Содержание

Уведомления о товарных знаках

О программе Kaspersky Security Element

Программа Kaspersky Security Element предназначена для защиты организаций от программ-вымогателей, которые могут, например, блокировать доступ к компьютерной системе до тех пор, пока не будет выплачена денежная сумма. Kaspersky Security Element также повышает осведомленность пользователей, предоставляя информацию о возникающих киберугрозах и существующих решениях для защиты.

Защита компьютеров

Kaspersky Security Element обнаруживает вредоносные программы или легальные программы, которые могут быть использованы для нанесения вреда данным (рекламные и другие программы), и автоматически блокирует подозрительную активность. Программа хранит области данных, измененные подозрительными процессами, в скрытом защищенном хранилище. Когда подозрительный процесс создает или изменяет файлы или системный реестр, Kaspersky Security Element обнаруживает такие изменения, блокирует процесс, а затем пытается откатить обнаруженные действия путем восстановления областей данных из защищенного хранилища. В программе Kaspersky Security Element имеется механизм самозащиты, который предотвращает изменение и удаление файлов программы с жесткого диска, процессов памяти программы и записей системного реестра.

> "Лаборатория Касперского" не получает области данных, используемые программой для отката действий обнаруженных объектов.

Методы обнаружения

Kaspersky Security Element обнаруживает подозрительную активность с помощью антивирусных баз и Kaspersky Security Network.

Антивирусные базы обеспечивают защиту от известных угроз. Kaspersky Security Element сравнивает поведение программ на компьютере с вирусами и другими вредоносными программами, зарегистрированными в антивирусных базах. Обратите внимание, что при обновлении антивирусных баз могут измениться недоступные пользователю параметры безопасности.

Kaspersky Security Network обеспечивает защиту от новейших угроз. Kaspersky Security Element автоматически отправляет статистику, полученную с вашего компьютера, в "Лабораторию Касперского". Участие в Kaspersky Security Network обеспечивает вашему компьютеру доступ к статистике репутации программ и веб-сайтов.

Режимы работы программы

Kaspersky Security Element поддерживает доступ пользователей к функциям на основе ролей. Можно выбрать один из следующих режимов работы программы:

- Администратор

  Этот режим подходит для выполнения общих задач администрирования, таких как установка программы Kaspersky Security Element на компьютеры организации и получение отчетов о защите.

- Пользователь (с отчетами по электронной почте)

  В этом режиме программа Kaspersky Security Element осуществляет защиту компьютеров и отправляет отчеты администратору.

- Пользователь

  В этом режиме программа Kaspersky Security Element осуществляет защиту компьютеров, но не отправляет отчеты администратору.

Режим работы программы выбирается во время установки и может быть изменен позже.

Новости и специальные предложения

Теперь мы и наши партнеры предоставляем информационные материалы, например, о специальных предложениях "Лаборатории Касперского" или возникающих киберугрозах, прямо в интерфейсе программы.

> В случае получения программного обеспечения от компании-партнера "Лаборатории Касперского", оно может быть кастомизировано. В кастомизированном программном обеспечении могут быть недоступны некоторые параметры или функции. Более подробную информацию о кастомизированном программном обеспечении можно получить у компании-партнера.

Аппаратные и программные требования

Общие требования:

- Интернет-соединение (для обновления антивирусных баз и модулей программы; в случае если вы хотите запустить установку приложения в автоматическом режиме).

Минимальные требования для ноутбуков и настольных компьютеров:

- Свободное место на жестком диске: 350 МБ (в зависимости от размера антивирусных баз).
- Процессор: Intel Pentium III CPU 1 ГГц для 32-разрядных и 64-разрядных систем или совместимый аналог.
- Оперативная память: 1 ГБ для 32-разрядных систем, 2 ГБ для 64-разрядных систем.

Минимальные требования для планшетов:

- Microsoft Tablet PC.
- Процессор: Intel Celeron CPU 1.66 ГГц.
- Оперативная память: 1 ГБ.

Минимальные требования для нетбуков:

- Intel Atom CPU 1.60 ГГц и выше.
- Оперативная память: 1 ГБ для 32-разрядных систем, 2 ГБ для 64-разрядных систем.
- Диагональ дисплея – 10.1 дюйм, разрешением экрана 1024x600 пикселей.
- Видеокарта: Intel GMA 950 или совместимый аналог.

