиты сетевого трафика компьютеров под управлением операционных систем Microsoft Windows.

Сетевые пакетные правила используются для ввода ограничений на сетевые пакеты независимо от приложения. Такие правила ограничивают входящую и исходящую сетевую активность по определенным портам выбранного протокола передачи данных.

Сетевые пакетные правила имеют приоритет над сетевыми правилами приложений.

При добавлении или изменении пакетного правила вы можете установить следующие настройки:

- Действие:
  - **Разрешить**. Приложение Kaspersky разрешает сетевое соединение.
  - **Запретить**. Приложение Kaspersky запрещает сетевое соединение.
  - **По правилам приложения**. Приложение Kaspersky не обрабатывает поток данных в соответствии с пакетным правилом, а применяет правило для приложения (см. **Правила приложений** выше).
- Название.

- Направление:
    - **Входящее**. Приложение Kaspersky применяет правило к сетевому соединению, которое открыл удаленный компьютер.
    - **Исходящее**. Приложение Kaspersky применяет правило к сетевому соединению, которое открыл ваш компьютер.
    - **Входящее/Исходящее**. Приложение Kaspersky применяет правило как к входящему, так и к исходящему пакету или потоку данных, независимо от того, какой компьютер (ваш или удаленный) инициировал сетевое соединение.
    - **Входящее (пакет)**. Приложение Kaspersky применяет правило к пакетам данных, которые принимает ваш компьютер.
    - **Исходящее (пакет)**. Приложение Kaspersky 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**. Приложение Kaspersky применяет правило к IP-адресам всех сетей, подключенных в данный момент и имеющих указанный тип (*Публичная*, *Локальная*

или *Доверенная*). Тип сети вы можете выбрать в раскрывающемся списке, который отображается ниже, если выбрано **Адреса подсети**.

- **Адреса из списка**. Приложение Kaspersky 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. Приложение Kaspersky контролирует передачу сетевых пакетов, у которых время жизни (TTL, Time to Live) не превышает указанного значения.

- Запись событий в отчет приложения Kaspersky.

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 приложения / Правила группы

Настройка	Описание
Файл (только в окне **Правила приложения**)	Справочная информация о приложении и об исполняемом файле приложения. Приложение Kaspersky получает информацию о приложении как из исполняемого файла приложения, так и из Kaspersky Security Network.
Файлы и системный реестр	Правила доступа к ключам системного реестра и к файлам, связанным с работой операционной системы или с вашими персональными данными. Настройки доступа для операций чтения, записи, создания и удаления можно установить независимо друг от друга, с помощью меню в ячейках соответствующих столбцов таблицы. Элементы меню описаны в разделе Правила Предотвращения вторжений.
Права	Права доступа к процессам и ресурсам операционной системы, права на запуск. Установить права доступа можно с помощью меню в ячейках столбца **Действие**. Элементы меню описаны в разделе Правила Предотвращения вторжений.
Сетевые правила	Правила, в соответствии с которыми приложение Kaspersky регулирует сетевую активность приложения или группы приложений.

По умолчанию в списке отображаются предустановленные сетевые правила приложений, которые рекомендованы специалистами "Лаборатории Касперского". Вы не можете удалить или изменить предустановленные сетевые правила (кроме изменения действия в столбце **Разрешение**, см. описание доступных действий в разделе Правила Предотвращения вторжений).

При добавлении правила или его изменении вы можете установить следующие настройки:

- Действие:
  - **Разрешить**. Приложение Kaspersky разрешает сетевое соединение.
  - **Запретить**. Приложение Kaspersky запрещает сетевое соединение.
  - **Спрашивать пользователя**. Приложение Kaspersky спрашивает пользователя о разрешении или запрете сетевого соединения, если в разделе **Настройки** → **Настройки производительности** → **Потребление ресурсов компьютера** снят флажок **Автоматически выполнять рекомендуемые действия**. Если флажок установлен, действие выбирается автоматически. По сноске в окне приложения вы можете прочитать, какое именно действие будет выбрано.
- Название.
- Направление:
  - **Входящее**. Приложение Kaspersky применяет правило к сетевому соединению, которое открыл удаленный компьютер.
  - **Исходящее**. Приложение Kaspersky применяет правило к сетевому соединению, которое открыл ваш компьютер.
  - **Входящее/Исходящее**. Приложение Kaspersky применяет правило как к входящему, так и к исходящему пакету или потоку данных, независимо от того, какой компьютер (ваш или удаленный) инициировал сетевое соединение.
- Протокол.
- Параметры ICMP. Вы можете указать тип и код проверяемых пакетов данных. Блок настроек доступен, если выбраны протоколы ICMP, ICMPv6.

- Удаленные порты (порты удаленного компьютера).
- Локальные порты (порты вашего компьютера).

  Вы можете указать диапазон удаленных или локальных портов (например, `6660 - 7000`), перечислить порты через запятую или сочетать оба способа (например, `80 - 83,443,1080`).

- Адрес:
  - **Любой адрес**.
  - **Адреса подсети**. Приложение Kaspersky применяет правило к IP-адресам всех сетей, подключенных в данный момент и имеющих указанный тип (*Публичная*, *Локальная* или *Доверенная*). Тип сети вы можете выбрать в раскрывающемся списке, который отображается ниже, если выбрано **Адреса подсети**.
  - **Адреса из списка**. Приложение Kaspersky применяет правило к IP-адресам, входящим в заданный диапазон. Вы можете указать IP-адреса в поле **Удаленные адреса**, которое отображается ниже, если выбрано **Адреса из списка**.
- Сетевые адаптеры, через которые передаются сетевые пакеты.
- Использование TTL. Приложение Kaspersky контролирует передачу сетевых пакетов, у которых время жизни (TTL, Time to Live) не превышает указанного значения.
- Запись событий в отчет приложения Kaspersky.

