Kaspersky
Free

Содержание

Предоставление данных

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

Предоставление данных в рамках Лицензионного соглашения

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.

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" .

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 **Положении 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.

Файлы отчетов могут содержать следующие персональные данные:

- IP-адрес устройства пользователя;
- история посещения сайтов;
- версия браузера и операционной системы;
- имена и пути расположения файлов cookie и других файлов;
- адрес электронной почты, отправитель, тема письма.

Файлы отчетов хранятся локально на вашем компьютере и не передаются в "Лабораторию Касперского". Путь к файлам отчетов: %allusersprofile%\Kaspersky Lab\AVP21.9\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 Free включена самозащита. Если самозащита выключена, файлы отчетов не защищаются.

Сохранение служебной информации о работе приложения

Приложение также обрабатывает и хранит следующие данные, которые могут понадобиться для анализа ошибок в работе:

- Данные, которые отображаются в интерфейсе приложения:
  - адрес электронной почты, используемый для подключения к My Kaspersky;
  - адреса сайтов, которые были добавлены в исключения (отображаются в компоненте Сеть и в окне Отчеты);
  - данные о лицензии.

  Эти данные хранятся локально в немодифицированном виде и доступны для просмотра под любой учетной записью на компьютере.
- Данные о системной памяти процессов Kaspersky Free 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. Состав данных описан в файле RDP.txt по адресу: %PROGRAMFILES%\Kaspersky Lab\Kaspersky 21.7\Doc\KFA\ru-RU.

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.

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 Kaspersky Free

Kaspersky Free – это обновление бесплатной версии защиты. При переходе на это обновление вы получаете уже знакомое вам высокое качество защиты, дополненное нашими новыми разработками, с полностью обновленным интерфейсом для удобного использования.

Вы также всегда можете перейти на платную подписку приложения Kaspersky без дополнительного скачивания и установки программного обеспечения.

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. Kaspersky Free 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. 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.

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.

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.

Анти-Фишинг

Анти-Фишинг позволяет проверять веб-адреса на принадлежность к списку фишинговых веб-адресов. Этот компонент встроен в Интернет-защиту.

Мониторинг активности

Компонент Мониторинг активности отменяет в операционной системе изменения, вызванные вредоносной и другой активностью программ.

Компонент защищает от вредоносных программ, в том числе от:

- эксплойтов;
- программ блокировки экрана;
- программ-шифровальщиков, которые шифруют данные;
- программ-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.

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, Kaspersky Free блокирует любую сетевую активность атакующего компьютера в отношении вашего компьютера.

Экранная клавиатура

Экранная клавиатура позволяет избежать перехвата данных, вводимых через аппаратную клавиатуру, и защищает персональные данные от перехвата посредством снятия снимков экрана.

Antimalware Scan Interface (AMSI)

Antimalware Scan Interface (AMSI) позволяет стороннему приложению с поддержкой AMSI отправлять объекты в Kaspersky Free для дополнительной проверки (например, скрипты PowerShell) и получать результаты проверки этих объектов.

Аппаратные и программные требования

Общие требования

- 1500 МБ свободного места на жестком диске.
- Процессор с поддержкой инструкций SSE2 (кроме Arm).
- 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 6.x (не ниже 6.0.10).

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)	Подсистема Windows для Linux 2 (WSL2) не поддерживается.
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 выше, Windows 8.1 Update)	1 ГГц или выше	1 ГБ (для 32-разрядной операционной системы) или 2 ГБ (для 64-разрядной операционной системы)
Microsoft Windows 8.1 Pro (Service Pack 0 или выше, Windows 8.1 Update)		
Microsoft Windows 8.1 Enterprise (Service Pack 0 или выше, Windows 8.1 Update)		
Microsoft Windows 8 (Service Pack 0 или выше)	1 ГГц или выше	1 ГБ (для 32-разрядной операционной системы) или 2 ГБ (для 64-разрядной операционной системы)
Microsoft Windows 8 Pro (Service Pack 0 или выше)		
Microsoft Windows 8 Enterprise (Service Pack 0 или выше)		

Microsoft Windows 7 Starter (Service Pack 1 или выше)	1 ГГц или выше	1 ГБ (для 32-разрядной операционной системы) или 2 ГБ (для 64-разрядной операционной системы)
Microsoft Windows 7 Home Basic (Service Pack 1 или выше)		
Microsoft Windows 7 Home Premium (Service Pack 1 или выше)		
Microsoft Windows 7 Professional (Service Pack 1 или выше)		
Microsoft Windows 7 Ultimate (Service Pack 1 или выше)		

Для работы компонента Интернет-защита в операционной системе должна быть запущена служба Base Filtering Engine (служба базовой фильтрации).

Поддержка браузеров

Браузеры, которые поддерживают полнофункциональную работу приложения:

- Microsoft Edge на базе Chromium 77.x – 107.x;
- Mozilla Firefox версий 52.x – 107.x;
- Mozilla Firefox ESR 52.x, 60.x, 68.x, 78.x, 91.x, 102.x;
- Google Chrome версий 48.x – 108.x;
- Яндекс.Браузер 18.3.1 – 22.11.2 (есть ограничения).

Браузеры, которые поддерживают установку расширения Kaspersky Protection:

- Microsoft Edge на базе Chromium 77.x – 107.x;
- Mozilla Firefox версий 52.x – 107.x;

- Mozilla Firefox ESR 52.x, 60.x, 68.x, 78.x, 91.x, 102.x;
- Google Chrome версий 48.x – 108.x.

Браузеры, которые поддерживают Экранную клавиатуру и Проверку защищенных соединений:

- Microsoft Edge на базе Chromium 77.x – 107.x;
- Mozilla Firefox версий 52.x – 107.x;
- Mozilla Firefox ESR 52.x, 60.x, 68.x, 78.x, 91.x; 102.x;
- Google Chrome 48.x – 108.x.

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

Kaspersky Free 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.

О вашей подписке

Подписка определяет настройки приложения (срок действия подписки, количество защищаемых устройств). Подписка предоставляется вам на основании Лицензионного соглашения.

Подписка включает в себя право на получение следующих видов услуг:

- Использование приложения на одном или нескольких устройствах.

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

- Обновление баз и предоставление новых версий приложения.
- Оповещение о выходе новых приложений "Лаборатории Касперского", а также о появлении новых вирусов и вирусных эпидемиях.

Подписка на использование Kaspersky Free продлевается автоматически без вашего участия.

Совместимость с другими приложениями "Лаборатории Касперского"

Приложение Kaspersky Free 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, 5.8, 5,9.

Что нового в последней версии приложения

В приложении Kaspersky Free появились следующие новые возможности и улучшения:

- Добавлена возможность изменять размер окна приложения.
- Улучшен процесс установки расширения Kaspersky Protection в браузерах. В раздел Безопасность добавлены статусы установки расширения в браузерах.
- Улучшен Игровой режим и режим "Не беспокоить". Если в приложении Kaspersky Free включены режимы "Не беспокоить" и Игровой режим, будет выключен показ уведомлений в приложениях Kaspersky Secure Connection и Kaspersky Password Manager, установленных на этом же устройстве.

- Улучшено главное окно приложения. Приведены к одному виду блоки компонентов.
- Улучшены уведомления приложения. В них добавлены графические изображения, раскрывающие тему уведомления.
- На главной странице в блок **История** добавлены события включения и выключения Игрового режима и режима "Не беспокоить".

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, а также подтвердить, что вам уже исполнилось 16 лет. Для прекращения работы мастера на любом шаге установки следует закрыть окно мастера.

Чтобы установить приложение на ваш компьютер,

запустите исполняемый файл мастера установки и удаления, скачанный вами из интернета.

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

Вы можете установить Kaspersky Free 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	Прим
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\sa
KLPASSWD=<значение>	Установить пароль на различные функции продукта. Если при этом не задано значение параметра KLPASSWDAREA, используется область действия пароля по умолчанию:	saas21.exe /pKLPASSWD=123

	• изменение настроек приложения; • 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 /pSELFPROTECTI(
ALLOWREBOOT=1	Разрешить перезагрузку в случае необходимости.	saas21.exe /pAl

SKIPPRODUCTCHECK=1	Не выполнять поиск приложений, несовместимых с Kaspersky Free.	saas21.exe /pSKIPPRODUCTCH
-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 Free 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.

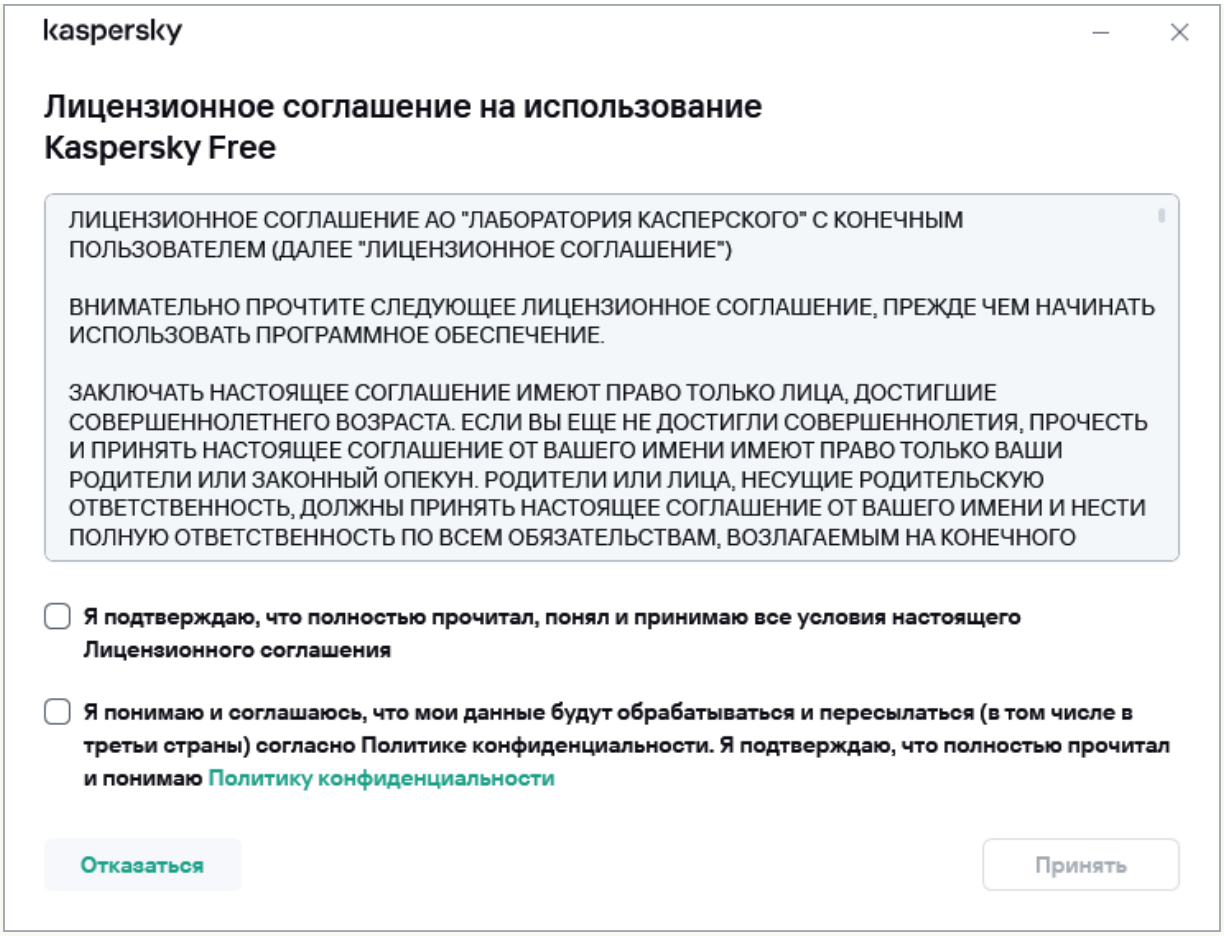
   В зависимости от типа установки и языка локализации на этом шаге мастер может предлагать вам ознакомиться с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", а также принять участие в программе Kaspersky Security Network.

   Просмотр Лицензионного соглашения

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

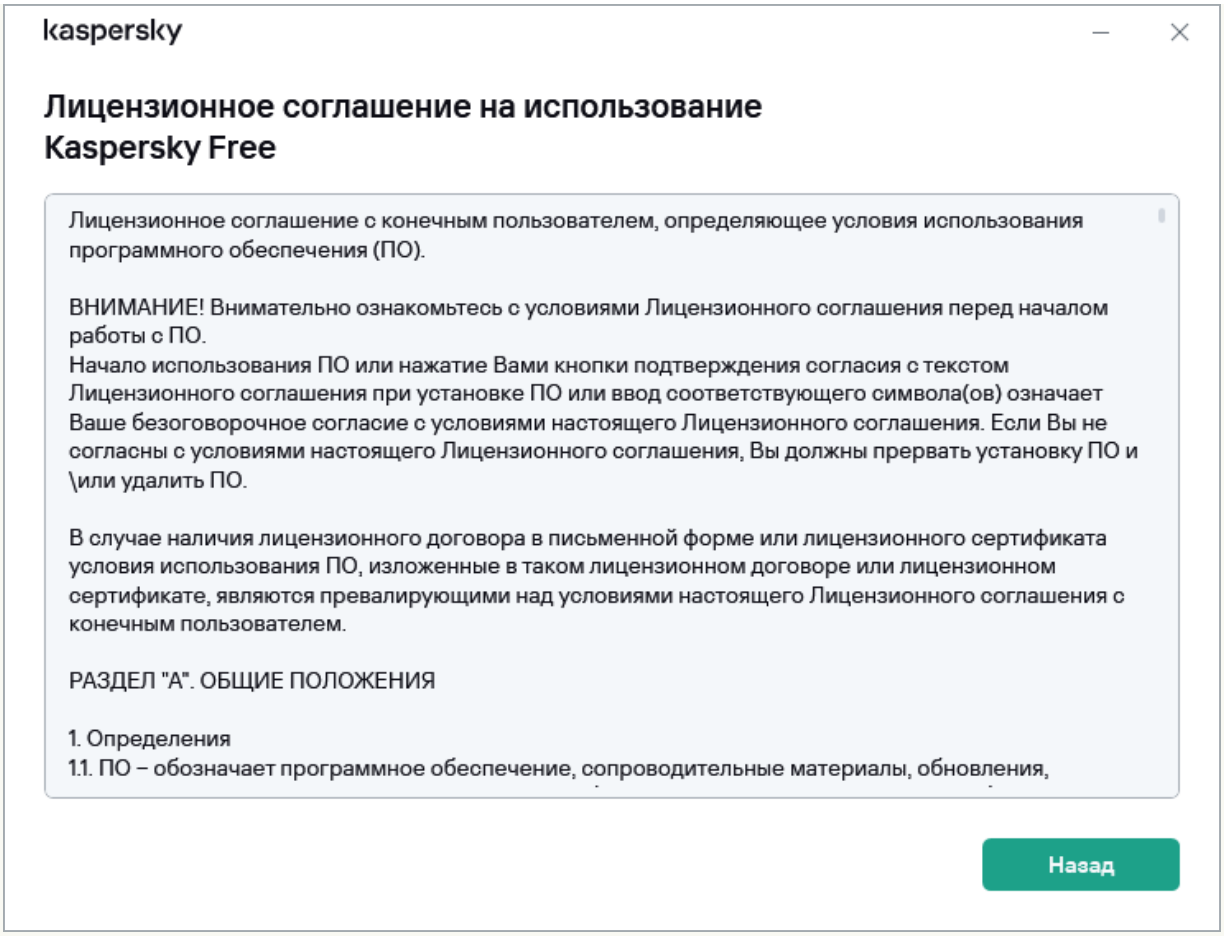
   На этом шаге мастер предлагает вам ознакомиться с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского".