Поддерживаемые операционные системы:

- Microsoft Windows 10 Enterprise (RTM, Threshold 2, Redstone 1, Redstone 2, Redstone 3, Redstone 4, Redstone 5, 19H1, 19H2, 20H1, 20H2), 32-разрядные и 64-разрядные.
- Microsoft Windows 10 Pro (RTM, Threshold 2, Redstone 1, Redstone 2, Redstone 3, Redstone 4, Redstone 5, 19H1, 19H2, 20H1, 20H2), 32-разрядные и 64-разрядные.
- Microsoft Windows 10 Home (RTM, Threshold 2, Redstone 1, Redstone 2, Redstone 3, Redstone 4, Redstone 5, 19H1, 19H2, 20H1, 20H2), 32-разрядные и 64-разрядные.
- Microsoft Windows 8.1 Core (RTM и выше) / Pro (RTM и выше) / Enterprise (RTM и выше), 32-разрядные и 64-разрядные.
- Microsoft Windows 8 Core / Pro / Enterprise, 32-разрядные и 64-разрядные.
- Microsoft Windows 7 Home Basic (RTM и выше) / Home Premium (RTM и выше) / Professional (RTM и выше), 32-разрядные и 64-разрядные.
- Windows Server Standard / Enterprise / Datacenter 2008 R2/2012/2012 R2/2016/2019/2019 19H1/2019 19H2, 20H2

Совместимость с другими программами

Совместимость с другими программами "Лаборатории Касперского"

Программа Kaspersky Security Element не может быть установлена, если на вашем компьютере имеются другие программы "Лаборатории Касперского". При установке Kaspersky Security Element проверяет наличие на компьютере других программ "Лаборатории Касперского". При обнаружении таких программ, установка Kaspersky Security Element прекращается.

Совместимость с другими антивирусными программами

Программа Kaspersky Security Element не совместима с антивирусными программами для конечных пользователей. Программу Kaspersky Security Element можно использовать только с антивирусными программами для бизнеса.

Ограничения и предупреждения

Kaspersky Security Element имеет следующие известные ограничения:

- Программа не проверяет сертификат сервера SMTP при отправке отчетов администратору.
- Если для подключения к интернету используется прокси-сервер, то для отправки отчетов администратору SMTP-сервер должен находиться в локальной сети.
- В некоторых случаях программа не удаляет файлы, созданные вредоносными программами.
- Программа не удаляет и не восстанавливает файлы, используемые другим процессом.
- Программа не защищает и не восстанавливает файлы на устройствах хранения, имеющих файловую систему, отличную от NTFS.
- Программа не восстанавливает ключи реестра, созданные вредоносными программами.
- Программа не поддерживает файлы, зашифрованные шифрующей файловой системой (Encrypting File System, EFS).
- При завершении процессов и потоков процессов в результате действий вредоносных программ, операционная система может работать нестабильно.
- Программа откатывает все изменения файлов, сделанные во время анализа процесса.

- В некоторых случаях после удаления программы могут оставаться пустые папки.
- В редких случаях интерфейс программы может работать нестабильно, если программа используется в нескольких пользовательских сеансах. Эта проблема не влияет на уровень защиты.
- Отчеты содержат информацию только об обнаруженных объектах. Если не удается проверить объект, информация о нем не включается в отчет.
- При обновлении с версий beta1 и beta2, параметры программы не переносятся автоматически.
- Для работы функции "Доверенные устройства" необходимо включить функцию "Аудит входа в систему" в Windows.
- Программа не обнаруживает активность в общих папках легальных программ, которые могут использоваться для причинения вреда данным пользователя, а также рекламную активность.
- Программа может не определить точный IP-адрес или имя удаленного устройства, которое инициирует вредоносную активность в общих папках. Однако сеанс атакующего устройства будет заблокирован на время, указанное в параметрах программы.
- Программа контролирует изменения файлов, инициированные через интерфейс внутреннего замыкания на себя (при осуществлении сетевого доступа к общему ресурсу локальной файловой системы с той же рабочей станции, на которой расположен общий ресурс), только для запросов по протоколу SMB.
- Программа не контролирует изменения файлов, инициированные процессами, запущенными на уровне ядра операционной системы.
- В рамках процедуры отката файлы можно загружать из облачного хранилища в папку, указанную в параметрах облачного хранилища.
- В промежутке между установкой программы и перезагрузкой компьютера действует ограничение на откат файлов. Их число равняется 10.

Обработка данных

Данные, предоставляемые при использовании основных функций программы, перечислены в положениях и условиях использования сервиса.

Условия и положения использования Kaspersky Security Element

Чтобы ознакомиться с условиями предоставления сервиса, выполните следующие действия:

1. Откройте главное окно программы.
2. В меню программы выберите пункт **Поддержка**.
3. Нажмите на ссылке **Условия и положения**.

Откроются документы.

Эти документы в формате TXT также находятся в папке C:\Program Files\Kaspersky Lab\Kaspersky Anti-Ransomware Tool for Business 4.0. Если вы используете 64-разрядную операционную систему, документы находятся в папке C:\Program Files (x86)\Kaspersky Lab\Kaspersky Anti-Ransomware Tool for Business 4.0.