Для быстрого добавления правила вы можете выбрать один из готовых шаблонов в раскрывающемся списке в нижней части окна.

Исключения (только в окне **Правила приложения**)	Вы можете выбрать правила, в соответствии с которыми приложение исключается из проверки: • Не проверять открываемые файлы. • Не контролировать активность приложений. Не контролируется любая активность приложения в рамках работы Предотвращения вторжений.

- Не наследовать ограничения родительского процесса (приложения). Если ограничения родительского процесса или приложения не наследуются, активность приложения контролируется по заданным вами правилам или по правилам группы доверия, в которую входит это приложение.

- Не контролировать активность дочерних приложений.

- Не блокировать взаимодействие с интерфейсом приложения Kaspersky. Приложению разрешено управлять приложением Kaspersky, используя графический интерфейс приложения Kaspersky. Необходимость разрешить приложению управлять интерфейсом приложение Kaspersky может возникнуть при использовании приложений удаленного доступа к рабочему столу или приложения, обеспечивающего работу устройства ввода данных. К таким устройствам относятся, например, сенсорные панели (тачпады), графические планшеты.

- Не проверять весь трафик (или зашифрованный трафик). В зависимости от выбранного варианта (**Не проверять весь трафик** или **Не проверять зашифрованный трафик**) приложение Kaspersky исключает из проверки весь сетевой трафик приложения или трафик, передаваемый по протоколу SSL. Значение настройки не влияет на работу Сетевого экрана: Сетевой экран проверяет трафик приложения в соответствии с установленными для него настройками. Исключения влияют на работу Почтового Антивируса, Интернет-защиты и Анти-Спама. Вы можете уточнить IP-адреса или сетевые порты, на которые должно распространяться ограничение контроля трафика.

История (только в окне **Правила приложения**)	Справочная информация о действиях с приложением, например, о запуске приложения или присвоении группы доверия.

Правила Предотвращения вторжений

Правило – это набор реакций Предотвращения вторжений на действия приложения над различными категориями ресурсов операционной системы и персональных данных.

Возможны следующие реакции Предотвращения вторжений на действия приложения:

- **Наследовать**. Предотвращение вторжений применяет правило к активности приложения, заданное для того статуса, который Предотвращение вторжений присвоило приложению.

  Эта реакция применяется по умолчанию. По умолчанию Предотвращение вторжений наследует права доступа из статуса, который Предотвращение вторжений присвоило приложению.

  Если вы изменили правило для приложения, то в этом случае правило для приложения будет иметь более высокий приоритет, чем правило для статуса, который присвоен приложению.

- **Разрешить**. Предотвращение вторжений позволяет приложению совершать действие.

- **Запретить**. Предотвращение вторжений запрещает приложению совершать действие.

- **Спрашивать пользователя**. Предотвращение вторжений запрашивает решение пользователя, если в разделе **Настройки** → **Настройки производительности** → **Потребление ресурсов компьютера** снят флажок **Автоматически выполнять рекомендуемые действия**. Если флажок установлен, действие выбирается автоматически. По сноске в окне приложения Kaspersky вы можете прочитать, какое именно действие будет выбрано.

- **Записывать в отчет**. Предотвращение вторжений записывает в отчет информацию об активности приложения и своей реакции. Добавление информации в отчет может быть использовано в комбинации с любым другим действием Предотвращения вторжений.

Настройки Защиты ввода данных

Настройка	Описание
Использовать аппаратную виртуализацию, если она доступна	Если флажок установлен, для работы Защищенного браузера используется аппаратная виртуализация (гипервизор). Приложение использует технологию гипервизора для дополнительной защиты от сложных вредоносных приложений, которые могут похищать ваши персональные данные с помощью буфера обмена и фишинга. Флажок отображается в 64-разрядной версии Windows 8, Windows 8.1 и Windows 10. Подробнее о том, что такое аппаратная виртуализация и как она работает, вы можете прочитать по ссылке.
Защита 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). Установите флажки для категорий сайтов, на которых нужно защищать ввод данных с аппаратной клавиатуры.

	По ссылке **Настройка исключений** можно сформировать списки сайтов, на которых нужно включить или выключить защиту ввода данных с аппаратной клавиатуры вне зависимости от выбранных категорий сайтов. При добавлении исключения вы можете использовать маски.
Экранная клавиатура	Многие приложения-шпионы обладают функциями снятия снимков экрана, которые автоматически передаются злоумышленнику для последующего анализа и извлечения персональных данных пользователя. Экранная клавиатура защищает вводимые персональные данные от перехвата посредством снятия снимков экрана. (Подробнее об Экранной клавиатуре). Чтобы Экранная клавиатура включилась, после установки приложение Kaspersky 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. Установите флажки для категорий сайтов, на которых нужно защищать ввод данных с помощью Экранной клавиатуры. По ссылке **Настройка исключений** в окне **Исключения для Экранной клавиатуры** можно сформировать списки сайтов, на которых нужно включить или выключить отображение значка быстрого вызова Экранной клавиатуры вне зависимости от выбранных категорий сайтов. При добавлении исключения вы можете использовать маски.
Показывать в браузере подсказки для создания сильных паролей	Если флажок установлен, приложение Kaspersky проверяет, насколько надежен пароль, который вы вводите в первый раз в браузере, и уведомляет вас об этом.
Защита от использования одинаковых паролей	Когда вы вводите пароль на сайте, где безопасность пароля особенно важна (например, в социальной сети), приложение Kaspersky 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 секретную папку. Файл или папку можно выбрать в дереве, расположенном выше поля ввода, или указать вручную.