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



Окно принятия Лицензионного соглашения

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.



Окно с текстом Лицензионного соглашения

Установка приложения на ваш компьютер будет продолжена.

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

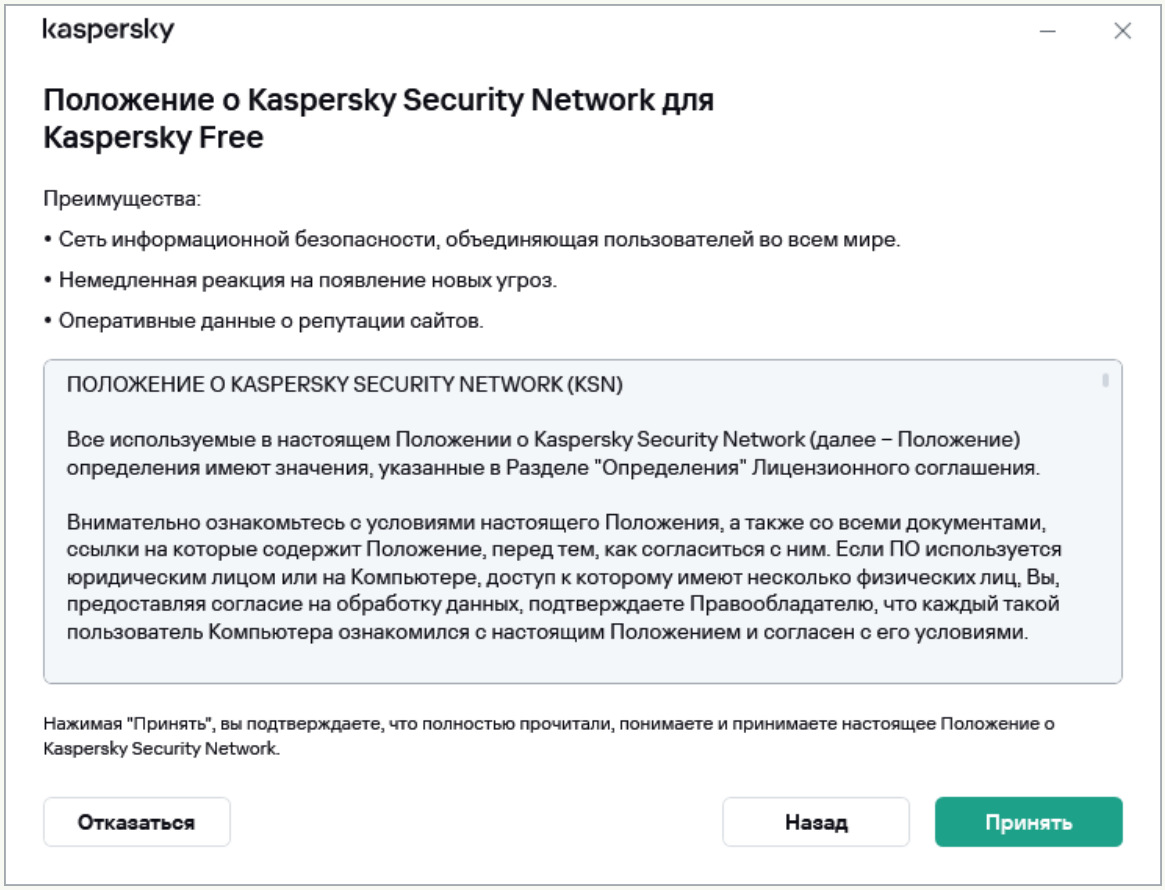
В некоторых регионах для продолжения установки приложения вы также должны принять условия Политики конфиденциальности.

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.

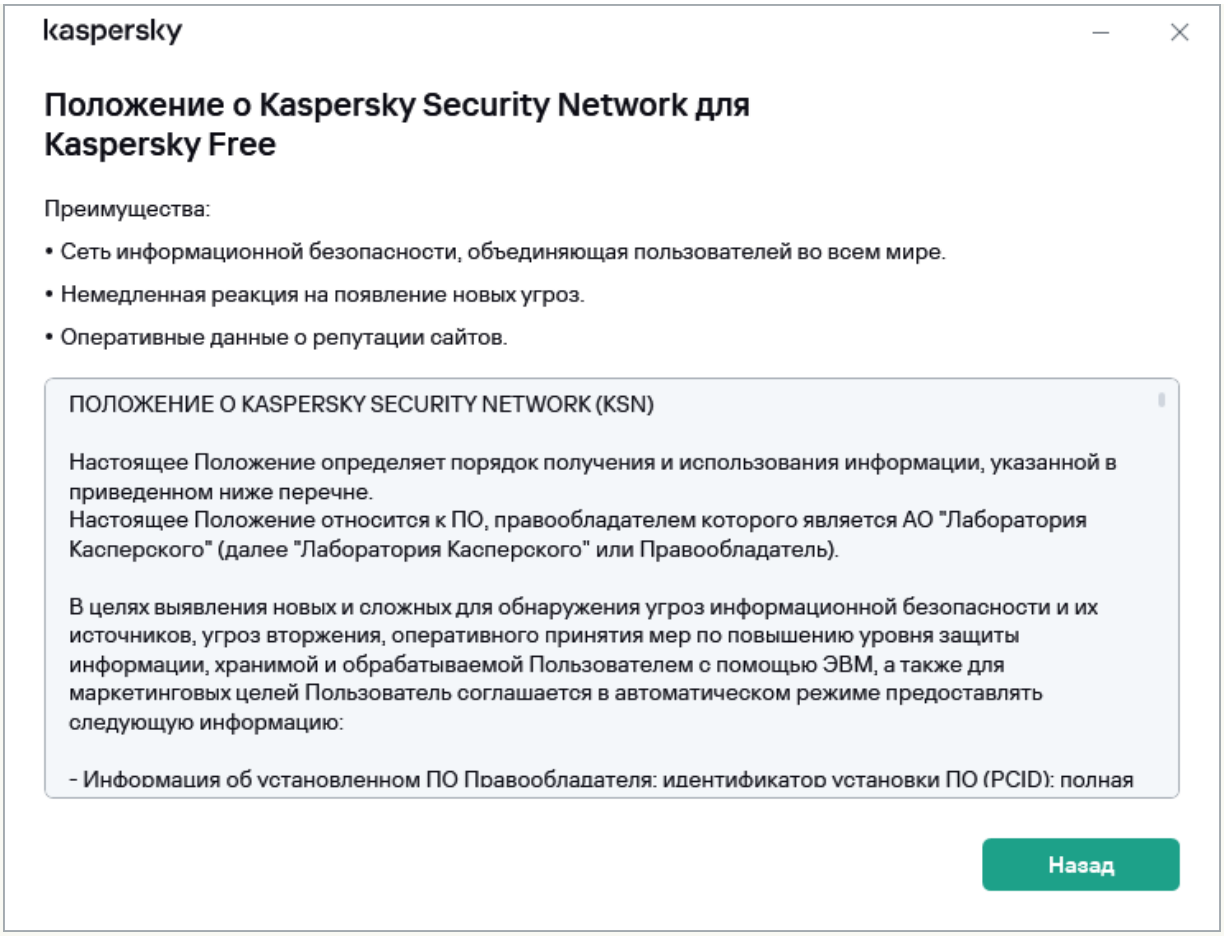
Ознакомьтесь с Положением о Kaspersky Security Network и выполните одно из действий.

- Если вы согласны со всеми его пунктами, нажмите на кнопку **Принять**.
- Если вы не хотите принимать участие в программе Kaspersky Security Network, нажмите на кнопку **Отказаться**.



Окно принятия Положения о Kaspersky Security Network

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.



Положение 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

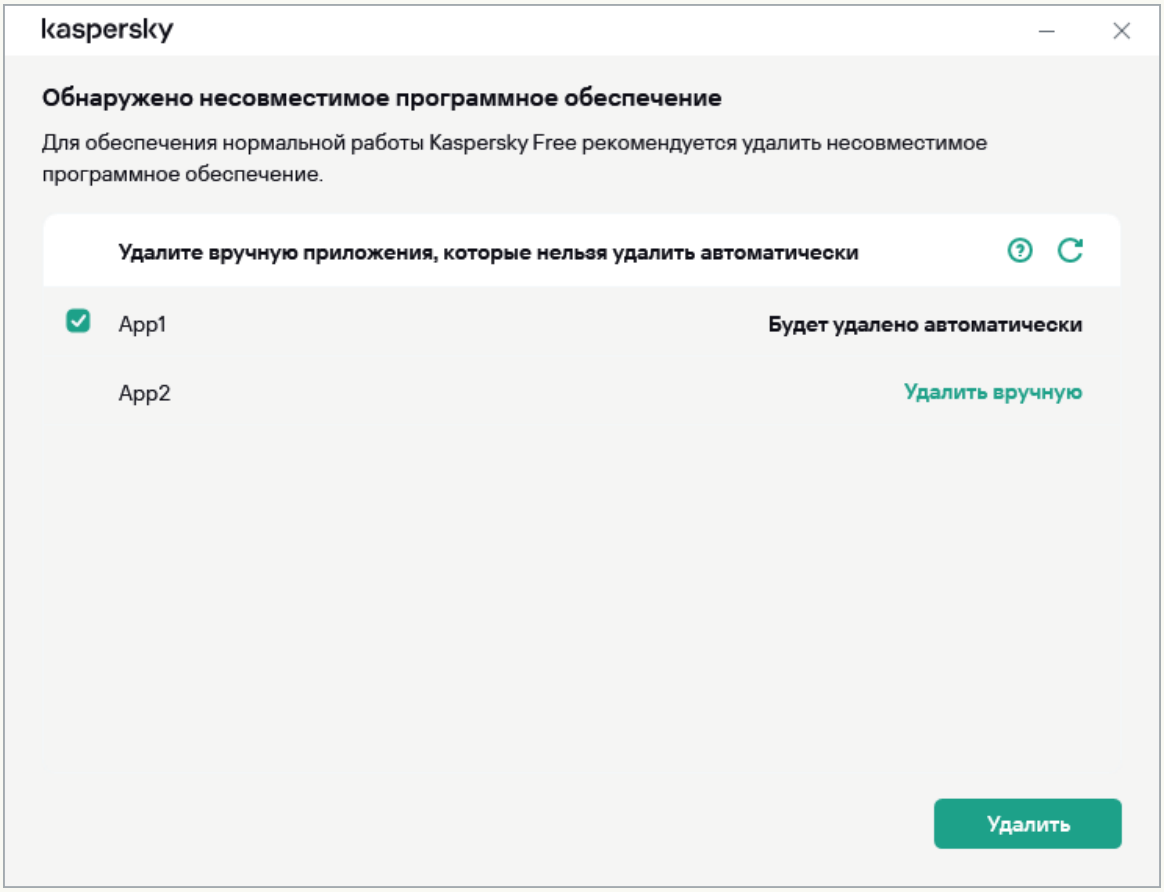
Во время установки приложение производит ряд проверок. В результате этих проверок могут быть обнаружены следующие проблемы:

- *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**.



Окно удаления несовместимых приложений

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

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.

Для дальнейшей работы с приложением вам потребуется подключиться к My Kaspersky и завершить активацию.

Как активировать приложение

Активация приложения осуществляется путем входа в аккаунт My Kaspersky с того устройства, на которое вы устанавливаете приложение. Kaspersky Free не работает, если ваше устройство не подключено к аккаунту. Вы можете создать его в окне подключения к аккаунту в процессе активации приложения или на сайте My Kaspersky. Вы также можете использовать для входа в аккаунт учетные данные других ресурсов "Лаборатории Касперского".

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.

Приложение автоматически подключается к My Kaspersky, если вы скачали приложение из вашего аккаунта или ранее вводили свои учетные данные в другом приложении "Лаборатории Касперского" на данном устройстве.

Для активации приложения необходимо подключение к интернету.

Чтобы активировать приложение:

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.