Чтобы предоставить вам информационные материалы в интерфейсе программы и повысить качество и удобство использования сервиса, "Лаборатория Касперского" может также обрабатывать следующие данные:

идентификатор устройства; семейство операционной системы; версия операционной системы, номер сборки операционной системы, номер обновления операционной системы, редакция операционной системы, расширенная информация о редакции операционной системы; версия запроса KSN о проверке репутации файла; идентификатор ПО, полученный из лицензии; полная версия ПО; идентификатор раздела справки ПО; идентификатор обновления ПО; локализация ПО; идентификатор установки ПО (PCID); идентификатор ребрендинга ПО; код партнерской организации, для которой был выполнен ребрендинг ПО; тип установленного ПО; группа ПО; имя ссылки; идентификатор запуска обновления ПО; обрабатываемый веб-адрес, наименование функции Продукта, события, произошедшие в сценарии использования контролируемой функции.

Для получения в интерфейсе программы информационных материалов "Лаборатории Касперского" и ее партнеров, вы предоставляете "Лаборатории Касперского" следующие данные:

информация о программе: тип, полная версия, уникальный идентификатор установщика, локализация, код партнерской организации, для которой был выполнен ребрендинг ПО; информация об оборудовании, установленном на компьютере: уникальный идентификатор компьютера с установленным ПО; информация об операционной системе, установленной на компьютере: тип, полная версия операционной системы и установленных пакетов обновления, разрядность, версия.

Кроме того, при обновлении программы, проверке настроенных параметров прокси-сервера или открытии ссылок из интерфейса программы, вы предоставляете "Лаборатории Касперского" данные в форме, которая сама по себе не устанавливает прямую связь с каким-либо конкретным лицом:

идентификатор программы; версия программы; идентификатор установщика программы; идентификатор запуска задачи обновления; полный номер версии программы; язык локализации программы; анонимный IP-адрес устройства пользователя (последний октет заменяется на 0); дата и время предоставления данных; идентификатор интерфейсной ссылки; тип интерфейсной ссылки; название компании-партнера "Лаборатории Касперского"; кастомизация программы; уникальный идентификатор установки.

Эти анонимные данные могут обрабатываться "Лабораторией Касперского" для повышения качества и удобства использования сервиса.

Ознакомьтесь также с разделом Запись событий работы программы, в котором описано использование файлов дампов и файлов журналов для устранения неполадок, поскольку эти файлы могут содержать персональные данные.

Установка и удаление программы

В этом разделе приведены пошаговые инструкции по установке и удалению программы Kaspersky Security Element.

Установка программы

Kaspersky Security Element устанавливается с помощью мастера установки, который обеспечивает выполнение всех этапов процесса установки. Для переходов между экранами мастера установки используйте кнопки **Назад** и **Далее**. По кнопке **Отмена** можно выйти из мастера установки.

Во время установки необходимо принять условия Лицензионного соглашения, Политики конфиденциальности и Дополнительного положения об обработке данных и выбрать режим работы программы.

Чтобы установить Kaspersky Security Element, выполните следующие действия:

1. Откройте установочный файл программы Kaspersky Security Element.

   Откроется мастер установки Kaspersky Security Element.

2. В открывшемся окне ознакомьтесь с Лицензионным соглашением, Политикой конфиденциальности и Дополнительным положением об обработке данных и выполните одно из следующих действий:

- Если вы согласны с условиями этих документов, подтвердите это, установив соответствующие флажки.

- Если вы не согласны с условиями этих документов, отмените установку Kaspersky Security Element и не используйте программу.

3. В открывшемся окне выберите пользователя программы. Если вы выбрали вариант **Пользователь (с отчетами по электронной почте)**, укажите адрес электронной почты и параметры подключения к SMTP-серверу.

4. Выберите типы объектов, обнаруживаемых и блокируемых программой.

5. Дождитесь завершения установки Kaspersky Security Element.

6. Если вы не хотите, чтобы программа Kaspersky Security Element запускалась автоматически после закрытия мастера установки, снимите флажок **Запустить Kaspersky Security Element**.

7. Нажмите на кнопку **Завершить**, чтобы завершить работу мастера установки.

   Программа Kaspersky Security Element успешно установлена на компьютер.

Обновление программы

Во время обновления мастер установки удаляет предыдущую версию Kaspersky Security Element и автоматически копирует настроенные параметры вашей программы.

> Убедитесь, что папка программы находится по заданному по умолчанию пути установки и доступна не только для чтения, чтобы мастер установки смог скопировать туда настроенные параметры.

Чтобы обновить Kaspersky Security Element, выполните следующие действия:

1. Загрузите последнюю версию программы.

2. Откройте установочный файл программы Kaspersky Security Element.