Окно открывания секретной папки

Развернуть всё | Свернуть всё

Пароль для доступа к секретной папке

Пароль для доступа к файлам в секретной папке.

Открыть в Проводнике

При нажатии на кнопку в Проводнике открывается папка со списком файлов и папок, хранящихся в секретной папке.

Окно Удаление секретной папки

Развернуть всё | Свернуть всё

Пароль для доступа к секретной папке

Пароль для доступа к файлам в секретной папке.

Удалить секретную папку

При нажатии на кнопку приложение Kaspersky удаляет секретную папку и все файлы в ней.

Файлы и папки, находящиеся в секретной папке, удаляются без возможности восстановления.

Окно переименования секретной папки

Развернуть всё | Свернуть всё

Новое название папки

Новое название, которое будет присвоено секретной папке.

Сохранить

При нажатии на кнопку приложение Kaspersky присваивает секретной папке новое название.

Окно изменения пароля от секретной папки

Развернуть всё | Свернуть всё

Старый пароль

Текущий пароль от секретной папки.

Новый пароль

Новый пароль от секретной папки.

Подтверждение пароля

Повторный ввод пароля, введенного в поле **Новый пароль**.

Сохранить

При нажатии на кнопку текущий пароль от секретной папки заменяется новым.

Окно Выбор файла секретной папке

Развернуть всё | Свернуть всё

Поле для ввода пути к файлу

Поле содержит путь к секретной папке. Секретную папку можно выбрать в дереве, расположенном выше поля ввода, или указать путь к секретной папке 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 приложение Kaspersky подключается к Онлайн-хранилищу и обновляет информацию о размере Онлайн-хранилища и о размере сохраненных в нем файлов.

Кнопка отображается, если приложению 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, приложение Kaspersky в процессе резервного копирования добавляет в хранилище утилиту восстановления Kaspersky Restore Utility. С помощью этой утилиты вы можете восстановить файлы из резервных копий в тех случаях, когда приложение Kaspersky повреждено или не установлено.

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, приложение создает резервную копию этого файла.

Если флажок напротив названия файла снят, приложение 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 Внешний диск

Развернуть всё | Свернуть всё

Список подключенных внешних дисков

В списке перечислены внешние диски, подключенные к компьютеру. Вы можете выбрать один из внешних дисков в качестве хранилища резервных копий.

Если внешний диск отсутствует в списке, вы можете указать путь к нему в поле, расположенном ниже, или нажать на кнопку **Обзор** и выбрать внешний 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 внешний 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 **ОК** 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, внешнего, 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 Поддержка

Развернуть всё | Свернуть всё

Блок **Поддержка "Лаборатории Касперского"** содержит информацию, необходимую для обращения в Службу технической поддержки "Лаборатории Касперского": версию приложения Kaspersky, дату и время выпуска баз и модулей приложения, версию операционной системы, ключ.

Лицензионный ключ

По ссылке **<ключ>** открывается окно **Информация о лицензии**, в котором приведены сведения о действующей лицензии.

Другие версии

По ссылке открывается сайт, с которого вы можете загрузить версию приложения, предназначенную для использования в вашем регионе. Ссылка доступна не во всех версиях приложения.

Ответы на часто задаваемые вопросы

По ссылке открывается окно браузера на странице интерактивной поддержки. Эта страница содержит ответы на вопросы, которые пользователи чаще всего задают специалистам технической поддержки "Лаборатории Касперского".

Рекомендации по настройке приложения

По ссылке открывается окно браузера на странице сайта Службы технической поддержки, где опубликованы статьи о настройке и использовании приложения Kaspersky.

Форум

По ссылке открывается окно браузера на странице Форума "Лаборатории Касперского", где вы можете просматривать опубликованные темы, оставлять свои комментарии, создавать новые темы, пользоваться поиском.

Мониторинг проблем

По ссылке открывается окно **Мониторинг проблем**. В этом окне можно собрать техническую информацию о работе приложения и создать отчет о состоянии системы.

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 удаляются устаревшие версии резервных копий. Количество наиболее новых версий резервных копий, которые нужно оставить в хранилище, указывается в поле **Количество версий резервных копий, которые нужно оставить**.

Резервные копии 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 приложения, соответствующего 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

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 приложение Kaspersky прекращает восстановление файлов из резервных копий.

Окно Восстанавливаемый файл уже существует

Развернуть всё | Свернуть всё

Заменить файл резервной копией

Приложение Kaspersky удаляет существующий файл и помещает на его место файл, восстановленный из резервной копии.

Не восстанавливать этот файл

Приложение Kaspersky оставляет существующий файл без изменений, не восстанавливая одноименный файл из резервной копии.

Сохранить оба файла

Приложение Kaspersky оставляет существующий файл без изменений и сохраняет файл, восстановленный из резервной копии, под новым именем в этой же папке.

Применять это действие во всех подобных случаях

Если флажок установлен, приложение Kaspersky выполняет выбранное действие в отношении всех восстанавливаемых файлов.

Окно Восстановление файлов

Развернуть всё | Свернуть всё

Остановить

При нажатии на кнопку приложение Kaspersky 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, приложение восстанавливает этот файл.

Если флажок напротив имени резервной копии файла снят, то приложение не восстанавливает этот файл.

По правой клавише мыши отображается контекстное меню элемента списка, содержащее следующие пункты:

- **Открыть файл** – файл открывается с помощью приложения, предназначенного для работы с файлами этого типа.
- **Восстановить последнюю версию резервной копии** – открывается окно **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.

Использование Родительского контроля

Родительский контроль позволяет контролировать действия разных пользователей на компьютере и в сети. С помощью Родительского контроля вы можете ограничивать доступ к интернет-ресурсам и приложениям, а также просматривать отчеты о действиях пользователей.