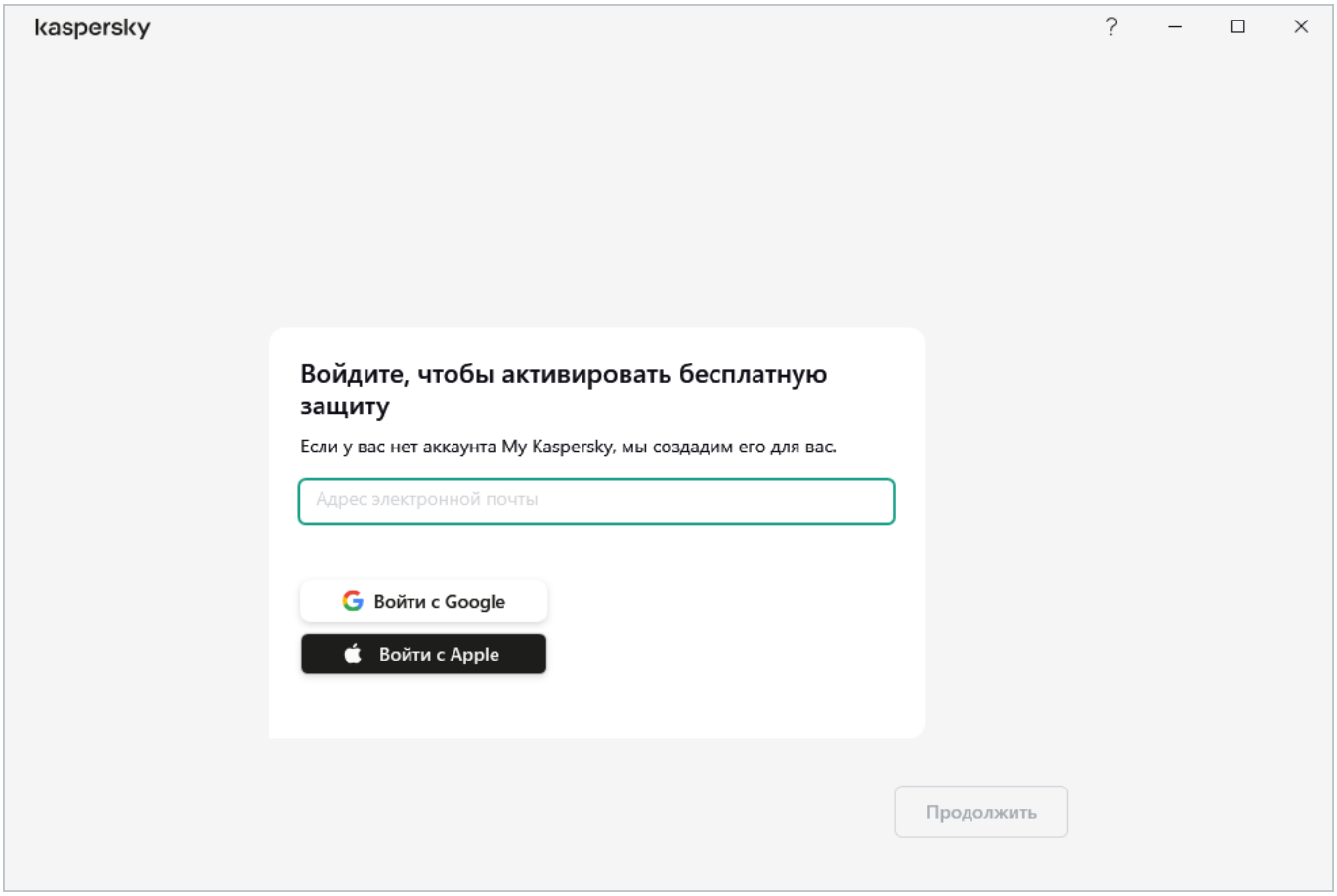
  Обработка данных при входе в аккаунт

  > 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**.

Окно входа в аккаунт My Kaspersky



*Facebook принадлежит компании META Inc, признанной экстремистской организацией на территории Российской Федерации.

Расширение Kaspersky Protection для браузеров

Для полноценной поддержки браузеров приложением Kaspersky Free в браузерах должно быть установлено и включено расширение Kaspersky Protection. Kaspersky Free с помощью расширения Kaspersky Protection внедряет в трафик скрипт. Приложение использует этот скрипт для взаимодействия с веб-страницей. 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:

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

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

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

1. Откройте главное окно приложения и выполните одно из следующих действий:

   - В главном окне найдите рекомендацию установить расширение для браузера и нажмите на кнопку **Включить**.
   - Выберите раздел **Безопасность**.

     a. В разделе **Безопасность** выберите блок **Расширение Kaspersky Protection**.

     b. В блоке **Расширение Kaspersky Protection** выберите необходимый браузер и по ссылке **Включить** перейдите в окно установки расширения.

2. Выполните стандартную процедуру установки расширения в вашем браузере (смотрите справку вашего браузера).

3. После установки включите расширение одним из следующих способов:

   - Нажмите на кнопку **Включить** в блоке **Расширение Kaspersky Protection** для выбранного браузера.

- Стандартными способом для вашего браузера (смотрите справку вашего браузера).

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

Поддержка Яндекс.Браузера

При использовании Яндекс.Браузера работают следующие компоненты приложения:

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

Поддержка Internet Explorer

Начиная с версии Kaspersky Free 2021, 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 Free** → **Удалить Kaspersky Free**.

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

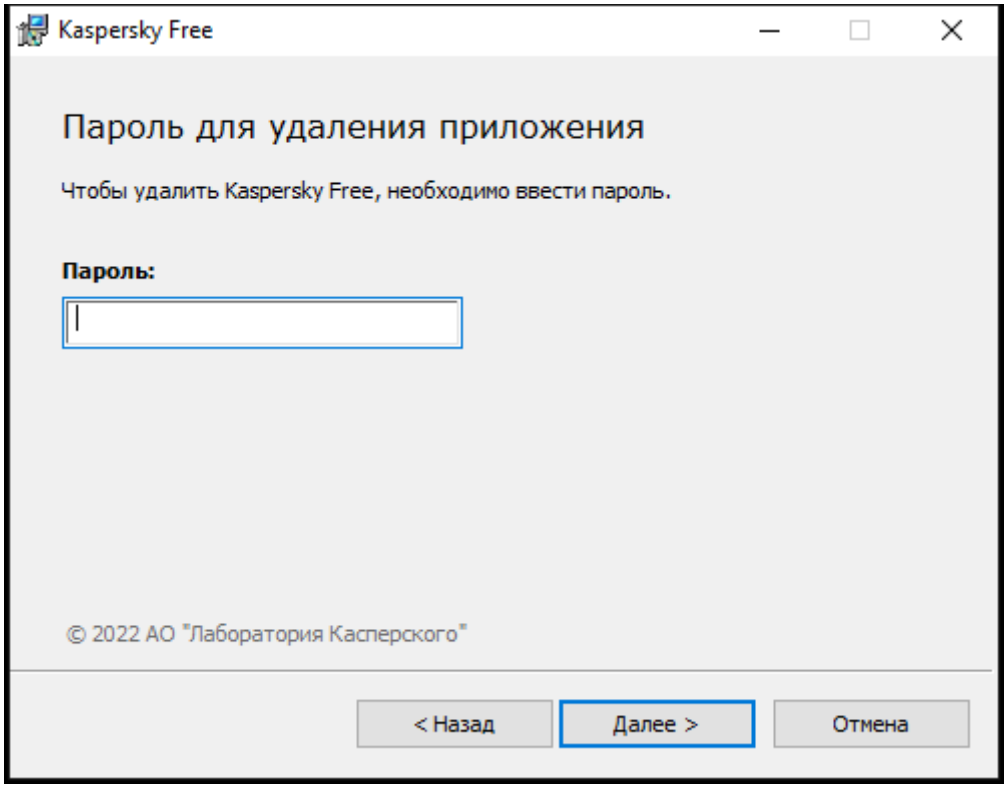
Чтобы запустить мастер в операционной системе Microsoft Windows 8 и выше:

1. Найдите установленное приложение одним из следующих способов:
   - В Windows 8 нажмите на кнопку **Пуск** и найдите приложение Kaspersky Free 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 Free.
3. В контекстном меню выберите пункт **Удалить**.
4. В открывшемся окне выберите в списке Kaspersky Free.
5. Нажмите на кнопку **Удалить** / **Изменить** в верхней части списка.

Будет запущен мастер установки и удаления приложения.

В процессе удаления необходимо выполнить следующие шаги:

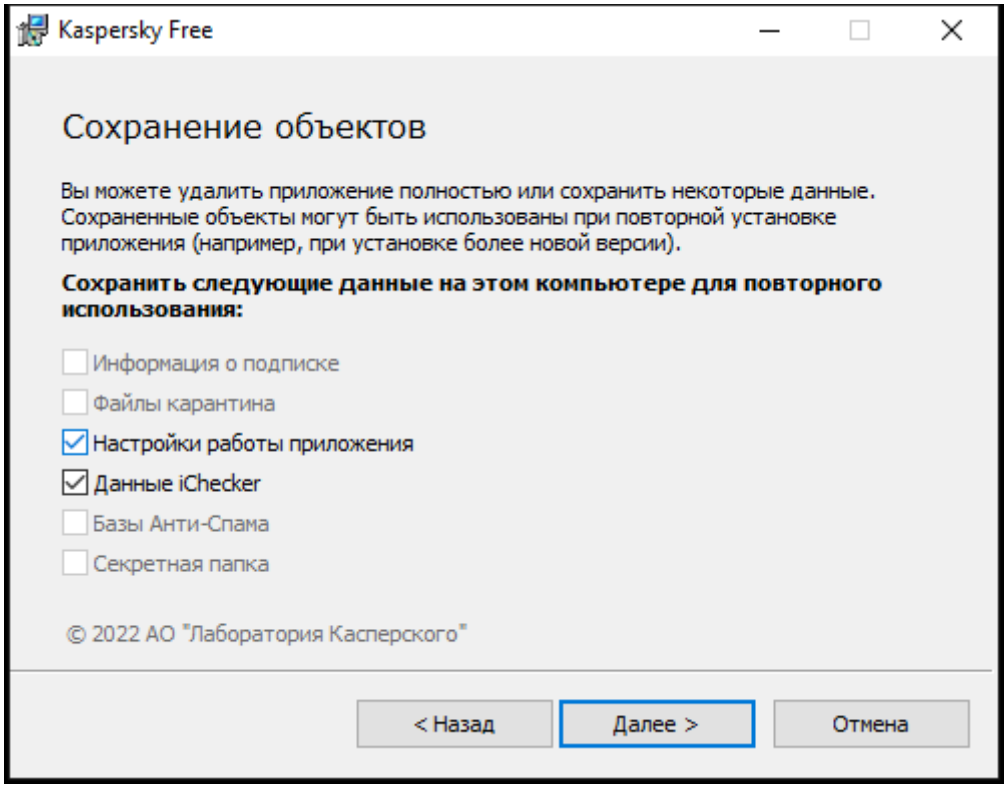
1. Чтобы удалить приложение, требуется ввести пароль для доступа к настройкам приложения. Если вы по каким-либо причинам не можете указать пароль, удаление приложения будет невозможно.



Окно ввода пароля

1. 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).



Окно сохранения настроек

Вы можете сохранить следующие данные:

- **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 Free.

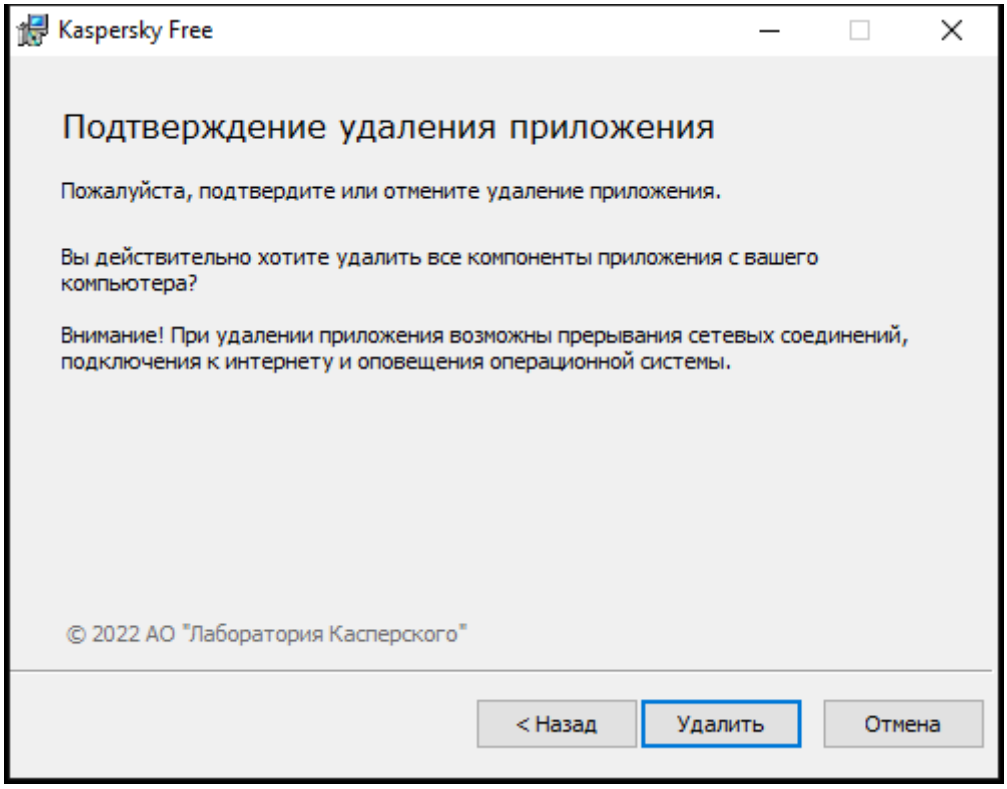
- **Настройки работы приложения** – параметры работы приложения, установленные во время его настройки.

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.

2. 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**.



Окно подтверждения удаления приложения

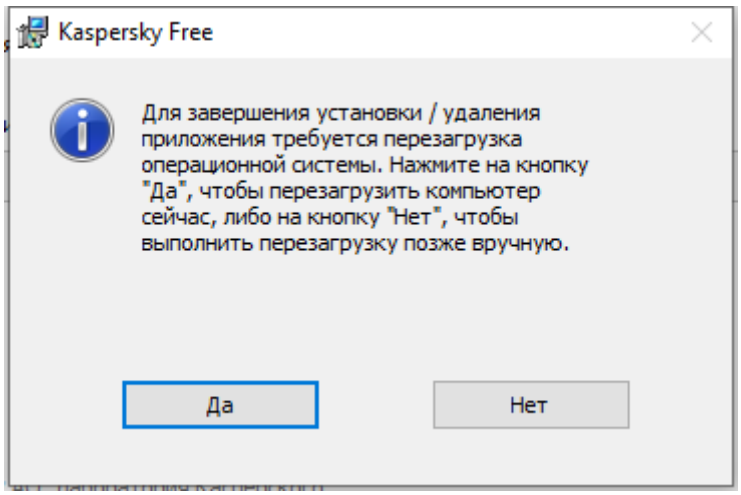
3. Завершение удаления

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.

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



Окно завершения удаления

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.