   Откроется мастер установки Kaspersky Security Element.

3. В открывшемся окне ознакомьтесь с Лицензионным соглашением, Политикой конфиденциальности и Дополнительным положением об обработке данных и выполните одно из следующих действий:

   - Если вы согласны с условиями этих документов, подтвердите это, установив соответствующие флажки.

- Если вы не согласны с условиями этих документов, отмените установку Kaspersky Security Element и не используйте программу.

4. Дождитесь завершения установки Kaspersky Security Element.

   Программа предложит вам перезагрузить компьютер.

5. Нажмите на кнопку **Перезагрузить сейчас**, чтобы завершить обновление.

   После перезагрузки компьютера программа Kaspersky Security Element обновится.

Удаление программы

Программу можно удалить с помощью мастера установки.

Чтобы удалить программу Kaspersky Security Element с компьютера, выполните следующие действия:

1. Откройте Панель управления одним из следующих способов:

   - Если вы используете Windows 7, в меню **Пуск** выберите **Панель управления**.
   - Если вы используете Windows 8 / Windows 8.1, нажмите сочетание клавиш **`Win + I`** и выберите пункт **Панель управления**.
   - Если вы используете Windows 10, откройте меню **Пуск** и начните вводить "панель". В результатах поиска выберите пункт **Панель управления**.

2. В открывшемся окне выберите **Программы и компоненты**.

3. В списке программ выберите Kaspersky Security Element и нажмите на кнопку **Удалить/Изменить**.

   Откроется мастер установки.

4. Нажмите на кнопку **Далее**.

5. При необходимости введите пароль.

   Начнется удаление Kaspersky Security Element.

6. Дождитесь завершения удаления Kaspersky Security Element.

7. Перезагрузите компьютер.

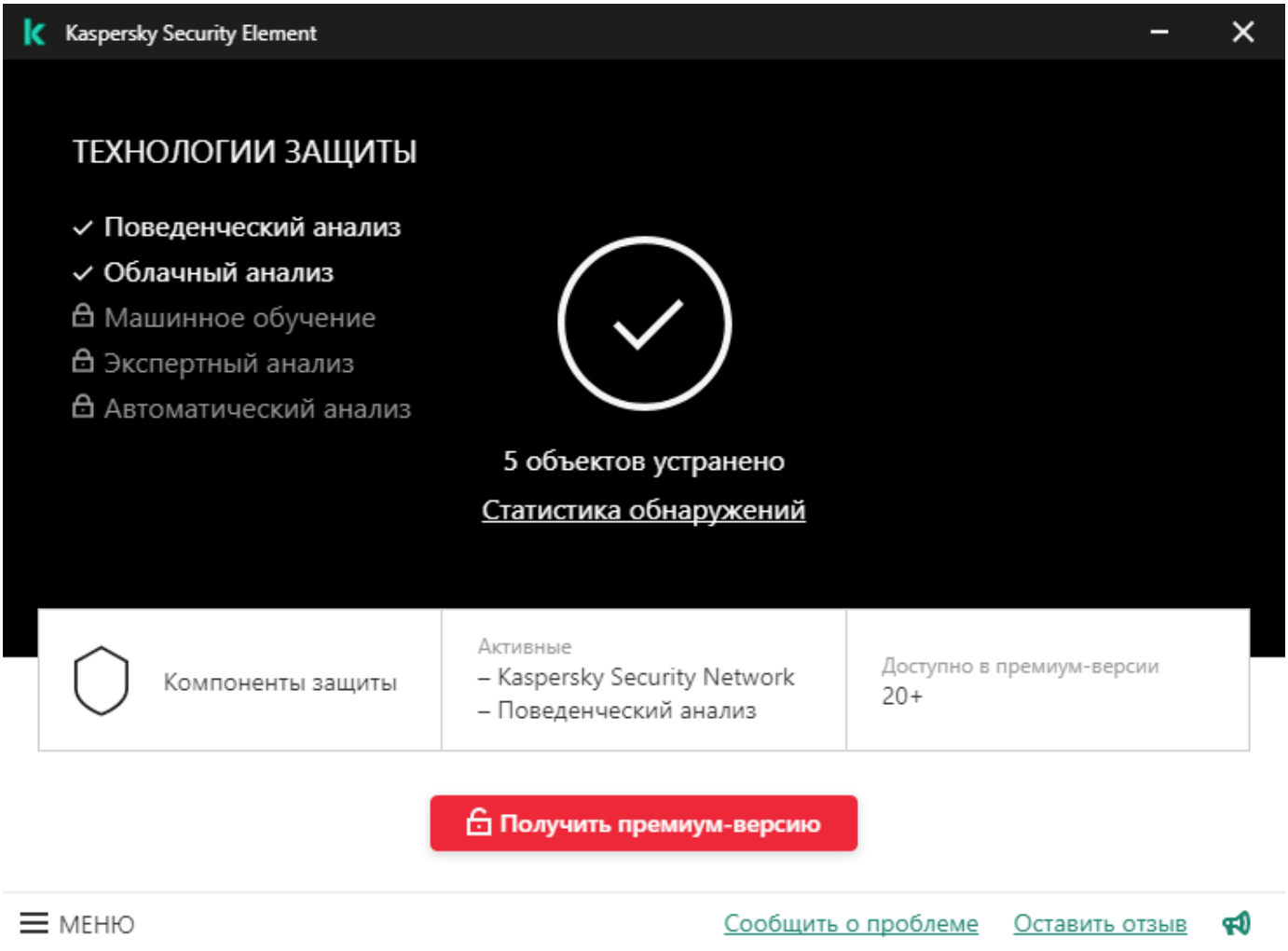
В некоторых случаях папка C:\Users\All Users\Kaspersky Lab\AntiRansom4 может остаться на компьютере после удаления программы.