В настоящее время доступ к компьютеру и интернет-ресурсам получает все большее количество детей и подростков. При использовании компьютера и интернета дети сталкиваются с целым рядом угроз:

- потеря времени и / или денег при посещении чатов, игровых ресурсов, интернет-магазинов, аукционов;
- доступ к веб-ресурсам, предназначенным для взрослой аудитории (например, содержащим порнографические, экстремистские материалы, затрагивающим темы оружия, наркотиков, насилия);
- скачивание файлов, зараженных вредоносными приложениями;
- ущерб для здоровья от чрезмерно длительного нахождения за компьютером;
- контакты с незнакомыми людьми, которые под видом сверстников могут получить информацию о ребенке (например, настоящее имя, адрес, время, когда никого нет дома).

Родительский контроль позволяет снизить риски, связанные с работой на компьютере и в интернете. Для этого используются следующие функции:

- ограничение использования компьютера и интернета по времени;

- создание списков разрешенных и запрещенных для запуска игр и приложений, а также временное ограничение запуска разрешенных приложений;
- создание списков разрешенных и запрещенных для доступа сайтов, выбор категорий не рекомендованного к просмотру содержимого веб-ресурсов;
- включение режима безопасного поиска с помощью поисковых систем (при этом ссылки на сайты с сомнительным содержимым не отображаются в результатах поиска);
- ограничение скачивания файлов из интернета;
- запрет пересылки определенных персональных данных.

Вы можете настраивать функции Родительского контроля для каждой учетной записи пользователя на компьютере отдельно. Если пользователь использует две учетные записи: например, локальную учетную запись операционной системы и учетную запись Microsoft, Родительский контроль следует настраивать для учетной записи Microsoft.

Вы также можете просматривать отчеты Родительского контроля о действиях контролируемых пользователей компьютера.

При смене часового пояса или переходе на зимнее или летнее время действуют следующие правила использования компьютера, интернета, а также запуска игр и приложений:

- Если при смене часового пояса не меняется дата, текущий отсчет времени до момента блокировки продолжается без изменений. Такое же правило действует при переходе на зимнее или летнее время.
- Если при смене часового пояса дата меняется в большую или меньшую сторону, израсходованное пользователем время обнуляется, и отчет времени до момента блокировки начинается заново.

Переход к настройке Родительского контроля

Чтобы перейти к настройке Родительского контроля:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Безопасность**.
3. В блоке **Родительский контроль** нажмите на кнопку **Включить**.
4. Если доступ к настройкам Родительского контроля не защищен паролем, приложение предложит задать пароль. Выберите один из предложенных вариантов действия:

- Если вы хотите защитить паролем доступ к настройкам Родительского контроля, выполните следующие действия:

  a. Заполните поля **Пароль** и **Подтверждение пароля** и нажмите на кнопку **Продолжить**.

  b. В окне **Область действия пароля** нажмите на кнопку **Создать пароль**.

  c. В окне **Введите пароль** повторите ввод пароля и нажмите на кнопку **Войти**.

- Если вы не хотите защищать паролем доступ к настройкам Родительского контроля, по ссылке **Пропустить** перейдите к настройке Родительского контроля.

Откроется окно **Родительский контроль**.

5. Выберите учетную запись пользователя и по ссылке **Настроить ограничения** перейдите к окну настройки Родительского контроля.

Контроль использования компьютера

Родительский контроль позволяет задать ограничения времени, проводимого пользователем за компьютером. Вы можете указать интервал времени, когда Родительский контроль должен блокировать доступ к компьютеру (время сна), а также общее ограничение времени использования компьютера в течение дня. Можно указать различные ограничения для рабочих и выходных дней.

Чтобы настроить ограничения времени использования компьютера:

1. Перейдите в окно настройки Родительского контроля.

2. В окне настройки Родительского контроля выберите раздел **Компьютер**.

3. Чтобы указать интервал времени, в течение которого Родительский контроль будет блокировать доступ к компьютеру, в блоках **Рабочие дни** и **Выходные дни** установите флажок **Блокировать доступ с N до N**.

4. В раскрывающемся списке рядом с флажком **Блокировать доступ с N** укажите время начала блокировки.

5. В раскрывающемся списке **до N** укажите время окончания блокировки.

   Родительский контроль будет блокировать пользователю доступ к компьютеру в течение указанного интервала времени.

6. Расписание времени использования компьютера также можно задать с помощью таблицы.

   Таблица отображается при нажатии на кнопку  .

Родительский контроль будет блокировать пользователю доступ к компьютеру **по расписанию**, заданному в таблице.

7. Чтобы ограничить общее время использования компьютера в течение дня, в блоках **Рабочие дни** и **Выходные дни** установите флажок **Разрешить доступ не более N часов в день** и выберите интервал времени в раскрывающемся списке рядом с флажком.

   Родительский контроль будет блокировать пользователю доступ к компьютеру, когда общее время использования компьютера в течение дня превысит указанный интервал.

8. Чтобы задать перерывы при использовании компьютера пользователем, в блоке **Перерывы в работе** установите флажок **Делать перерыв <время> в течение <интервал>** и выберите периодичность (например, каждый час) и длительность (например, 10 минут) перерывов в раскрывающихся списках рядом с флажком.

9. Установите переключатель, расположенный в верхней части окна, в положение **Контроль включен**  .

Родительский контроль будет блокировать доступ пользователя к компьютеру в соответствии с указанными настройками.

Контроль использования интернета

С помощью Родительского контроля вы можете ограничить время использования интернета, а также запретить доступ пользователя к избранным категориям сайтов и отдельным сайтам. Кроме того, вы можете запретить пользователю скачивать из интернета файлы определенных типов (например, архивов, видео).