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

Ограничения при обновлении предыдущей версии приложения

Обновление приложения Kaspersky Free имеет следующие ограничения:

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

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

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

Для чего нужен аккаунт My Kaspersky

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

Чтобы иметь доступ к возможностям My Kaspersky, нужен аккаунт.

На My Kaspersky вы можете:

- просматривать информацию о подписках и сроках их действия;
- безопасно хранить и синхронизировать пароли и другую личную информацию, если вы используете Kaspersky Password Manager;
- скачивать приобретенные приложения;
- узнавать о новых приложениях и специальных предложениях "Лаборатории Касперского".

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

Как защитить другое устройство

Вы можете поделиться бесплатной защитой с другим вашим устройством на операционной системе Windows, Android, iOS или macOS.

Вы всегда можете посмотреть, сколько устройств вы уже защитили, а сколько вам еще доступно, в разделе **Профиль** в приложении, а также в вашем аккаунте My Kaspersky . Там же вы найдете удобные инструменты для того, чтобы поделиться защитой с другим устройством.

Чтобы поделиться защитой из приложения, выполните следующие шаги:

1. Откройте главное окно приложения.

2. Перейдите в раздел **Профиль**.

3. Нажмите на кнопку +. В некоторых подписках кнопка называется **Защитить устройство**.

4. В окне **Защитите больше устройств** выберите один из следующих вариантов:

   - **Отсканировать QR-код**

     На закладке **QR-код** наведите камеру смартфона на QR-код.

     На вашем мобильном устройстве откроется магазин Google Play, App Store или Huawei AppGallery на странице загрузки приложения. После того как вы загрузите и установите приложение, оно 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.

   - **Отправить ссылку по email**

     a. Перейдите на закладку **По email**.

     b. Перейдите по ссылке.

     В браузере по умолчанию откроется ваш аккаунт My Kaspersky.

     c. В окне **Отправка по эл. почте** введите адрес электронной почты в поле ввода и нажмите **Отправить**.

     d. Скачайте приложение по ссылке из письма.

     После скачивания и установки приложение автоматически подключится к вашему аккаунту My Kaspersky.

> В некоторых подписках доступна только информация об общем количестве устройств, которые вы можете защитить.

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

Переход с Kaspersky Free на другую подписку

Kaspersky Free позволяет перейти на платный план подписки без дополнительного скачивания и установки программного обеспечения.

Вы можете временно перейти на пробную подписку Kaspersky Standard или Kaspersky Plus, чтобы узнать о преимуществах платной подписки, или купить подписку и перейти к постоянному использованию приложения по платной подписке.

Переход к использованию Kaspersky Standard

Kaspersky Standard – это план подписки, предназначенный для комплексной защиты вашего компьютера.

По сравнению с Kaspersky Free план подписки Kaspersky Standard обладает рядом дополнительных возможностей, которые реализуются с помощью следующих компонентов и функций:

- Предотвращение вторжений.
- Сетевой экран.
- Безопасные платежи.
- Менеджер приложений.
- Мониторинг сети.
- Защита веб-камеры.
- Защита от сбора данных в интернете.
- Анти-Спам.
- Анти-Баннер.

Переход к использованию Kaspersky Plus

С Kaspersky Plus вы сможете усилить защиту приватности и улучшить производительность компьютера. Этот план подписки предоставляет те же возможности, что и Kaspersky Standard, а также ряд дополнительных функций:

- Поиск утечки данных (проверка любого количества аккаунтов).
- Безопасность вашей сети Wi-Fi.
- Резервное копирование.
- Секретная папка.

Как перейти на пробную подписку

Вы можете временно перейти на бесплатную пробную подписку Kaspersky Standard или Kaspersky Plus, чтобы оценить их возможности. Когда срок действия пробной подписки истечет, вы автоматически вернетесь к использованию Kaspersky Free. Чтобы продолжить пользоваться расширенным функционалом приложения, вам нужно купить подписку на Kaspersky Standard или Kaspersky Plus.

Пробный период недоступен, если вы уже использовали пробную подписку на устройстве.

Чтобы оформить пробную подписку:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Профиль**.
3. В блоке с информацией о подписке нажмите на кнопку **Расширить защиту**.
4. На странице расширения защиты нажмите на кнопку **Попробовать бесплатно**.

   Если приложение не подключено к аккаунту My Kaspersky, вам потребуется войти в аккаунт. Если у вас нет аккаунта, вы можете создать его в окне подключения. На территории Европейского союза вам обязательно потребуется принять Положение об обработке данных для использования Веб-Портала или Положение об обработке данных для использования Веб-Портала и контроля лицензионных ограничений.

5. Запустится мастер миграции.

   При переходе на Kaspersky Standard или Kaspersky Plus на территории Европейского союза приложение предложит вам посмотреть и принять Лицензионное соглашение, Положение о Kaspersky Security Network и Положение об обработке данных в маркетинговых целях. Вам также может потребоваться принять Положение об обработке данных для использования Веб-Портала или Положение об обработке данных для использования Веб-Портала и контроля лицензионных ограничений.

   Настройка и запуск приложения могут занять некоторое время. По завершении процесса приложение автоматически активируется по пробной подписке.

   В процессе активации вам может быть предложено установить дополнительные приложения, входящие в состав подписки.

6. Нажмите на кнопку **Закрыть** для завершения работы мастера и **Начать**, чтобы начать пользоваться приложением по пробной подписке.

Как перейти на платную подписку

Вы можете купить подписку Kaspersky Standard или Kaspersky Plus из интерфейса приложения.

Чтобы купить подписку:

1. Откройте главное окно приложения.
2. Перейдите в раздел **Профиль**.
3. В блоке с информацией о подписке нажмите на кнопку **Расширить защиту**.
4. На странице расширения защиты нажмите на кнопку **Купить сейчас**.

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

   После успешной покупки подписка добавится в ваш аккаунт My Kaspersky.

   > Если приложение не подключено к аккаунту My Kaspersky, вам потребуется войти в аккаунт. На территории Европейского союза вам также обязательно потребуется принять Положение об обработке данных для использования Веб-Портала или Положение об обработке данных для использования Веб-Портала и контроля лицензионных ограничений.

5. Запустится мастер миграции. Для продолжения работы мастера нажмите на кнопку **Продолжить**.

   > При переходе на Kaspersky Standard или Kaspersky Plus на территории Европейского союза приложение предложит вам посмотреть и принять Лицензионное соглашение, Положение о Kaspersky Security Network и Положение об обработке данных в маркетинговых целях. Вам также может потребоваться принять Положение об обработке данных для использования Веб-Портала или Положение об обработке данных для использования Веб-Портала и контроля лицензионных ограничений.

   Настройка и запуск приложения могут занять некоторое время. По завершении процесса приложение автоматически активируется по новой подписке.

   В процессе активации вам может быть предложено установить дополнительные приложения, входящие в состав подписки.

6. Нажмите на кнопку **Закрыть** для завершения работы мастера и **Начать**, чтобы начать пользоваться приложением по новой подписке.

Как настроить интерфейс приложения

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

Как настроить уведомления приложения

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

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

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

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

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

Уведомление может быть закрыто автоматически при перезагрузке компьютера, закрытии Kaspersky Free или в режиме Connected Standby в Windows 8. При автоматическом закрытии уведомления Kaspersky Free 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.

   В правой части окна отобразится список событий, которые могут произойти во время работы этого компонента.

6. Выберите в списке событие и установите флажки:

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

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

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

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

Как настроить получение 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 одно из следующих действий:

   - Установите флажок **Получать информационные и рекламные сообщения "Лаборатории Касперского"**, если вы хотите получать уведомления о новостях компьютерной безопасности.
   - Установите флажок **Отображать информацию о специальных предложениях на сайтах**, если вы хотите получать наиболее выгодные предложения при посещении сайтов "Лаборатории Касперского".
   - Установите флажок **Получать информационные и рекламные сообщения после истечения 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 Free, 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 Free, когда компьютером пользуется ребенок.

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

Подробнее о том, как настроить работу приложения Kaspersky Free, 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.
   - **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 программе** 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 Free в области уведомлений в зависимости от статуса приложения:

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

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

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

Как защитить доступ к управлению приложением с помощью пароля

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

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

Чтобы создать пароль администратора `KLAdmin`:

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

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

   Рекомендации по созданию надежного пароля:

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

Забытый пароль восстановить нельзя. Если пароль забыт, для восстановления доступа к настройкам Kaspersky Free вы можете воспользоваться рекомендациями из статьи на сайте Службы технической поддержки.

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

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

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

Как добавить пользователя или группу пользователей

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

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

2. По ссылке **Выбрать пользователя или группу** 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 **Настройки интерфейса** в блоке **Отображать состояние приложения в области уведомлений** выберите пользователя или группу пользователей в списке и нажмите на кнопку **Изменить**.

Как разрешить какое-либо действие отдельному пользователю или группе пользователей

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

Как запретить какое-либо действие отдельному пользователю или группе пользователей

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

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

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

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 Free, чтобы вы оставались на шаг впереди современных угроз. Посмотрите, какие инструменты защиты входят в него.

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.

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 Free не создает резервные копии. Для восстановления таких объектов необходимо использовать средства восстановления операционной системы (подробную информацию можно получить из документации к операционной системе, установленной на вашем компьютере) либо обновить приложения через Магазин Windows.

Чтобы восстановить удаленный или вылеченный файл:

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

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

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 Free 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.

О проверке файлов в облачном хранилище OneDrive

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

Следующие компоненты не проверяют файлы в облачном хранилище OneDrive:

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

Отчет о работе Kaspersky Free 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.

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

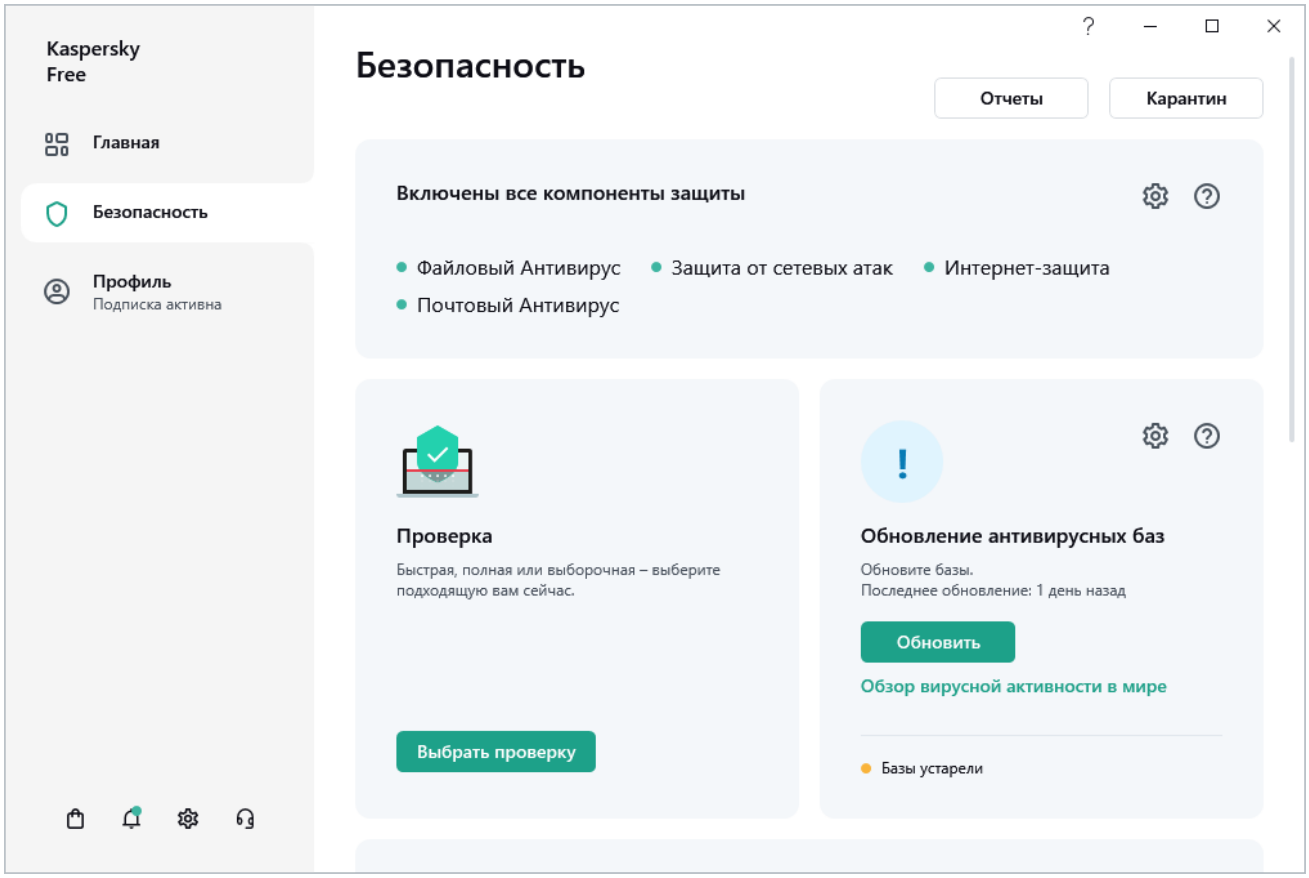
При получении пакета исправлений (патча) приложение устанавливает его автоматически. Для завершения установки пакета исправлений требуется перезагрузить компьютер. До перезагрузки компьютера значок приложения в области уведомлений имеет красный цвет, а в окне **Центр уведомлений** приложения отображается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

Как запустить обновление баз и модулей приложения

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

Чтобы запустить обновление баз и модулей приложения:

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



Обновление антивирусных баз

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 .

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 операционной системы, оно предложит вам исправить их таким образом, чтобы восстановить безопасность операционной системы. Подробную информацию по каждой небезопасной настройке вы можете получить по ссылке напротив этой настройки в окне приложения.

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.

Проверка почтовых сообщений

Kaspersky Free 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.

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

Если во время проверки приложение Kaspersky Free 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.

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 Free, 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 Free 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 **Настройки безопасности → Настройки приватности → Защита ввода данных**.

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

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

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

О защите с помощью Antimalware Scan Interface

Antimalware Scan Interface (AMSI) позволяет стороннему приложению с поддержкой AMSI отправлять объекты в приложение Kaspersky Free 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 Free может отклонить запрос от стороннего приложения, например, если это приложение превысило максимальное количество запросов за промежуток времени. В этом случае приложение Kaspersky Free показывает уведомление о том, что запрос был отклонен. При получении такого уведомления вам не требуется выполнять никаких действий.