Интерфейс программы

В этом разделе приведено описание основных элементов интерфейса программы.

Главное окно программы

В главном окне программы отображается информация о состоянии защиты и включенных технологиях защиты.



Главное окно программы

Главное окно программы содержит меню, позволяющее выполнять следующие действия:

- Просмотр статистики защиты и списка обнаруженных объектов
- Управление заблокированными программами
- Управление заблокированными устройствами
- Изменение режима работы программы
- Настройка и проверка параметров электронной почты

- Отправка отчетов администратору
- Настройка прокси-сервера
- Настройка функции Защита от эксплойтов
- Настройка защиты параметров паролем
- Получение технической поддержки
- Запись событий работы программы

Из главного окна программы можно также перейти на веб-сайт "Лаборатории Касперского" и получить Премиум-защиту для вашей компании, сообщить о проблеме на странице Поддержка на веб-сайте или оставить отзыв о программе Kaspersky Security Element.

Значок в нижней части главного окна показывает, что у вас есть непрочитанные новости от "Лаборатории Касперского".

Значок программы

После установки Kaspersky Security Element в области уведомлений панели задач появляется значок программы .

С помощью контекстного меню значка программы можно открыть главное окно программы, перейти к параметрам программы или выйти из программы Kaspersky Security Element.

Управление уведомлениями программы

Уведомления, отображаемые в области уведомлений панели задач, информируют вас о событиях программы, требующих вашего внимания.

Вы можете получить следующие уведомления:

- *Обнаруженные объекты* – программа Kaspersky Security Element обнаружила объект на компьютере.
- *Обнаруженные ранее объекты* – программа Kaspersky Security Element в течение последних 24 часов обнаружила объект на компьютере.
- *Действия, для которых выполнен откат* – программа Kaspersky Security Element обнаружила объект на компьютере и успешно откатила его действия.
- *Заблокированные устройства* – программа Kaspersky Security Element обнаружила удаленное устройство, пытающееся зашифровать общую папку, и заблокировала его

подключение к общей папке.

- *Предложения по установке* – преимущества программы Kaspersky Security Element и предложение установить программу на все компьютеры в компании. Вы можете отключить эти уведомления, установив флажок **Больше не показывать это сообщение** в окне уведомлений.

- *Недопустимые параметры программы* – предупреждение о том, что программа Kaspersky Security Element не может выполнить некоторые задачи из-за некорректных параметров прокси-сервера или SMTP-сервера. Эти уведомления могут содержать поля учетных записей или ссылку для открытия окна настройки параметров.

- *Результаты и предложения выполнить действия* – результаты проверки параметров прокси-сервера, отправки тестового сообщения, отправки отчета вручную; предложение перезагрузить компьютер, ввести пароль или принять обновленные соглашения.

- *Уведомления журнала* – информация о том, что включена запись событий программы в журнал.

- *Новости и специальные предложения* – информация о специальных предложениях от "Лаборатории Касперского" или возникающих киберугрозах.

- *Запросы обратной связи* – сообщения о том, что мы будем благодарны за ваши отзывы о программе.

Некоторые уведомления содержат ссылку **Получить премиум-версию** для перехода на веб-сайт "Лаборатории Касперского", где можно выбрать и приобрести средства премиум-защиты для компании.

Выполнение типовых задач

В этом разделе приведены пошаговые инструкции по выполнению типовых задач, реализованных в программе Kaspersky Security Element.

Управление программами

Вы можете разблокировать программы, которые были автоматически заблокированы Kaspersky Security Element, или переместить их в список доверенных программ, чтобы они не были заблокированы в будущем.

Чтобы разблокировать программу, выполните следующие действия:

1. Откройте главное окно программы.