Как ограничить время использования интернета

Чтобы ограничить время использования интернета:

1. Перейдите в окно настройки Родительского контроля.

2. В окне настройки Родительского контроля выберите раздел **Интернет**.

3. Если вы хотите ограничить общее время использования интернета по рабочим дням, в блоке **Ограничение доступа в интернет** установите флажок **Ограничивать доступ в рабочие дни до N часов в день** и выберите ограничение по времени в раскрывающемся списке рядом с флажком.

4. Если вы хотите ограничить общее время использования интернета по выходным дням, установите флажок **Ограничивать доступ в выходные дни до N часов в день** и выберите ограничение по времени в раскрывающемся списке рядом с флажком.

5. Установите переключатель, расположенный в верхней части окна, в положение **Контроль включен**  .

   Родительский контроль будет ограничивать общее время, проводимое пользователем в интернете, в соответствии с указанными значениями.

Как ограничить посещение определенных сайтов

Чтобы ограничить посещение определенных сайтов:

1. Перейдите в окно настройки Родительского контроля.
2. В окне настройки Родительского контроля выберите раздел **Интернет**.
3. Чтобы в результатах поиска не отображалось содержимое "для взрослых", в блоке **Контроль посещения сайтов** установите флажок **Включить безопасный поиск с помощью поисковых систем**.

   При поиске информации на сайтах, таких как Google, YouTube (только для пользователей, не вошедших на сайт youtube.com под своей учетной записью), Bing, Yahoo!, Yandex среди результатов поиска не будет присутствовать содержимое "для взрослых".
4. Чтобы запретить доступ к сайтам определенных категорий, выполните следующие действия:
   a. В блоке **Контроль посещения сайтов** установите флажок **Контролировать доступ к сайтам**.
   b. Выберите вариант **Блокировать доступ к сайтам из выбранных категорий** и по ссылке **Выбрать категории сайтов** откройте окно **Блокировать доступ к категориям сайтов**.
   c. Установите флажки напротив категорий сайтов, открытие которых необходимо блокировать.

      Родительский контроль будет блокировать открытие сайта пользователем, если его содержимое относится к какой-либо из запрещенных категорий.
5. Чтобы запретить доступ к отдельным сайтам, выполните следующие действия:
   a. В блоке **Контроль посещения сайтов** установите флажок **Контролировать доступ к сайтам**.
   b. По ссылке **Настроить исключения** откройте окно **Исключения**.

c. В нижней части окна нажмите на кнопку **Добавить**.

Откроется окно добавления новой маски веб-адреса.

d. Введите адрес сайта, посещение которого необходимо запретить, в поле **Маска веб-адреса**.

e. Выберите область действия запрета в блоке **Область применения**: весь сайт или только указанная веб-страница.

f. Если вы хотите запретить посещение указанного сайта, в блоке **Действие** выберите вариант **Запретить**.

g. Нажмите на кнопку **Добавить**.

Указанный сайт появится в списке в окне **Исключения**. Закройте окно **Исключения**.

6. Установите переключатель, расположенный в верхней части окна, в положение **Контроль включен**  .

Родительский контроль будет блокировать посещение сайтов в соответствии с указанными настройками.

Как запретить скачивание файлов определенных типов

Чтобы запретить скачивание из интернета файлов определенных типов:

1. Перейдите в окно настройки Родительского контроля.
2. В окне настройки Родительского контроля выберите раздел **Интернет**.
3. В блоке **Запрет загрузки файлов** установите флажки напротив типов файлов, скачивание которых необходимо блокировать.
4. Установите переключатель, расположенный в верхней части окна, в положение **Контроль включен**  .

Родительский контроль будет блокировать скачивание файлов указанных типов из интернета.

Контроль запуска игр и приложений

С помощью Родительского контроля вы можете разрешать или запрещать пользователю запуск игр в зависимости от их возрастной категории. Также вы можете запретить пользователю запуск определенных приложений (например, игр, IM-клиентов) или ограничить время использования приложений.

Как запретить запуск игр, содержимое которых не соответствует возрасту пользователя

Чтобы запретить запуск игр, содержимое которых не соответствует возрасту пользователя:

1. Перейдите в окно настройки Родительского контроля.
2. В окне настройки Родительского контроля выберите раздел **Приложения**.
3. Если вы хотите заблокировать запуск всех игр, содержимое которых не соответствует возрасту пользователя, установите флажок **Ограничить запуск игр для возраста младше** и выберите возрастное ограничение в раскрывающемся списке рядом с флажком.
4. Если вы хотите заблокировать запуск игр с определенным содержимым, выполните следующие действия:
   a. Установите флажок **Блокировать игры из категорий для взрослых**.
   b. По ссылке **Выбрать категории игр** откройте окно **Блокировать игры по категориям**.
   c. Установите флажки напротив категорий содержимого игр, которые нужно блокировать.
5. Вернитесь в раздел **Приложения**.
6. Если вы хотите воспользоваться рейтинговой системой для блокировки игр, выберите тип рейтингов и категоризации содержимого игр в раскрывающемся списке **Для блокирования игр использовать рейтинговую систему**:
   - **Определять автоматически** – Родительский контроль выбирает тип рейтингов игр в зависимости от вашего местоположения: европейскую рейтинговую систему (PEGI) или систему рейтингов для США и Канады (ESRB).
   - **PEGI** – при настройке разрешений запуска игр Родительский контроль использует европейскую рейтинговую систему.
   - **ESRB** – при настройке расширений запуска игр Родительский контроль использует рейтинговую систему для США и Канады.

7. Установите переключатель, расположенный в верхней части окна, в положение **Контроль включен**  .