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

Как 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.

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)**.

Игровой режим

При одновременной работе приложения Kaspersky Free 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 Free отвлекают от игры.

Чтобы не изменять настройки приложения Kaspersky Free 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 Free 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**.

Пока включен Игровой режим, также не будут показаны уведомления приложений Kaspersky Secure Connection и Kaspersky Password Manager, установленных на этом же устройстве.

Защита персональных данных в интернете

Этот раздел содержит информацию о том, как сделать работу в интернете безопасной и защитить ваши данные от кражи.

О защите персональных данных в интернете

С помощью Kaspersky Free вы можете защитить от кражи свои персональные данные:

- пароли, имена пользователя и другие регистрационные данные;
- номера счетов и банковских карт.

В состав Kaspersky Free входят компоненты и инструменты, позволяющие защитить ваши персональные данные от кражи злоумышленниками, использующими такие методы как фишинг и перехват данных, вводимых с клавиатуры.

Для защиты от фишинга предназначен Анти-Фишинг, включенный в состав компонентов Интернет защита. Включите эти компоненты, чтобы обеспечить максимально эффективную защиту от фишинга.

Для защиты от перехвата данных, введенных с клавиатуры, предназначена Экранная клавиатура.

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 Free 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 Free 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 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.

Проверка безопасности сайта

Kaspersky Free 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 Free отображает один из следующих значков:

– если веб-страница, которая открывается по ссылке, безопасна по данным "Лаборатории Касперского";

– если нет информации о безопасности веб-страницы, которая открывается по ссылке;

– если веб-страница, которая открывается по ссылке, по данным "Лаборатории Касперского" может быть использована злоумышленниками для нанесения вреда компьютеру или вашим данным;

– если веб-страница, которая открывается по ссылке, по данным "Лаборатории Касперского" может быть заражена или взломана;

– если веб-страница, которая открывается по ссылке, опасна по данным "Лаборатории Касперского".

При наведении курсора мыши на значок отображается всплывающее окно с более подробным описанием ссылки.

По умолчанию Kaspersky Free проверяет ссылки только в результатах поиска.

Как изменить настройки защищенных соединений

Защищенные соединения – это соединения, которые устанавливаются по протоколам SSL и TLS. По умолчанию приложение Kaspersky Free выполняет проверку таких соединений по запросу компонента Проверка ссылок.

Чтобы изменить настройки защищенных соединений, 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 безопасности**.
4. В блоке **Расширенные настройки** нажмите на кнопку **Настройки сети**.
5. В окне **Настройки сети** перейдите в раздел **Проверка защищенных соединений**.
6. Выберите вариант действия при подключении к сайтам по защищенному соединению:

- **Не проверять защищенные соединения**. Kaspersky Free не проверяет защищенные соединения.

- **Проверять защищенные соединения по запросу компонентов защиты**. Kaspersky Free проверяет защищенные соединения, только если на это будет запрос от компонента Проверка ссылок. Этот вариант действия выбран по умолчанию.

- **Всегда проверять защищенные соединения**. Kaspersky Free 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 Free. 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.

1. Выберите вариант действия, если возникают ошибки при проверке защищенных соединений:

   - **Игнорировать**. Если выбран этот вариант, Kaspersky Free разрывает соединение с сайтом, на котором возникла ошибка проверки защищенного соединения.

   - **Спрашивать**. Если выбран этот вариант, при возникновении ошибки проверки защищенного соединения с сайтом, Kaspersky Free показывает уведомление, в котором вы можете выбрать вариант действия:

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

     - **Добавить домен в исключения**. Если выбран этот вариант, Kaspersky Free добавляет адрес сайта в список доверенных адресов. Kaspersky Free 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, Kaspersky Free добавляет сайт в список доверенных адресов. Kaspersky Free не проверяет защищенные соединения на сайтах, входящих в список доверенных адресов. Такие сайты

отображаются в окне **Доверенные адреса**, которое можно открыть по ссылке **Доверенные адреса**.

2. 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**.

   Нажмите на кнопку **Добавить**. Приложение не будет проверять защищенное соединение с этим сайтом. Обратите внимание, что добавление сайта в список исключений означает, что функциональность проверки этого сайта компонентом Проверка ссылок будет ограничена.

Как получить доступ к файлам, хранящимся в секретной папке

Чтобы получить доступ к файлам, хранящимся в секретной папке:

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

   Откроется окно **Настройка**.
3. В разделе **Настройки приватности** выберите **Секретная папка**.
4. В блоке **Секретная папка** нажмите на кнопку **У меня уже есть секретная папка**.

   Откроется окно **Секретная папка**.
5. Нажмите на кнопку **Открыть** рядом с секретной папкой.
6. Введите пароль и нажмите на кнопку **Открыть в Проводнике**.

Файлы, сохраненные в секретной папке, отобразятся в окне Проводника.

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 **Информационные материалы** выполните одно из следующих действий:

   - Если вы хотите получать новости безопасности, установите флажок **Получать информационные и рекламные сообщения "Лаборатории Касперского"**.
   - Если вы не хотите получать новости безопасности, снимите флажок **Получать информационные и рекламные сообщения "Лаборатории Касперского"**.

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**.

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 плане подписки Kaspersky Free позволяет вам вручную проверить только аккаунт My Kaspersky. Автоматическая проверка аккаунта My Kaspersky и других учетных записей доступна только в плане Kaspersky Plus.

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

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

При проверке учетных записей "Лаборатория Касперского" не получает данные в открытом виде, использует их только для указанной проверки и не хранит их. При обнаружении утечки Kaspersky Free не получает доступа к самим пользовательским данным и предоставляет информацию только о категориях данных, которые могли попасть в публичный доступ.

Kaspersky Free может уведомить вас о возможной утечке следующих категорий данных:

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

По умолчанию Kaspersky Free 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. 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 Kaspersky Free на разных устройствах не синхронизируются. Проверка добавленных учетных записей выполняется раз в сутки.

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

Kaspersky Free периодически проверяет адрес электронной почты, привязанный к вашему аккаунту My Kaspersky. Первая такая проверка осуществляется через двое суток после установки приложения Kaspersky Free. Далее проверка производится каждые 24 часа.

Поиск утечки данных для аккаунта My Kaspersky не работает, если Kaspersky Free 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 Kaspersky Free.
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 Kaspersky Free.
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**.

Kaspersky Free начнет проверку указанного адреса. 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 Kaspersky Free, вы можете проверить на предмет возможной утечки данных не только свои, но и другие учетные записи, например, учетные записи ваших близких и друзей.

Как удалить несовместимые приложения

Приложение Kaspersky Free 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 Free не сможет защитить ваш компьютер в полной мере.

Причины несовместимости стороннего приложения с приложением Kaspersky Free 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 **Обнаружено несовместимое программное обеспечение** со списком найденных несовместимых приложений.

4. Оставьте флажки напротив названий несовместимых приложений, которые нужно удалить, и нажмите **Удалить**. Удаление выполняется с помощью средств удаления, предоставляемых этими приложениями. В процессе удаления от вас может потребоваться согласие на удаление или изменение настроек, связанных с удалением приложений.

5. Если на компьютере остались несовместимые приложения, которые невозможно удалить автоматически, откроется окно со списком таких приложений. Чтобы удалить несовместимые приложения вручную, нажмите **Удалить вручную**. Откроется стандартное окно операционной системы со списком установленных приложений. Удалите несовместимые приложения в соответствии с инструкциями для вашей операционной системы.

6. После удаления несовместимых приложений перезагрузите компьютер.

Как приостановить и возобновить защиту компьютера

Приостановка защиты означает выключение на некоторое время всех ее компонентов.

Чтобы приостановить защиту компьютера:

1. В контекстном меню значка Kaspersky Free 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 Free в области уведомлений панели задач.

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 просмотреть отчет о работе приложения

Приложение ведет отчеты о работе каждого компонента защиты. С помощью отчета вы можете получить статистическую информацию о работе приложения (например, узнать, сколько обнаружено и обезврежено вредоносных объектов за определенный период, сколько раз за это время обновлялись базы и модули приложения и многое другое).

Чтобы просмотреть отчет о работе приложения:

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

3. Нажмите на кнопку **Отчеты** в верхней части окна.

   В окне **Отчеты** данные представлены в табличном виде. Для удобства просмотра отчетов вы можете выбирать различные варианты фильтрации записей.

Как применить настройки приложения на другом компьютере

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

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

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

1. Сохранение настроек приложения Kaspersky Free 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 Free, установленное на другом компьютере.

Как экспортировать настройки

Чтобы экспортировать настройки Kaspersky Free:

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 Free 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 Free только для текущего пользователя. При импортировании настроек на другом компьютере адреса сайтов не сохраняются.

Как импортировать настройки

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

1. Откройте главное окно приложения Kaspersky Free, 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 Free, установленное на другом компьютере.

Участие в Kaspersky Security Network

Чтобы повысить эффективность защиты вашего компьютера, приложение Kaspersky Free 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 Free 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 Free.

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 Free 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 Free вместо информации о Kaspersky Security Network в окне **Kaspersky Security Network** отображается **Положении о Kaspersky Security Network**.

Чтобы принять Положение о Kaspersky Security Network:

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

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

2. Если вы принимаете условия положения, нажмите на кнопку **Принять**.

Чтобы отказаться от Положения о Kaspersky Security Network,

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

Как проверить подключение к Kaspersky Security Network

Подключение к Kaspersky Security Network может отсутствовать по следующим причинам:

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

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

Чтобы проверить подключение к Kaspersky Security Network:

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

Откроется окно **Настройка**.

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

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

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

Ограничения и предупреждения

Kaspersky Free имеет ряд некритичных для работы приложения ограничений.

Ограничения работы некоторых компонентов и обработки файлов в автоматическом режиме

Обработка зараженных файлов 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.

Особенности обработки файлов в интерактивном режиме защиты

Если зараженный файл является частью приложения из Магазина Windows, в интерактивном режиме защиты приложение показывает уведомление с предложением удалить такой файл. Действие Лечить недоступно.

Ограничения функциональности Мониторинга активности

Функциональность противодействия приложениям-шифровальщикам (шифрование файлов пользователя вредоносным приложением) имеет следующие ограничения:

- Для обеспечения функциональности используется системная папка Temp. Если на системном диске, на котором расположена папка Temp, недостаточно свободного места для создания временных файлов, защита от приложений-шифровальщиков не

предоставляется. При этом уведомление о невыполнении копирования (непредоставлении защиты) не выводится.

- Временные файлы удаляются автоматически при завершении работы Kaspersky Free или отключении компонента Мониторинг активности.

- В случае нештатного завершения работы Kaspersky Free временные файлы автоматически не удаляются. Чтобы удалить временные файлы, необходимо вручную очистить папку Temp. Для этого откройте окно **Выполнить** и в поле **Открыть** введите `%TEMP%`. Нажмите на кнопку **OK**.

- Защита от приложений-шифровальщиков выполняется только для файлов, расположенных на носителях информации, отформатированных в файловой системе NTFS.

- Количество подлежащих восстановлению файлов не должно превышать 50 на один процесс шифрования.

- Суммарный объем изменений в файлах не должен превышать 100 МБ. Файлы, изменения в которых превышают этот лимит, не подлежат восстановлению.

- Не контролируются изменения файлов, инициированные через сетевой интерфейс.

- Не поддерживаются файлы, зашифрованные системой EFS.

- Для включения защиты от приложений-шифровальщиков после установки Kaspersky Free требуется перезагрузить компьютер.

Ограничения проверки файлов и сертификатов сайтов

При проверке файла приложение может обращаться за информацией об этом файле в Kaspersky Security Network. Если данные из Kaspersky Security Network получить не удалось, приложение принимает решение о том, является ли этот файл зараженным, на основании локальных антивирусных баз.

Ограничения функциональности проверки защищенных соединений

В связи с техническими ограничениями реализации алгоритмов проверки проверка защищенных соединений не поддерживает некоторые расширения протокола TLS 1.0 и выше (в частности NPN и ALPN). Подключение по этим протоколам может быть ограничено. Браузеры с поддержкой протокола SPDY используют вместо SPDY протокол HTTP поверх TLS, даже если сервер, к которому выполняется подключение, поддерживает SPDY. При этом уровень защиты соединения не снижается. Если сервер поддерживает только протокол SPDY и возможность установить соединение с помощью протокола HTTPS отсутствует, приложение не будет контролировать установленное соединение.

Также приложение не обрабатывает трафик, передаваемый через расширения протокола HTTP/2.

Приложение Kaspersky Free 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 Free 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;
- Проверка ссылок.

Kaspersky Free не контролирует трафик, если браузер загружает веб-страницу или ее элементы из локального кеша, а не из интернета.

Ограничения проверки защищенных соединений клиента the Bat

Так как почтовый клиент The Bat использует собственное хранилище сертификатов, Kaspersky Free 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, компонент Проверка ссылок может продолжать проверять защищенные соединения. Компонент Интернет-защита не проверяет сайты, добавленные в исключения.

Особенности обработки зараженных файлов компонентами приложения

Kaspersky Free по умолчанию может удалять зараженные файлы, если их лечение невозможно. Удаление по умолчанию может выполняться при обработке файлов такими компонентами, как Почтовый Антивирус, Файловый Антивирус, при выполнении задач проверки.

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** (**Запуск программы** в Windows XP), в поле **Открыть** ввести %TEMP% и нажать на кнопку **ОК**.

В файлы трассировки сохраняются пути к файлам установки, загруженным в ходе использования autorun. Данные хранятся в течение работы процесса autorun и безвозвратно удаляются при завершении этого процесса. Данные никуда не отправляются.

Ограничения работы Kaspersky Free при включенном режиме Device Guard на Microsoft Windows 10 RS4

Частично ограничена работа следующей функциональности:

- защита буфера обмена;
- защита браузера от приложений эмуляции ввода с клавиатуры и мыши (подмен вводимых данных);
- защита от приложений удаленного управления;
- защита браузера (управление через API, защита от атак при помощи опасных сообщений окнам браузера, защита от управления очередью сообщений);
- эвристический анализ (эмуляция запуска вредоносных приложений).