2. В меню программы выберите пункт **Управление приложениями**.

3. В списке **Заблокированные приложения** выберите требуемую программу и нажмите **Разблокировать**.

   Программа будет удалена из списка заблокированных программ. В случае обнаружения подозрительной активности она может быть заблокирована повторно.

Чтобы переместить заблокированную программу в список доверенных программ, выполните следующие действия:

1. Откройте главное окно программы.
2. В меню программы выберите пункт **Управление приложениями**.
3. В списке **Заблокированные приложения** выберите требуемую программу и нажмите **Перенести в доверенные**.

   Программа будет удалена из списка заблокированных и появится в списке доверенных. Kaspersky Security Element не будет блокировать эту программу.

Чтобы добавить программу в список доверенных программ, выполните следующие действия:

1. Откройте главное окно программы.
2. В меню программы выберите пункт **Управление приложениями**.
3. В списке **Доверенные приложения** нажмите кнопку **Добавить** и укажите путь к файлу программы.

   Программа будет добавлена в список доверенных. Kaspersky Security Element не будет блокировать эту программу.

Чтобы удалить программу из списка доверенных программ, выполните следующие действия:

1. Откройте главное окно программы.
2. В меню программы выберите пункт **Управление приложениями**.
3. В списке **Доверенные приложения** выберите требуемую программу и нажмите **Удалить**.

   Программа будет удалена из списка доверенных программ.

Управление устройствами

Если удаленный компьютер попытается зашифровать общую папку, Kaspersky Security Element заблокирует доступ этого устройства к общей папке. Вы можете переместить удаленные устройства, которые были автоматически заблокированы Kaspersky Security Element, в список доверенных устройств, чтобы они не были заблокированы в будущем.

Чтобы переместить заблокированное устройство в список доверенных устройств, выполните следующие действия:

1. Откройте главное окно программы.
2. В меню программы выберите пункт **Управлять устройствами**.
3. В списке **Заблокированные устройства** выберите требуемое устройство и нажмите **Перенести в доверенные**.

   Устройство будет перемещено в список доверенных. Kaspersky Security Element не будет блокировать это устройство.

Чтобы добавить устройство в список доверенных устройств, выполните следующие действия:

1. Откройте главное окно программы.
2. В меню программы выберите пункт **Управлять устройствами**.
3. В списке **Доверенные устройства** нажмите на кнопку **Добавить** и укажите IP-адрес.
4. Нажмите на кнопку **ОК**.

   Устройство будет добавлено в список доверенных. Kaspersky Security Element не будет блокировать это устройство.

Чтобы удалить устройство из списка доверенных устройств, выполните следующие действия:

1. Откройте главное окно программы.
2. В меню программы выберите пункт **Управлять устройствами**.
3. В списке **Доверенные устройства** выберите требуемое устройство и нажмите **Удалить**.

   Устройство будет удалено из списка доверенных устройств.

Для работы функции "Доверенные устройства" в настройках Windows необходимо включить функцию "Аудит входа в систему".

Установка времени блокировки устройства

Если удаленное устройство попытается зашифровать общую папку, Kaspersky Security Element заблокирует доступ этого устройства к общей папке на время, указанное в параметрах программы.

Чтобы установить время блокировки устройства, выполните следующие действия:

1. Откройте главное окно программы.
2. В меню программы выберите пункт **Параметры**.

   Откроется окно **Параметры**.
3. Перейдите в раздел **Защита общих папок**.
4. Укажите количество минут, на которое требуется заблокировать соединение. Максимальное значение – 99 минут.
5. Сохраните изменения.

   Время блокировки будет установлено.

Просмотр информации об обнаруженных объектах

Чтобы просмотреть информацию об обнаруженных объектах, выполните следующие действия:

1. Откройте главное окно программы.
2. В меню программы выберите пункт **Статистика обнаружений**.

   Отобразится список обнаруженных объектов.
3. Нажмите на значок рядом с обнаруженным объектом, чтобы просмотреть подробную информацию об этом объекте.

Изменение режима работы программы

После установки Kaspersky Security Element можно изменить режим работы программы. При изменении режима работы программы все настроенные ранее параметры сохраняются.

Чтобы изменить режим работы программы, выполните следующие действия:

1. Откройте главное окно программы.
2. В меню программы выберите пункт **Параметры**.

   Откроется окно **Параметры**.
3. Перейдите в раздел **Режим**.
4. В разделе **Режим** выберите один из следующих режимов работы программы:

   - **Пользователь (с отчетами по электронной почте)**

При выборе этого режима необходимо настроить параметры электронной почты для отправки отчетов.

- **Пользователь**
- **Администратор**

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Настройка и проверка параметров электронной почты

Если вы используете Kaspersky Security Element в режиме **Пользователь (с отчетами по электронной почте)**, необходимо настроить параметры электронной почты для отправки отчетов администратору.