[Как ограничить запуск определенного приложения]

Чтобы ограничить запуск определенного приложения:

1. Перейдите в окно настройки Родительского контроля.
2. В окне настройки Родительского контроля выберите раздел **Приложения**.
3. По ссылке **Настроить** перейдите в окно **Использование приложений**.
4. По кнопке **Добавить приложение** откройте окно **Открыть** и выберите исполняемый файл приложения.

   Выбранное приложение появится в списке **Использование приложений**. Приложение Kaspersky автоматически добавит это приложение в определенную категорию, например, *Игры*.
5. Выполните следующие действия:

   - Если вы хотите заблокировать запуск приложения, в раскрывающемся списке напротив названия приложения выберите элемент **Блокировать**.
   - Если вы хотите заблокировать запуск всех приложений определенной категории, установите флажок напротив названия категории в списке (например, вы можете заблокировать приложения категории *Игры*).
   - Если вы хотите разрешить запуск приложения, в раскрывающемся списке напротив названия приложения выберите элемент **Разрешить**.
   - Если вы хотите установить ограничения на время использования приложения, в раскрывающемся списке напротив названия приложения выберите элемент **Ограничить**.

     Откроется окно **Ограничение использования приложения**.

     Выполните следующие действия:

     a. Если вы хотите ограничить время использования приложения в рабочие и выходные дни, в блоках **Рабочие дни** и **Выходные дни** установите флажок **Разрешить доступ не более <N> часов в день** и в раскрывающемся списке укажите количество часов в день, в течение которых пользователю разрешено использовать приложение. Также вы можете указать точное

время, когда пользователю разрешено / запрещено использовать приложение, воспользовавшись таблицей **Точное время использования**.

b. Если вы хотите задать перерывы в использовании приложения, в блоке **Перерывы в работе** установите флажок **Делать перерыв <время> в течение <интервал>** и выберите частоту и длительность перерыва в раскрывающихся списках.

c. Нажмите на кнопку **Сохранить**.

6. Закройте окно **Использование приложений**.

7. Установите переключатель, расположенный в верхней части окна, в положение **Контроль включен**  .

   Родительский контроль будет применять заданные ограничения при работе пользователя с приложением.

Контроль содержимого переписки

С помощью Родительского контроля вы можете отслеживать и запрещать пользователю употребление в переписке указанных персональных данных (например, фамилии, номера телефона, номера банковских карт).

Как настроить контроль пересылки персональных данных

Чтобы настроить контроль пересылки персональных данных:

1. Перейдите в окно настройки Родительского контроля.

2. В окне настройки Родительского контроля выберите раздел **Контроль содержимого**.

3. В блоке **Контроль передачи персональных данных** установите флажок **Запретить передачу персональных данных третьим лицам**.

4. По ссылке **Изменить список персональных данных** откройте окно **Список персональных данных**.

5. В нижней части окна нажмите на кнопку **Добавить**.

   Откроется окно добавления персональных данных.

6. Выберите тип персональных данных (например, "номер телефона") по ссылке или введите описание в поле **Название поля**.

7. Укажите персональные данные (например, фамилию, номер телефона) в поле **Значение**.

8. Нажмите на кнопку **Добавить**.

   Персональные данные появятся в списке в окне **Список персональных данных**.

9. Закройте окно **Список персональных данных**.

10. Установите переключатель, расположенный в верхней части окна, в положение **Контроль включен**  .

Родительский контроль будет отслеживать и блокировать употребление указанных персональных данных в переписке через интернет.

Просмотр отчета о действиях пользователя

Вы можете просмотреть отчеты о действиях каждого пользователя, для которого настроен Родительский контроль, отдельно для каждой категории контролируемых событий.

Чтобы просмотреть отчет о действиях контролируемого пользователя:

1. Перейдите в окно настройки Родительского контроля.

2. Выберите учетную запись пользователя и по ссылке **Посмотреть отчет** перейдите к окну отчетов.

3. В блоке с нужным типом ограничения (например, **Интернет**) откройте отчет о контролируемых действиях по ссылке **Подробнее**.

В окне отобразится отчет о контролируемых действиях пользователя.

Окно Категории сайтов

Развернуть всё | Свернуть всё

Интернет-банки и платежные системы

Если флажок установлен, приложение показывает предупреждение, если вы создаете или вводите в интернете пароль, который ранее использовали на сайтах банков и платежных систем.

Социальные сети

Если флажок установлен, приложение показывает предупреждение, если вы создаете или вводите в интернете пароль, который ранее использовали в социальных сетях.

Почтовые сервисы

Если флажок установлен, приложение 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.
- **Приложение долго ищет устройства в сети**. Выберите этот элемент, если компонент Устройства в моей сети работает слишком медленно.
- **Приложение неправильно определяет устройства в сети**. Выберите этот элемент, если приложение неправильно определяет названия и / или типы устройств, подключенных к сети.
- **Много сообщений о новых устройствах в сети**. Выберите этот элемент, если приложение 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 приложению не удается отправить отзыв (например, отсутствует соединение с интернетом), приложение сохраняет отзыв на вашем компьютере. Отзывы хранятся в открытом виде в течение 30 дней.