Если в операционной системе Windows включен режим работы UMCI, Kaspersky Free 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 Free может классифицировать такое приложение как вредоносное. Чтобы избежать этого, вы можете исключить приложение из проверки, настроив приложение Kaspersky Free 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 Поддержку пользователей. 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.

Ограничение первого запуска приложения после обновления операционной системы Microsoft Windows 7 до Microsoft Windows 10

Если вы обновили операционную систему Microsoft Windows 7 до Microsoft Windows 8 / 8.1 или Microsoft Windows 10 / RS1 / RS2 / RS3, при первом запуске Kaspersky Free работает со следующими ограничениями:

- Работает только Файловый Антивирус (постоянная защита). Остальные компоненты приложения не работают.
- Работает самозащита файлов и системного реестра. Самозащита процессов не работает.
- Интерфейс приложения недоступен до перезагрузки компьютера. Приложение показывает уведомление о том, что некоторые компоненты приложения не работают, и о том, что требуется перезагрузка компьютера после завершения адаптации к новой операционной системе.
- В контекстном меню значка в области уведомлений доступен только пункт **Выход**.
- Приложение не показывает уведомления и автоматически выбирает рекомендованное действие.

Предупреждение об ошибке адаптации драйверов приложения при обновлении операционной системы с Windows 7 до Windows 10

При обновлении Windows с версии 7 до версии 10 может произойти ошибка адаптации драйверов Kaspersky Free. 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:

- функцией обнаружения угроз во время загрузки операционной системы;
- функцией защиты процессов приложения с помощью технологии Protected Process Light (PPL) от Microsoft.

Вы можете воспользоваться следующими способами исправления ошибки:

- перезагрузить компьютер и повторить адаптацию приложения из оповещения в Центре уведомлений;
- удалить и заново установить приложение.

Ограничения проверки трафика, передаваемого по протоколу HTTPS, в браузере Mozilla Firefox

В версиях Mozilla Firefox 58.x и выше приложение не проверяет трафик, передаваемый по протоколу HTTPS, если изменение настроек браузера защищено Основным паролем. При обнаружении Основного пароля в браузере, приложение показывает уведомление, в котором содержится ссылка на статью в Базе знаний. Статья содержит инструкцию для решения этой проблемы.

Если трафик, передаваемый по протоколу HTTPS, не контролируется, ограничена работа следующих компонентов:

- Интернет-защита;
- Анти-Фишинг;
- Защита ввода данных.

Ограничения работы расширения Kaspersky Protection в браузерах Google Chrome и Mozilla Firefox

Расширение Kaspersky Protection не работает в браузерах Google Chrome и Mozilla Firefox, если на вашем компьютере установлено приложение Malwarebytes for Windows.

Особенности установки приложения на операционной системе Microsoft Windows 7 Service Pack 0 и Service Pack 1

При установке приложения на операционные системы, которые не поддерживают сертификаты с цифровой подписью SHA256, приложение устанавливает свой доверенный сертификат.

Об автоматическом тестировании функциональности приложений "Лаборатории Касперского"

В приложениях "Лаборатории Касперского", включая Kaspersky Free, 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 Free в Базе знаний

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

На странице приложения Kaspersky Free 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 Free, 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.

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.

Сетевые параметры для взаимодействия с внешними службами

Приложение Kaspersky Free использует следующие сетевые параметры для взаимодействия с внешними службами.

Сетевые параметры

Адрес	Описан
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Протокол: `HTTPS` Порт: `443`	Активация прило

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`s08.upd.kaspersky.com`
`s09.upd.kaspersky.com`
`s10.upd.kaspersky.com`
`s11.upd.kaspersky.com`
`s12.upd.kaspersky.com`
`s13.upd.kaspersky.com`
`s14.upd.kaspersky.com`
`s15.upd.kaspersky.com`
`s16.upd.kaspersky.com`
	Обновление баз и приложения.

`s17.upd.kaspersky.com`

`s18.upd.kaspersky.com`

`s19.upd.kaspersky.com`

`cm.k.kaspersky-labs.com`

Протокол: `HTTPS`

Порт: `443`

`downloads.upd.kaspersky.com`

Протокол: `HTTPS`

Порт: `443`

- Обновление б
модулей прил

- Проверка дос
серверам "Ла
Касперского"
доступа к сер
через систем
приложение б
использовать
DNS. Это нуж
обновления
антивирусных
поддержки ур
безопасности
компьютера. В
Kaspersky Fre
использовать
публичные DN
порядке их об

1. Google Pu
(8.8.8.8).

2. Cloudflar

3. Alibaba C
(223.6.6.6)

4. Quad9 DN

5. CleanBro
(185.228.16

Запросы
приложения
содержать а
доменов и в
IP-адрес
пользовател
приложение
устанавлива
DNS-сервер
TCP/UDP-
соединение
данные нуж
например, д
проверки
сертификат
ресурса при
обращении
HTTPS. Если
приложение
Kaspersky Fr
использует
публичный D
сервер, пра
обработки д
регламенти
Политикой
конфиденци
этого серви
требуется з
приложени
Kaspersky Fr
использова
публичный D
сервер, обр
в Службу
технической
поддержки
приватным

`touch.kaspersky.com`

Протокол: `HTTP`

- Получение дс
времени для
срока действ

	сертификата соединение). • Предупрежде запрете дост ресурсу в бра работе Интер защиты.

`p00.upd.kaspersky.com`
`p01.upd.kaspersky.com`
`p02.upd.kaspersky.com`
`p03.upd.kaspersky.com`
`p04.upd.kaspersky.com`
`p05.upd.kaspersky.com`
`p06.upd.kaspersky.com`
`p07.upd.kaspersky.com`
`p08.upd.kaspersky.com`
`p09.upd.kaspersky.com`
`p10.upd.kaspersky.com`
`p11.upd.kaspersky.com`
`p12.upd.kaspersky.com`
`p13.upd.kaspersky.com`
`p14.upd.kaspersky.com`
`p15.upd.kaspersky.com`
`p16.upd.kaspersky.com`
`p17.upd.kaspersky.com`
`p18.upd.kaspersky.com`
`p19.upd.kaspersky.com`
`downloads.kaspersky-labs.com`
`cm.k.kaspersky-labs.com`
Протокол: `HTTP`
Порт: `80`
	Обновление баз и приложения.

`ds.kaspersky.com` Протокол: `HTTPS`	Использование Ka Security Network.

Порт: 443

ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com Протокол: Any Порт: 443, 1443	Использование Ka Security Network.
click.kaspersky.com redirect.kaspersky.com Протокол: HTTPS	Переход по ссылк интерфейса.

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 файлы**.

   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 Free удаляет существующий файл и помещает на его место файл, восстановленный из резервной копии.

   - **сохранить оба файла** – приложение Kaspersky Free 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 Free 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.

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.

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.

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.

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.

Код активации

Код, который вы получаете, приобретая лицензию на использование Kaspersky Free. Этот код необходим для активации программы.

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

Компоненты защиты

Части Kaspersky Free, предназначенные для защиты компьютера от отдельных типов угроз (например, 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.

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 Free.

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.

Руткит

Программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в операционной системе.

В операционных системах Windows под руткитом принято подразумевать программу, которая внедряется в операционную систему и перехватывает системные функции (Windows API). Перехват и модификация низкоуровневых API-функций, в первую очередь, позволяет такой программе достаточно качественно маскировать свое присутствие в операционной системе. Кроме того, как правило, руткит может маскировать присутствие в операционной системе любых описанных в его конфигурации процессов, каталогов и файлов на диске, ключей в реестре. Многие руткиты устанавливают в операционную систему свои драйверы и службы (они также являются "невидимыми").

Серверы обновлений "Лаборатории Касперского"

HTTP-серверы "Лаборатории Касперского", с которых программа "Лаборатории Касперского" получает обновления баз и программных модулей.

Скрипт

Небольшая компьютерная программа или независимая часть программы (функция), как правило, написанная для выполнения конкретной задачи. Наиболее часто применяется при использовании программ, встраиваемых в гипертекст. Скрипты запускаются, например, когда вы открываете некоторые сайты.

Если включена постоянная защита, программа отслеживает запуск скриптов, перехватывает их и проверяет на присутствие вирусов. В зависимости от результатов проверки вы можете запретить или разрешить выполнение скрипта.

Срок действия лицензии

Период времени, в течение которого вы можете пользоваться функциями программы и дополнительными услугами.

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.

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, Acrobat, Reader являются либо зарегистрированными товарными знаками, либо товарными знаками компании Adobe в США и/или других странах.

Apple, App Store, macOS, Safari – товарные знаки Apple Inc., зарегистрированные в США и других странах и регионах.

Arm – зарегистрированный товарный знак Arm Limited (или дочерних компаний) в США и/или других странах.

Cloudflare, логотип Cloudflare и Cloudflare Workers являются товарными знаками и/или зарегистрированными товарными знаками компании Cloudflare, Inc. в США и других юрисдикциях.

Google, Google Public DNS, Google Play, Google Chrome, Chromium, Android, SPDY – товарные знаки Google LLC.

Huawei является товарным знаком Huawei Technologies Co., Ltd.

Intel, Celeron, Atom – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Выполнен автоматический переход на Kaspersky Free

Развернуть всё | Свернуть всё

Готово

При нажатии на кнопку открывается главное окно Kaspersky Free.

Окно Расширение защиты

Развернуть всё | Свернуть всё

Купить сейчас

Кнопка, при нажатии на которую открывается окно браузера на странице интернет-магазина, в котором вы можете приобрести подписку.

Пробовать бесплатно

По ссылке запускается переход на пробную подписку.

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.

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

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 Free.

Отмена

По ссылке вы можете отменить активацию приложения.

Продолжить

При нажатии на кнопку запускается установка и активация приложения, которому соответствует введенный вами код активации.

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 Free удаляет существующий файл и помещает на его место файл, восстановленный из резервной копии.
- **сохранить оба файла** – Приложение Kaspersky Free 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 Free 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 **Продолжить** будет запущен мастер миграции. В результате работы мастера миграции вы перейдете на новую подписку.

По кнопке **Отказаться** вы можете отменить переход на новую подписку.

Об использовании приложения ребенком

Если на вашем компьютере установлено и используется приложение Kaspersky Safe Kids, ребенок может выключить Kaspersky Safe Kids средствами приложения Kaspersky Free. Чтобы этого не произошло, рекомендуется установить пароль на изменение настроек Kaspersky Free.

Если вы вошли в операционную систему под учетной записью, которая привязана к профилю ребенка в приложении Kaspersky Safe Kids, приложение Kaspersky Free 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 приложения. 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.
Завершение работы приложения	Выход из приложения.
Удаление / изменение / восстановление приложения	Удаление, изменение или восстановление приложения.
Просмотр отчетов	Переход в окно **Отчеты**.
Выключение компонентов защиты	Приостановка защиты из контекстного меню значка приложения в области уведомлений.

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.

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 лицензии:

- Лицензионный ключ.
- Статус ключа.
- Количество компьютеров, на которое распространяется лицензия.
- Дата активации.
- Дата окончания срока действия лицензии.
- Количество дней, оставшихся до окончания срока действия лицензии.

О лицензии / О подписке

По ссылке открывается окно со сведениями о действующей лицензии или подписке.

Лицензионное соглашение

При нажатии на кнопку открывается окно с текстом Лицензионного соглашения.

В зависимости от наличия лицензии и от особенностей вашей версии приложения в окне могут отображаться различные кнопки для запуска действий, связанных с лицензией. Ниже приведены описания кнопок, предусмотренных по умолчанию.

Расширить защиту

Кнопка, при нажатии на которую открывается окно **Расширение защиты**. В окне вы можете ознакомиться с информацией о новом приложении или перейти к использованию этого приложения.

Активировать приложение

Кнопка, при нажатии на которую запускается мастер активации приложения.

Кнопка отображается, если приложение не активировано.

Обновить базы

Кнопка, при нажатии на которую запускается обновление баз приложения.

Кнопка отображается, если возникшие проблемы с лицензией можно решить обновлением баз (например, дата выпуска баз не соответствует сроку действия лицензии).

Причины и возможные решения

Кнопка, при нажатии на которую открывается окно браузера на сайте Службы технической поддержки с информацией о возникшей проблеме.

Кнопка отображается, если возникли проблемы с действующей лицензией.

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 Free 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 Free завершает работу мастера установки сертификата.

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.

Разрыв сетевых соединений

Если в момент завершения работы на компьютере или приостановки защиты были установлены сетевые соединения, контролируемые приложением, на экран будет выведено уведомление о разрыве этих соединений. Это необходимо для корректного завершения работы приложения. Разрыв происходит автоматически по истечении 10 секунд либо при нажатии на кнопку **Да**. Большинство прерванных соединений восстанавливается через некоторое время.

Если во время разрыва соединения вы скачиваете файл без использования менеджера загрузки, передача данных будет прервана. Для получения файла вам потребуется повторно инициировать его загрузку.

Вы можете отменить разрыв соединений. Для этого в окне уведомления нажмите на кнопку **Нет**. При этом приложение продолжит свою работу.

Обнаруженные объекты

Развернуть всё | Свернуть всё

Устранить

При нажатии на кнопку приложение Kaspersky Free 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 Free

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.

Регистрация

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.

Войти

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 отображаются следующие параметры:

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 отображаются следующие параметры:

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

*Facebook принадлежит компании META Inc, признанной экстремистской организацией на территории Российской Федерации.

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 Free возвращает файл, выбранный в списке, в папку, в которой он находился до помещения на карантин.

Удалить

Кнопка, при нажатии на которую приложение Kaspersky Free удаляет файл, выбранный в списке.

Удалить все

При нажатии на кнопку приложение Kaspersky Free удаляет все резервные копии файлов, помещенные на карантин.

Приложение Kaspersky Free 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 Free не создает резервные копии. Для восстановления таких объектов необходимо использовать средства восстановления операционной системы (подробную информацию можно получить из документации к операционной системе, установленной на вашем компьютере) либо обновить приложения через Магазин Windows.

Окно Новости

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.

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 Free выполняет задачу один раз в сутки согласно внутренним настройкам. **По минутам** / **По часам** / **По дням** / **Еженедельно** / **Ежемесячно** / **В указанное время**. Приложение Kaspersky Free выполняет задачу по сформированному вами расписанию, которое можно уточнить до минут. При выборе одного из этих вариантов доступен список **Отложить запуск после старта приложения на N минут**. **После запуска приложения**. Приложение Kaspersky Free выполняет задачу после своего запуска, спустя столько минут, сколько указано в поле **Запускать через N минут**. **После каждого обновления**. Приложение Kaspersky Free 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 Free выполняет задачу после включения компьютера. Флажок отображается, если выбран один из следующих режимов запуска: **По дням** / **Еженедельно** / **Ежемесячно** / **В указанное время**.