> В режимах **Пользователь** и **Администратор** настройка параметров электронной почты недоступна.

Чтобы настроить параметры электронной почты, выполните следующие действия:

1. Откройте главное окно программы.
2. В меню программы выберите пункт **Параметры**.

   Откроется окно **Параметры**.
3. Перейдите в раздел **Режим**.
4. В разделе **Параметры электронной почты** укажите следующие параметры:
   - Ваш адрес электронной почты.
   - Адрес электронной почты администратора.
   - Адрес или имя SMTP-сервера.
   - Порт SMTP-сервера.
5. При необходимости укажите имя и должность пользователя.
6. В раскрывающемся списке **Безопасность подключения** выберите тип зашифрованного подключения.
7. Если при подключении к почтовому серверу необходимо указать имя пользователя и пароль, установите флажок **Использовать аутентификацию** и укажите имя пользователя и

пароль для подключения к почтовому серверу.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

   После сохранения изменений можно отправить тестовое сообщение и проверить правильность параметров.

Никакие из этих данных не передаются в "Лабораторию Касперского". Они используется только для формирования и отправки отчетов системному администратору.

Чтобы проверить параметры электронной почты, выполните следующие действия:

1. Откройте главное окно программы.
2. В меню программы выберите пункт **Параметры**.

   Откроется окно **Параметры**.
3. Перейдите в раздел **Режим**.
4. В нижней части окна нажмите **Отправить тестовое сообщение**.

   Программа отправит тестовое сообщение, чтобы проверить правильность настроенных параметров электронной почты.

Отправка отчетов администратору

В режиме работы программы **Пользователь (с отчетами по электронной почте)** можно отправлять администратору отчеты о состоянии защиты вашего компьютера и обнаруженных на нем объектов. Отчеты можно отправлять вручную или настроить автоматическую отправку. По умолчанию программа Kaspersky Security Element отправляет отчеты каждый понедельник в 12:00.

В отчете содержится следующая информация:

- Имя пользователя
- Должность пользователя
- Название компьютера пользователя
- IP-адрес компьютера пользователя
- Название операционной системы пользователя
- Обнаруженные объекты

В режимах **Пользователь** и **Администратор** отправка отчетов недоступна.

Чтобы настроить расписание отправки отчетов, выполните следующие действия:

1. Откройте главное окно программы.
2. В меню программы выберите пункт **Параметры**.

   Откроется окно **Параметры**.
3. Перейдите в раздел **Режим**.
4. В разделе **Расписание отчетов** выберите периодичность отправки отчетов:

   - **Каждый месяц**. Можно указать день месяца и время отправки отчета.

     Имейте в виду, что количество дней в разных месяцах отличается. Например, если выбрать 30-й день месяца, отправка отчетов в феврале будет недоступна.

   - **Каждую неделю**. Можно указать день недели и время отправки отчета.
   - **Каждый день**. Можно указать время отправки отчета.
   - **Вручную**. Автоматическая отправка отчетов отключена.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

   Программа будет отправлять отчеты в соответствии с заданным расписанием.

Чтобы отправить отчет вручную, выполните следующие действия:

1. Откройте главное окно программы.
2. Убедитесь, что для параметра **Параметры > Режим > Расписание отчетов** задано значение **Вручную**.
3. В меню программы выберите пункт **Отправить отчет администратору**.

   Отчет будет отправлен администратору.

Настройка и проверка параметров прокси-сервера

Если вы используете прокси-сервер для подключения к интернету, необходимо указать параметры подключения к прокси-серверу.

По умолчанию программа автоматически пытается определить параметры прокси-сервера и подключиться к интернету. Если автоматически определить параметры прокси-сервере не удалось, программа запрашивает имя пользователя и пароль для аутентификации на прокси-сервере. Программа автоматически сохраняет указанные имя пользователя и пароль.

Чтобы настроить прокси-сервер, выполните следующие действия:

1. Откройте главное окно программы.
2. В меню программы выберите пункт **Параметры**.

   Откроется окно **Параметры**.
3. В разделе **Прокси-сервер** выберите один из следующих вариантов:

   - Если вы не хотите использовать прокси-сервер для подключения к интернету, выберите **Не использовать прокси-сервер**.
   - Если вы хотите, чтобы программа автоматически определяла параметры подключения к прокси-серверу, выберите **Автоматически определять параметры прокси-сервера**.
   - Если вы хотите указать параметры подключения к прокси-серверу вручную, выберите **Использовать указанные параметры прокси-сервера** и укажите адрес и порт, используемые при подключении к прокси-серверу.