О Лицензионном соглашении

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

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

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

О режиме ограниченной функциональности

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

Функции приложения Kaspersky в режиме ограниченной функциональности

Функциональность	Ограничения	Режим ограниченной функциональности
Проверка на вирусы		есть
Обновление антивирусных баз и модулей приложения	Доступны только критические обновления.	нет
Поиск уязвимостей в приложениях		есть
Интернет-защита		есть на Windows 7, 8 / нет на Windows 10, 11
Файловый Антивирус		есть на Windows 7, 8 / нет на Windows 10, 11
Почтовый Антивирус		есть на Windows 7, 8 / нет на Windows 10, 11
Мониторинг активности		есть на Windows 7, 8 / нет на Windows 10, 11
Проверка репутации файлов в Kaspersky Security Network		нет
Защита ввода данных		нет
Восстановление зараженного компьютера	Доступно скачивание Kaspersky Rescue Disk через интерфейс приложения.	есть
Угрозы и исключения		есть

Настройки сети		есть
Отчеты и карантин		есть
Настройка отображения приложения		есть
Игровой режим		нет
Режим "Не беспокоить"		нет
Предотвращение вторжений		есть на Windows 7, 8 / нет на Windows 10, 11
Сетевой экран		есть
Защита от сетевых атак		есть
Анти-Спам		есть
Анти-Баннер		есть
Безопасные платежи		нет
Защита от сбора данных в интернете		есть
Удаление следов активности		нет
Устройства в моей сети		нет
Защита веб-камеры		есть на Windows 7, 8 / нет на Windows 10, 11
Мониторинг сети		есть
Менеджер приложений		нет
Менеджер паролей		есть
Уничтожитель файлов		есть
Секретная папка	Доступно только получение доступа к данным в ранее созданных секретных папках.	нет
Резервное копирование	Доступно только восстановление данных из ранее созданных резервных копий.	нет

Обновление приложений	нет
Очистка компьютера	нет
Ускорить работу	нет
Безопасное VPN-соединение	есть
Поиск утечки данных	нет
Устранение неполадок Windows	есть
Быстрый запуск	нет
Поиск небезопасных настроек	нет
Дубликаты файлов	нет
Большие файлы	нет
Неиспользуемые приложения	нет
Диагностика жесткого диска	нет
Текущая активность	нет
Экономия заряда батареи	нет
Сталкерские приложения	нет
Блокировщик скрытых установок	нет
Удалять рекламные приложения	нет
AMSI-защита	есть только на Windows 10, 11
Управление настройками	есть
Защита паролем настроек приложения	есть

Настройка потребления ресурсов компьютера		есть
История		есть
Советы		есть
Родительский контроль	Доступен только просмотр отчетов.	нет
Обращение в техническую поддержку		есть

О фишинге

Фишинг – это вид интернет-мошенничества, заключающийся в краже персональных данных пользователей, распространяемый по электронной почте и другим каналам.

Электронные письма представляют собой поддельные уведомления от банков, провайдеров, онлайн-магазинов, электронных платежных систем или других организаций. В письмах получателя заманивают пройти на сайт мошенников под предлогом, например, обновить регистрационные данные или узнать подробнее о товаре или услуге.

Ничего не подозревающий получатель такого письма проходит по указанной ссылке и оказывается на фишинговом сайте, который выглядит как точная копия официального сайта организации.

Как правило, мошенники могут преследовать разные цели. Одна из них – обманным путем получить конфиденциальные данные пользователей, такие как логины, пароли и другие регистрационные данные, номера счетов и банковских карт. Пользователь вводит данные в веб-форму на сайте, и мошенники получают доступ к деньгам пользователя. Заражение компьютера вирусами и вредоносными приложениями – еще одна ловушка, которая может поджидать пользователя, перешедшего по фишинговой ссылке.

Как распознать мошеннические письма и сайты

Мошеннические письма и сайты на первый взгляд ничем себя не выдают. Усыпляет бдительность наличие логотипов организаций, идентичных настоящим, или официальных контактных номеров телефонов. В письме могут содержаться ссылки, ведущие на официальный сайт, за исключением основной фишинговой ссылки, по которой пользователь и должен будет пройти на сайт злоумышленника.

Насторожить пользователя могут следующие признаки фишинга:

- Домены фишинговых сайтов внешне похожи на настоящие. Однако, внимательно присмотревшись, пользователь может заметить лишние слова (например, официальный домен www.example.com изменен на www.login-example.com), точки или тире вместо слешей (www.example.com/personal/login изменен на www.example.com.personal.login или www.example.com-personal.login). Стоит обратить внимание, что в теле письма может быть указан настоящий домен организации, но когда пользователь перейдет по ссылке, в адресной строке домен будет иным.

- В электронном письме используется неличное обращение, например "Уважаемый пользователь!" или "Здравствуйте!".

- Графика в электронном письме или на сайте выполнена непрофессионально, в тексте встречаются грамматические ошибки.

- Получателя электронного письма просят незамедлительно подтвердить конфиденциальные данные, пройдя по ссылке, а иногда ввести данные прямо в письме. Причиной такой срочности может быть якобы блокировка или взлом аккаунта, угроза потери данных.

Проверка на фишинг

В приложении Kaspersky предусмотрена проверка содержимого электронных писем и веб-ресурсов на наличие фишинговых и вредоносных ссылок. Ссылки проверяются по базе веб-адресов, которые определены специалистами "Лаборатории Касперского" как вредоносные и фишинговые. Базы фишинговых и вредоносных веб-адресов регулярно обновляются.

Для дополнительной защиты во время проверки используется эвристический анализ, а также осуществляются запросы к облачным службам Kaspersky Security Network (KSN). Kaspersky Security Network содержит самые актуальные данные о недавно появившихся угрозах, в том числе о фишинговых и вредоносных веб-ресурсах, которые еще не успели попасть в базы "Лаборатории Касперского". Данные, поступающие в KSN, анализируются сотрудниками Вирусной лаборатории в режиме реального времени.

Если вы попали на фишинговый сайт, вы можете сообщить о нем в Kaspersky Security Network с помощью расширения Kaspersky Protection.

Профиль

Развернуть всё | Свернуть всё

Подключение устройства к My Kaspersky

Аккаунт My Kaspersky необходим для управления подпиской, активации подписки на разных устройствах и управления защитой этих устройств удаленно. В аккаунте My Kaspersky вы можете просматривать состояние всех подключенных к аккаунту устройств, на которых установлено приложение, управлять подписками и хранить коды активации в безопасном месте.