Искать обновления для приложений только в случае, когда компьютер заблокирован или включена экранная заставка (Обновление приложений) **Выполнять анализ объектов только в случае, когда компьютер заблокирован или включена экранная заставка** (Менеджер приложений)	Приложение Kaspersky Free запускает задачу тогда, когда вы закончили работу на компьютере. Таким образом, задача не будет занимать ресурсы компьютера во время работы. Флажок отображается, если выбран режим запуска **После каждого обновления**.

Настройки обновления

Настройка	Описание
Расписание обновления баз	По ссылке открывается окно **Расписание обновления баз**, в котором можно выбрать один из режимов запуска обновлений баз: **Автоматически**. Режим запуска задачи обновления, при котором приложение Kaspersky Free 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 Free скачивает его и устанавливает обновления на компьютер. **Вручную**. Этот режим запуска задачи обновления позволяет вам запускать задачу обновления вручную. **По минутам** / **По часам** / **По дням** / **Еженедельно** / **Ежемесячно** / **В указанное время** / **После запуска приложения**. Режим запуска задачи обновления, при котором приложение Kaspersky Free выполняет задачу обновления по сформированному вами расписанию. Если выбран этот режим запуска задачи обновления, вы также можете запускать задачу обновления приложения Kaspersky Free 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 Free 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 Free запускается от имени пользователя, с правами которого вы зарегистрированы в операционной системе. Однако обновление приложения Kaspersky Free 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 Free от имени этого пользователя.

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 Free.

Запомнить пароль на эту сессию

Если флажок установлен, приложение Kaspersky Free запоминает введенный пароль и больше не запрашивает его во время текущего сеанса работы.

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 Free 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 Free.

Критические события. События критической важности, указывающие на проблемы в работе приложения Kaspersky Free 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 Free будет запускать задачи обновления. Функция доступна для запуска задачи обновления приложения Kaspersky Free 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**.

Выберите zip-файл или папку

Применение альтернативных тем оформления доступно не во всех регионах.

При выборе темы оформления учитывайте следующие ограничения:

- Приложение Kaspersky Free 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 Free 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 Free.

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 приложение Kaspersky Free удаляет данные из папки отчетов.

По умолчанию приложение Kaspersky Free удаляет отчеты задач проверки, отчеты задачи обновления.

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 Free 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 Free блокирует любую попытку удаленного управления сервисами приложений. При попытке удаленного управления появляется уведомление над значком Kaspersky Free в области уведомлений панели задач Microsoft Windows (если уведомления не отключены).

Разрешить управление настройками Kaspersky Free через приложения удаленного управления

Если флажок установлен, доверенные приложения удаленного администрирования (такие как TeamViewer, LogMeIn Pro и Remotely Anywhere) могут изменять настройки приложения Kaspersky Free.

Недоверенным приложениям удаленного администрирования изменение настроек приложения Kaspersky Free 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 Free использует подключение к интернету в работе некоторых компонентов защиты, а также для обновления баз и модулей приложения.

Автоматически определять настройки прокси-сервера

Приложение Kaspersky Free 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 Free использует настройки прокси-сервера, указанные в браузере Microsoft Edge на базе Chromium. Kaspersky Free не учитывает настройки прокси-серверов, указанные для других браузеров, установленных на компьютере пользователя.

Использовать указанные настройки прокси-сервера

Приложение Kaspersky Free 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 Free попытается выполнить NTLM-, а затем BASIC-аутентификацию.

Если флажок не установлен или настройки прокси-сервера не указаны, то приложение Kaspersky Free 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 Free будет использовать в дальнейшем указанные имя пользователя и пароль. В противном случае приложение Kaspersky Free 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 Free не использует прокси-сервер при обновлении баз и модулей приложения из локальной или сетевой папки.

Если флажок снят, приложение Kaspersky Free 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 не можете настраивать компоненты защиты в Kaspersky Free.

Расширить защиту

По кнопке открывается окно **Изменение уровня защиты**, в котором вы можете перейти к использованию Kaspersky Internet Security и получить доступ к дополнительным компонентам защиты.

Окно Ввод пароля

Развернуть всё | Свернуть всё

Текущий пароль

Текущий пароль, который используется для доступа к управлению приложением Kaspersky Free.

Запомнить пароль на эту сессию

Если флажок установлен, приложение Kaspersky Free 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 Free 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 Free.

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.

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 Free применяет разные наборы настроек. Наборы настроек, сохраненные в приложении, называются *уровнями безопасности*. • **Предельный**. Приложение Kaspersky Free проверяет файлы всех типов. Во время проверки составных файлов приложение дополнительно проверяет файлы почтовых форматов. • **Оптимальный**. Приложение Kaspersky Free 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 Free 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 Free обнаруживает зараженный или возможно зараженный объект, оно сразу уведомляет вас об этом и запрашивает действие над обнаруженным объектом. Этот вариант доступен, если в разделе **Настройка → Настройки производительности → Потребление ресурсов компьютера** снят флажок **Автоматически выполнять рекомендуемые действия**. • **Выбирать действие автоматически**. При обнаружении зараженных или возможно зараженных объектов приложение Kaspersky Free выполняет действие,

рекомендуемое специалистами "Лаборатории Касперского":

- Зараженный объект приложение Kaspersky Free сначала пытается вылечить и, если это не удается - удаляет.

- Возможно зараженный объект приложение Kaspersky Free удаляет, если установлен флажок **Удалять вредоносные утилиты, рекламные приложения, приложения автодозвона и подозрительные упаковщики**. Если флажок снят, приложение не удаляет возможно зараженный объект; уведомление об обнаружении такого объекта отображается в центре уведомлений (открывается по кнопке **Подробнее** в главном окне приложения).

  Этот вариант доступен, если в разделе **Настройка → Настройки 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 Free 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 Free 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 Free. 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 Free считает исполняемыми. Приложение проверяет исполняемые файлы всегда, независимо от того, файлы какого типа вы выбрали для проверки. **Все файлы**. Если выбран этот параметр, Kaspersky Free 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. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива).
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 Free 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 Free разбирает файл почтового формата и анализирует на наличие вирусов каждый его компонент (тело письма, вложения).

	Если флажок снят, приложение Kaspersky Free 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 Free, 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 Free, 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 Free 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 Free 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 Free проверяет внешние устройства, размер которых не превышает указанный максимальный размер. Если флажок снят, то Kaspersky Free проверяет внешние устройства любого размера.
Отображать ход проверки	Если флажок установлен, то Kaspersky Free отображает ход проверки внешних устройств в отдельном окне, а также в окне запуска проверки.
Запретить остановку задачи проверки	Если флажок установлен, то для задачи проверки внешних устройств недоступна кнопка **Остановить** в окне запуска проверки.

Настройки фоновой проверки

Если фоновая проверка включена, приложение Kaspersky Free 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 Free проверяет системную память, системные разделы, загрузочные секторы и объекты автозапуска, а также выполняет поиск руткитов.

Если компьютер работает от аккумулятора, приложение Kaspersky Free не выполняет фоновую проверку компьютера.

Настройки поиска уязвимостей в приложениях

Настройка	Описание
Изменить область поиска	По ссылке открывается окно **Область поиска уязвимостей** со списком объектов, которые проверяются при поиске уязвимостей в приложениях. Вы можете добавить в список объекты или удалить добавленные вами объекты. Чтобы исключить объект из проверки, не обязательно удалять объект из списка, достаточно снять флажок напротив названия объекта.
Расписание поиска	**Вручную**. Режим запуска, при котором вы запускаете поиск уязвимостей в приложениях вручную в удобное для вас время. **По расписанию**. Режим запуска задачи проверки, при котором приложение выполняет задачу проверки по сформированному вами расписанию. Если выбран этот режим запуска задачи проверки, вы также можете запускать задачу проверки вручную.

Настройки учетной записи

Развернуть всё | Свернуть всё

Запускать проверку с правами

Выбор учетной записи, с правами которой приложение Kaspersky Free 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 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 Free блокирует сетевое соединение с атакующим компьютером. Описания известных в настоящее время видов сетевых атак и методов борьбы с ними содержатся в базах приложения Kaspersky Free. 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.

Добавлять атакующий компьютер в список блокирования на N мин	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 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 Free. Мониторинг активности анализирует активность приложений и предоставляет собранную информацию о событиях другим компонентам приложения Kaspersky Free.

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 Free отслеживает исполняемые файлы, запускаемые уязвимыми приложениями. Если приложение Kaspersky Free 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 обновлении приложения Kaspersky Free с версии более ранней, чем Kaspersky Free 2018, эта настройка принимает значение по умолчанию.

При обнаружении угрозы

В раскрывающемся списке можно выбрать действие, которое должен выполнять Мониторинг активности в случае запуска исполняемых файлов из контролируемых уязвимых приложений.

Список содержит следующие варианты действий:

- **Спрашивать пользователя**. Мониторинг активности запрашивает действие у пользователя. Этот вариант доступен, если в разделе **Настройка → Настройки производительности → Потребление ресурсов компьютера** снят флажок **Автоматически выполнять рекомендуемые действия**.
- **Выбирать действие автоматически**. Мониторинг активности автоматически выполняет действие, указанное в настройках приложения Kaspersky Free и добавляет информацию о выбранном действии в отчет. Этот вариант доступен, если в разделе **Настройка → 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 **Настройка → 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 **Настройка → Настройки производительности → Потребление ресурсов компьютера** установлен флажок **Автоматически выполнять рекомендуемые действия**.

- **Удалять приложение**. Мониторинг активности удаляет приложение.

- **Завершать работу приложения**. Мониторинг активности завершает все процессы приложения.

- **Завершать работу приложения**. Мониторинг активности не предпринимает никаких действий с приложением.

При возможности отменить последствия вредоносной или другой активности приложения

В раскрывающемся списке можно выбрать действие, которое Мониторинг активности должен выполнять при наличии возможности отменить последствия вредоносной или другой активности приложения.

- **Спрашивать пользователя**. Если в результате работы Мониторинга активности, Файлового Антивируса или выполнения задачи проверки подтверждается необходимость отмены последствий, Мониторинг активности запрашивает действие у пользователя. Этот вариант доступен, если в разделе **Настройка → Настройки 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 **Настройка → 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.

При обновлении приложения Kaspersky Free с версии более ранней, чем Kaspersky Free 2018, эта настройка принимает значение по умолчанию.

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.

Потребление ресурсов компьютера

Настройка	Описание
Автоматически выполнять рекомендуемые действия	Если флажок снят, основные компоненты приложения Kaspersky Free работают в интерактивном режиме. Это значит, что приложение Kaspersky Free 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 Free 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 Free 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 Free 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 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 Free 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 Free 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 Free приостанавливает выполнение задач по расписанию и высвобождает ресурсы операционной системы для других приложений.
Выполнять поиск небезопасных настроек операционной системы	Если флажок установлен, приложение Kaspersky Free выполняет поиск небезопасных настроек операционной системы в автоматическом режиме.
Запускать Kaspersky Free при включении компьютера (рекомендуется)	Если флажок установлен, то приложение Kaspersky Free запускается после загрузки операционной системы и защищает компьютер пользователя в течение всего сеанса работы.

	Если флажок не установлен, то приложение Kaspersky Free 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 (использует значительные ресурсы компьютера)	Если флажок установлен, при обнаружении вредоносной активности в операционной системе на экране отображается всплывающее уведомление. В уведомлении приложение Kaspersky Free предлагает провести процедуру лечения активного заражения компьютера. После подтверждения пользователем этой процедуры приложение Kaspersky Free устраняет угрозу. Завершив процедуру лечения активного заражения, приложение Kaspersky Free 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.
Автоматически искать, как ускорить компьютер	Если флажок установлен, выполняется автоматический поиск возможностей для ускорения компьютера.
Включить самозащиту	Если флажок установлен, то Kaspersky Free предотвращает изменение и удаление файлов приложения на жестком диске, процессов в памяти и записей в системном реестре.
Разрешить управление настройками Kaspersky Free через приложения удаленного управления	Если флажок установлен, доверенные приложения удаленного администрирования (такие как TeamViewer, LogMeIn Pro и Remotely Anywhere) могут изменять настройки Kaspersky Free. Недоверенным приложениям удаленного администрирования изменение настроек Kaspersky Free будет запрещено, даже если флажок установлен.

Включить возможность внешнего управления системными службами	Если флажок установлен, то Kaspersky Free разрешает управление службами приложения с удаленного компьютера. При попытке управления службами приложениями с удаленного компьютера, над значком приложения в области уведомлений панели задач Microsoft Windows отображается уведомление (если служба уведомлений не выключена пользователем).
Включить запись дампов	Если флажок установлен, то Kaspersky Free записывает дампы в случае сбоев в работе. Если флажок снят, то Kaspersky Free 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 папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.

  - Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

- Тип объектов, которые должны исключаться из проверки. Введите название типа объекта по классификации Энциклопедии "Касперского" (например, `Email-Worm`, `Rootkit` или `RemoteAdmin`). Вы можете использовать маски с символами `?` (заменяет любой символ) и `*` (заменяет любые несколько символов). Например, если указана маска `Client*`, приложение исключает из проверки объекты типов `Client-IRC`, `Client-P2P` и `Client-SMTP`.

- Хеш-сумму объекта. Сверка хеш-суммы объекта с указанной в этой настройке позволяет исключить из проверки объект, если он не изменялся.

- Компоненты защиты, при работе которых действует исключение.

Вместо удаления исключения из списка можно изменить статус исключения на **Неактивно** (в окне добавления или изменения исключения), в этом случае оно не будет действовать.

Указать доверенные приложения

По ссылке открывается окно со списком доверенных приложений. Приложение Kaspersky Free 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 Free 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 Free 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 Free. Приложению разрешено управлять приложением Kaspersky Free, используя графический интерфейс приложения Kaspersky Free. Необходимость разрешить приложению управлять интерфейсом приложение Kaspersky Free 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 Free исключает из проверки весь сетевой трафик приложения или трафик, передаваемый по протоколу SSL. 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 Free 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 Free исключает из проверки приложения, подписанные доверенной цифровой подписью. Kaspersky Free автоматически помещает такие приложения в группу **Доверенные**.