Войти

При нажатии на кнопку открывается окно подключения устройства к аккаунту My Kaspersky. Кнопка доступна, если вы еще не подключили устройство к вашему аккаунту My Kaspersky или не подтвердили, что это ваше устройство.

В зависимости от вашей подписки некоторые функции приложения могут быть недоступны без подключения устройства к вашему аккаунту My Kaspersky.

Управлять аккаунтом

При нажатии на кнопку в браузере по умолчанию открывается ваш аккаунт на сайте My Kaspersky. Кнопка доступна после того, как вы войдете в аккаунт на этом устройстве.

Кнопка 

При нажатии на кнопку устройство будет отключено от аккаунта My Kaspersky. Кнопка доступна, если устройство подключено к аккаунту My Kaspersky.

В зависимости от вашей подписки, подключение устройства к вашему аккаунту My Kaspersky может быть обязательным. В этом случае после отключения устройства от аккаунта вы больше не сможете пользоваться приложением.

Подробнее об аккаунте My Kaspersky

Информация о подписке

Здесь содержится общая информация о подписке, по которой работает ваше приложение. Вы можете посмотреть статус подписки, количество дней, оставшихся до окончания оплаченного периода, статус автопродления подписки, имя владельца подписки, если вы им не являетесь.

Подробнее

При нажатии на кнопку открывается окно **Информация о подписке** с детальной информацией о вашей подписке. Здесь вы можете найти следующую информацию:

- статус подписки;
- статус автопродления подписки;
- лицензионный ключ, который может понадобиться при обращении в Техническую поддержку;
- ссылку на Лицензионное соглашение;
- ссылку на Положение о Веб-Портале;
- общее количество устройств, которые вы можете защитить по подписке;
- количество устройств, которые вы защищаете по подписке;
- дату активации;
- дату истечения срока действия оплаченного периода.

Чтобы открыть другие доступные действия с вашей подпиской, нажмите на кнопку ••• . В зависимости от вашей подписки и ее статуса список доступных действий различается.

Обновить статус

При нажатии на кнопку можно получить актуальную информацию о статусе вашей подписки.

Ввести код активации

По кнопке открывается окно ввода кода активации. В зависимости от вашей подписки кнопка может быть недоступна.

Более подробную информацию о кодах активации вы можете прочитать в разделах Если вы купили коробку или карту активации и Продление подписки с помощью резервного кода активации.

Выбрать другую подписку

По кнопке открывается окно со списком подписок, доступных в аккаунте My Kaspersky и совместимых с вашим приложением.

Кнопка доступна, если вы подключили устройство к аккаунту My Kaspersky.

Управлять подпиской

По кнопке открывается ваш аккаунт My Kaspersky на странице управления подпиской. Кнопка доступна, если вы подключили устройство к аккаунту My Kaspersky.

Продлить сейчас / Купить сейчас

В зависимости от статуса вашей подписки вы можете продлить текущую подписку или купить новую подписку.

Кнопка доступна, если ваша подписка истекла, у вас не активирована функция автопродления и вы не добавляли в приложение резервный код активации.

Возобновить

Кнопка доступна, если вы отменили подписку. В течение некоторого времени после отмены подписки вам будет доступна возможность возобновить ее.

Возможность возобновить текущую подписку может быть недоступна в вашем регионе.

Подробнее о том, как управлять вашей подпиской

Защита других устройств

Здесь вы можете посмотреть сколько устройств вы можете защитить по вашей подписке, сколько устройств вы защищаете, а также начать защищать новые устройства. Информация обновляется после запуска приложения, если вы подключили устройство к аккаунту My Kaspersky.

Количество устройств, на которых вы можете использовать подписку, определяется планом подписки и условиями Лицензионного соглашения.

Кнопка +

По кнопке открывается окно **Защитите больше устройств**, где вы можете выбрать удобный для вас способ отправить подписку на устройство.

Кнопка доступна, если по вашей подписке вы можете защитить больше одного устройства.

В зависимости от вашей подписки, кнопка может не отображаться.

При нажатии на кнопку доступны следующие действия:

Защитить устройство

По кнопке открывается окно **Защитите больше устройств**, где вы можете выбрать удобный для вас способ отправить подписку на другое устройство.

Кнопка доступна, если по вашей подписке вы можете защитить больше одного устройства.

Управлять устройствами

По кнопке открывается ваш аккаунт My Kaspersky на странице управления подпиской в разделе **Мои устройства**. Здесь вы можете посмотреть все устройства, работающие по вашей подписке, и проверить состояние этих устройств.

Если вы еще не подключили устройство к аккаунту My Kaspersky, то откроется окно подключения к аккаунту.

Подробнее о том, как управлять устройствами удаленно, вы можете прочитать в Справке My Kaspersky.

В зависимости от вашей подписки может быть доступна только информация об общем количестве устройств, которые вы можете защитить.

Подробнее о том, как защитить другие устройства по вашей подписке

Предложения для вас

На этой странице будут собраны интересные для вас предложения от "Лаборатории Касперского" или наших партнеров. Здесь вы сможете купить подходящее именно вам решение, а также найти уже приобретенные вами приложения или услуги, посмотреть статус подписки, перейти к установке приложения или прочитать инструкцию по использованию.

По кнопке **Купить** вы будете перенаправлены в интернет-магазин, чтобы ознакомится с выбранным решением подробнее и оформить покупку. Вся информация о покупке и инструкции по активации отправляются на вашу электронную почту.

Управлять приобретенными подписками вы сможете в вашем аккаунте My Kaspersky.