Если выбрано **Не использовать**, то Kaspersky Free проверяет приложения независимо от наличия цифровой подписи. Приложение Kaspersky Free помещает приложение в группу доверия в зависимости от уровня опасности, которую это приложение может представлять для компьютера.

Настройки сети

Настройка	Описание
Ограничивать трафик при лимитном подключении	Если флажок установлен, приложение ограничивает собственный сетевой трафик в том случае, если подключение к интернету является лимитным. Приложение Kaspersky Free 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 Free внедряет в трафик скрипт взаимодействия с веб-страницами. Этот скрипт обеспечивает работу таких компонентов как Проверка ссылок.
Поддерживать работу DNS поверх HTTPS (DoH)	Если флажок установлен, приложение корректно обрабатывает данные DNS при передаче их по протоколу HTTPS. Мы не рекомендуем снимать этот флажок.
Управлять DoH-серверами	По ссылке открывается окно, в котором вы можете добавить вручную DoH-сервер, через который будет выполняться передача данных DNS в браузере. Здесь вы можете прочитать о том, что такое DNS поверх HTTPS (DoH) и как добавить DoH-сервер.
Контролируемые порты	**Контролировать все сетевые порты**. Режим контроля портов, при котором Почтовый Антивирус и Интернет-защита контролируют все открытые порты вашего компьютера.

Контролировать только выбранные сетевые порты. Режим контроля портов, при котором Почтовый Антивирус и Интернет защита контролируют выбранные вами порты вашего компьютера. Указать контролируемые сетевые порты можно в окне **Сетевые порты**, которое открывается по ссылке **Выбрать**. Вы также можете указать, при работе каких приложений нужно контролировать все сетевые порты, используемые этими приложениями:

- **Контролировать все порты для приложений из списка, рекомендованного "Лабораторией Касперского"**. Список таких приложений задан по умолчанию и входит в комплект поставки приложения Kaspersky Free.

  Если установлен этот флажок, приложение Kaspersky Free контролирует все порты для следующих приложений:

  - Adobe Acrobat Reader.
  - Apple Application Support.
  - Google Chrome.
  - Microsoft Edge.
  - Mozilla Firefox.
  - Internet Explorer.
  - Java.
  - mIRC.
  - Opera.
  - Pidgin.
  - Safari.
  - Агент Mail.ru.
  - Яндекс.Браузер.

- **Контролировать все порты для указанных приложений**. Указать приложения можно в окне

	Приложения, которое открывается по ссылке **Выбрать**.
Сетевые порты	Список портов, которые обычно используются для передачи почты и веб-трафика, включен в комплект поставки приложения Kaspersky Free. По умолчанию приложение Kaspersky Free 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 Free контролирует трафик, проходящий через этот порт. Если в графе **Статус** в строке порта установлено значение *Неактивно*, то приложение Kaspersky Free 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 Free использует установленный сертификат "Лаборатории Касперского" для проверки SSL-соединений, если этого требуют компоненты Интернет защита и Проверка ссылок. Если эти компоненты выключены, приложение Kaspersky Free не проверяет SSL-соединения. После того как приложение Kaspersky Free 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 Free не проверяет в процессе своей работы. Вы можете выбрать виды активности приложения, которые приложение Kaspersky Free не будет контролировать (например, не проверять сетевой трафик). Приложение Kaspersky Free 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 Free использует эти параметры в работе некоторых компонентов защиты, в том числе для обновления баз и модулей приложения. Для автоматической настройки прокси-сервера приложение Kaspersky Free 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 Free.
- **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**.

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 с помощью аппаратной виртуализации	Защита ввода данных с аппаратной клавиатуры позволяет избежать перехвата данных, которые вы вводите с клавиатуры на сайтах (см. подробнее в разделе О защите ввода данных с аппаратной клавиатуры). Установите флажки для категорий сайтов, на которых нужно защищать ввод данных с аппаратной клавиатуры. По ссылке **Настройка исключений** можно сформировать списки сайтов, на которых нужно включить или выключить защиту ввода данных с аппаратной клавиатуры вне зависимости от выбранных категорий сайтов. При добавлении исключения вы можете использовать маски.
Экранная клавиатура	Многие приложения-шпионы обладают функциями снятия снимков экрана, которые автоматически передаются злоумышленнику для последующего анализа и извлечения персональных данных пользователя. Экранная клавиатура защищает вводимые персональные данные от перехвата посредством снятия снимков экрана. (Подробнее об Экранной клавиатуре). Чтобы Экранная клавиатура включилась, после установки приложение Kaspersky Free 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 Free 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 Free 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.

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**.

Обзор

При нажатии на кнопку открывается окно **Выбор папки**. В этом окне можно выбрать внешний диск, используемый в качестве хранилища резервных копий.

Окно Поддержка

Развернуть всё | Свернуть всё

Окно содержит информацию, необходимую для обращения в Службу технической поддержки: версию приложения Kaspersky Free, дату и время выпуска баз и модулей приложения, версию операционной системы, ключ.

Ключ

По ссылке **<ключ>** открывается окно **Информация о лицензии**, в котором приведены сведения о действующей лицензии.

Ответы на часто задаваемые вопросы

По ссылке открывается окно браузера на странице интерактивной поддержки. Эта страница содержит ответы на вопросы, которые пользователи чаще всего задают специалистам Службы технической поддержки.

Рекомендации по настройке приложения

По ссылке открывается окно браузера на странице сайта Службы технической поддержки, где опубликованы статьи о настройке и использовании приложения Kaspersky Free.

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.

Окно Восстановление файлов

Развернуть всё | Свернуть всё

Остановить

При нажатии на кнопку приложение Kaspersky Free прекращает восстановление файлов из 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.

О фишинге

Фишинг – это вид интернет-мошенничества, заключающийся в краже персональных данных пользователей, распространяемый по электронной почте и другим каналам.

Электронные письма представляют собой поддельные уведомления от банков, провайдеров, онлайн-магазинов, электронных платежных систем или других организаций. В письмах получателя заманивают пройти на сайт мошенников под предлогом, например, обновить регистрационные данные или узнать подробнее о товаре или услуге.

Ничего не подозревающий получатель такого письма проходит по указанной ссылке и оказывается на фишинговом сайте, который выглядит как точная копия официального сайта организации.

Пользователь интернета может попасть на фишинговый сайт другими способами, например, перейдя по ссылке в поисковой системе.

Как правило, мошенники могут преследовать разные цели. Одна из них – обманным путем получить конфиденциальные данные пользователей, такие как логины, пароли 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 Free предусмотрена проверка содержимого электронных писем и веб-ресурсов на наличие фишинговых ссылок. Ссылки проверяются по базе фишинговых веб-адресов, которая регулярно обновляется.

Для дополнительной защиты во время проверки используется эвристический анализ, а также осуществляются запросы к облачным службам Kaspersky Security Network (KSN). Kaspersky Security Network содержит самые актуальные данные о недавно появившихся угрозах, в том числе о фишинговых веб-ресурсах, которые еще не успели попасть в базы "Лаборатории Касперского". Данные, поступающие в KSN, анализируются сотрудниками Вирусной лаборатории в режиме реального времени.

Если вы попали на фишинговый сайт, вы можете сообщить о нем в Kaspersky Security Network с помощью расширения Kaspersky Protection.

О криптоджекинге

Криптоджекинг – это вид киберпреступления, которое заключается в использовании чужих устройств (компьютеров, планшетов, смартфонов и серверов) без ведома их владельцев для скрытого создания (майнинга) криптовалют, например, биткоина.

Как работает криптоджекинг

Преступник взламывает устройство и устанавливает на него специальное программное обеспечение, которое работает в фоне и не вызывает никаких подозрений у пользователя.

Вредоносный код устанавливается следующими способами:

- Пользователь проходит по фишинговой ссылке в почтовом сообщении, в результате чего на устройство загружается код, предназначенный для майнинга.
- Пользователь переходит на сайт, на котором загружаются якобы рекламные баннеры, которые при открытии запускают вредоносный код (JavaScript).

Когда программное обеспечение, предназначенное для криптоджекинга, установлено на устройстве, начинается процесс майнинга, то есть создания криптовалюты. Майнинг требует значительных вычислительных мощностей, что негативно сказывается на работе устройства.

В чем опасность криптоджекинга

Хотя криптоджекинг и не вредит напрямую операционной системе и данным пользователя, он все же может представлять значительную угрозу. Например, криптоджекинг может вызвать перегрев устройства и привести к поломке компьютера или сокращению срока его службы.

Как распознать криптоджекинг

О криптоджекинге могут сигнализировать следующие признаки:

- **Снижение скорости работы устройства**. Криптоджекинг можно заподозрить, если снизилось быстродействие операционной системы, стали медленнее запускаться приложения, быстро расходуется заряд батареи или устройство начало выключаться без видимой причины.
- **Перегрев устройства**. Криптоджекинг расходует большое количество ресурсов, что может приводить к перегреву устройства. Постоянный шум вентиляторов охлаждения может быть признаком того, что на устройстве запущено программное обеспечение, предназначенного для криптоджекинга.
- **Возросшая нагрузка на центральный процессор**. Если вы заходите на сайт, на котором нет видео или аудио-контента, при этом нагрузка на центральный процессор возрастает,

это может свидетельствовать о том, что на этом сайте запущен скрипт для криптоджекинга. Проверить уровень загрузки процессора вы можете в Диспетчере задач на закладке **Производительность**.

Как защититься от криптоджекинга

Приложение Kaspersky Free включает инструменты, которые помогут защитить ваше устройство от криптоджекинга. Сайты, которые вы посещаете, проверяются на наличие встроенного вредоносного кода. В случае обнаружения попытки криптоджекинга, приложение показывает уведомление, в котором вы сможете удалить вредоносный код.

Ссылки проверяются по базе фишинговых веб-адресов и поддельных криптовалютных бирж, которая регулярно обновляется. При попытке перейти по вредоносной ссылке, приложение покажет предупреждение.

Даже если код для криптоджекинга попадет на устройство, приложение Kaspersky Free определит его как вредоносный и заблокирует его запуск.

Для дополнительной защиты во время проверки используется эвристический анализ, а также осуществляются запросы к облачным службам Kaspersky Security Network (KSN). Kaspersky Security Network содержит самые актуальные данные о недавно появившихся угрозах, в том числе об угрозах криптоджекинга.

О криптомошенничестве

Мошенничество с криптовалютой – это вид киберпреступлений, целью которых является кража криптовалюты, например, биткоинов. За первую половину 2022 года приложения "Лаборатории Касперского" обнаружили почти 200 000 попыток кражи криптовалют и данных криптокошельков пользователей.

Виды криптомошенничества

Существуют следующие виды мошенничества с криптовалютой:

- **Поддельные сайты и криптокошельки**. Мошенники создают поддельный сайт известной криптовалютной биржи или поддельный криптокошелек. Отличить подобный сайт от настоящего не всегда возможно, так как доменное имя и оформление сайта похожи на настоящие. Пользователь заходит на такой сайт и вводит свои данные, которые в итоге попадают в руки мошенников.

- **Криптофишинг**. Мошенники создают фишинговые ссылки, которые ведут на поддельные сайты, криптовалютные биржи и инвестиционные площадки. Затем рассылают их в почтовых сообщениях, а также размещают на других сайтах. Пользователи переходят по таким ссылкам, в результате чего теряют свои данные или средства.

- **Поддельные инвестиции в "новую" криптовалюту**. Мошенники создают фиктивное коммерческое предложение о начале инвестиций в новый проект, например, создание новой криптовалюты. Заинтересованные пользователи переводят средства на указанный криптокошелек, однако никакой новой криптовалюты не создается, а вложенные средства не возвращаются.

- **Поддельные инвестиции в криптовалюте**. Мошенники размещают рекламу в социальных сетях о выгодных вложениях в криптовалюте, обещая увеличить сумму вложений в несколько раз. Вместо полученной выгоды пользователи теряют вложенные средства.

- **Мошенничество при покупке оборудования для майнинга**. Пользователи переводят средства на покупку оборудование для создания (майнинга) криптовалюты, но не получают обещанный товар.

- **Поддельные сайты покупки криптовалют**. Мошенники создают сайт, на котором вы якобы можете приобрести криптовалюту за обычные деньги по хорошему курсу. Вы переводите свои средства, но не получаете криптовалюту.

- **Создание ажиотажного спроса на криптовалюту**. Мошенники создают массированную рекламную компанию по раскрутке какой-либо одной криптовалюты. При этом они обещают, что цена на эту криптовалюту будет расти. Инвесторы в спешке скупают рекламируемую криптовалюту. Затем мошенники быстро продают эту валюту по высокой цене в большом объеме, в результате чего цена на эту криптовалюту может упасть ниже начальной в течение нескольких минут.

Как защититься от мошенничества с криптовалютой

Приложение Kaspersky Free включает инструменты, которые помогут вам защититься от мошенничества с криптовалютой. Приложение определит, что сайт или криптовалютная биржа является поддельной и уведомит вас об этом.

Ссылки на сайтах и в почтовых сообщениях проверяются по базе фишинговых веб-адресов и поддельных криптовалютных бирж, которая регулярно обновляется. При попытке перейти по вредоносной ссылке, приложение покажет предупреждение.

Для дополнительной защиты во время проверки используется эвристический анализ, а также осуществляются запросы к облачным службам Kaspersky Security Network (KSN). Kaspersky Security Network содержит самые актуальные данные о недавно появившихся угрозах, в том числе об угрозах криптомощенничества.

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.

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.

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 Службу технической поддержки;
- 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.

Управлять подпиской

По кнопке открывается ваш аккаунт My Kaspersky на странице управления подпиской. Кнопка доступна, если вы подключили устройство к аккаунту My Kaspersky.

Расширить защиту

По кнопке открывается окно, где вы можете перейти на подписку Kaspersky Standard или Kaspersky Plus без дополнительного скачивания и установки программного обеспечения.

Вы можете временно перейти на пробную подписку, чтобы узнать о преимуществах платной подписки, или купить подписку и перейти к постоянному использованию приложения по платной подписке. Подробнее о переходе на платную подписку вы можете прочитать в разделе Переход с Kaspersky Free на другую подписку.

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.

В зависимости от вашей подписки, кнопка может быть недоступна.

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.

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.

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 ознакомиться 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.