     По умолчанию используется порт 0.
   - Если при подключении к прокси-серверу необходимо указать имя пользователя и пароль, установите флажок **Использовать аутентификацию на прокси-сервере** и укажите имя пользователя и пароль для подключения к прокси-серверу.
   - Если вы хотите использовать прокси-сервер только для внешних ресурсов, установите флажок **Не использовать прокси-сервер для локальных адресов**.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

   Параметры подключения к прокси-серверу будут сохранены.

Никакие из этих данных не передаются в "Лабораторию Касперского". Они используется только для формирования и отправки отчетов системному администратору.

Чтобы проверить параметры прокси-сервера, выполните следующие действия:

1. Откройте главное окно программы.
2. В меню программы выберите пункт **Параметры**.

Откроется окно **Параметры**.

3. В разделе **Прокси-сервер** нажмите на кнопку **Проверить параметры**.

   Программа установит тестовое соединение с серверами "Лаборатории Касперского". Результаты проверки отобразятся в новом окне.

Защита от эксплойтов

Эксплойты используют ошибки и уязвимости, чтобы вызвать нежелательное поведение программ. Kaspersky Security Element отслеживает подозрительные действия уязвимых программ и блокирует эти действия. Информация об обнаружении сохраняется в отчетах.

Защита памяти системных процессов

Некоторые программы, запущенные на компьютере пользователя, могут считывать память системных процессов (например, процесса lsaas.exe, который может хранить имена и пароли пользователей). Можно дополнительно защитить память системных процессов от чтения внешними процессами. Для этой функции информация об обнаружениях не сохраняется в отчетах и не отображается во всплывающих сообщениях.

Чтобы включить защиту от эксплойтов, выполните следующие действия:

1. Откройте главное окно программы.
2. В меню программы выберите пункт **Параметры**.

   Откроется окно **Параметры**.
3. В разделе **Защита от эксплойтов** включите переключатель **Блокировать эксплойты**.
4. При необходимости включите переключатель **Защищать память системных процессов**.
5. Нажмите на кнопку **Сохранить**.

   Функция будет включена.

Настройка защиты параметров программы паролем

Вы можете защитить параметры программы паролем, чтобы предотвратить несанкционированные или случайные изменения. Если программа Kaspersky Security Element защищена паролем, выход из нее и удаление (кроме удаления средствами KavRemover) также будет ограничено.

Чтобы настроить защиту параметров паролем, выполните следующие действия:

1. Откройте главное окно программы.
2. В меню программы выберите пункт **Параметры**.

   Откроется окно **Параметры**.
3. В разделе **Пароль администратора** включите переключатель **Параметры защиты паролем**.
4. Введите пароль, а затем и введите его повторно.

   > Пароль не должен быть пустым и содержать кавычки.
5. Нажмите на кнопку **Сохранить**.

   Параметры программы будут защищены паролем.

Разблокировать параметры программы

Чтобы разблокировать параметры программы, выполните следующие действия:

1. Откройте главное окно программы.
2. В меню программы выберите пункт **Параметры**.
3. Перейдите в раздел **Пароль администратора**.
4. В верхней части окна нажмите на ссылку **Ввести пароль**.
5. Введите пароль и нажмите на кнопку **Подтвердить**.

   > В результате будет разблокирован только открытый в данный момент раздел параметров. Чтобы разблокировать все параметры, установите флажок **Запомнить для этого сеанса**. Программа не будет запрашивать пароль до тех пор, пока она не будет перезапущена или пока не завершится сеанс пользователя Windows.
6. Отключите переключатель **Параметры защиты паролем**.
7. Нажмите на кнопку **Сохранить**.

   Параметры программы будут разблокированы. Пароль будет сброшен.

Изменить пароль

Чтобы изменить пароль администратора, выполните следующие действия:

1. Откройте главное окно программы.
2. В меню программы выберите пункт **Параметры**.
3. Перейдите в раздел **Пароль администратора**.
4. В верхней части окна нажмите на ссылку **Ввести пароль**.
5. Введите пароль и нажмите на кнопку **Подтвердить**.

   В результате будет разблокирован только открытый в данный момент раздел параметров. Чтобы разблокировать все параметры, установите флажок **Запомнить для этого сеанса**. Программа не будет запрашивать пароль до тех пор, пока она не будет перезапущена или пока не завершится сеанс пользователя Windows.

6. Введите новый пароль, а затем и введите его повторно.
7. Нажмите на кнопку **Сохранить**.

   Параметры программы будут защищены новым паролем.

Забыли пароль? Сбросить пароль

Чтобы сбросить пароль, выполните следующие действия:

1. Перезагрузите компьютер в безопасном режиме.
2. Войдите в систему с правами администратора.
3. Откройте реестр и выберите ключ **SettingsProtectionKey**.
4. Удалите этот ключ.

   Пароль будет сброшен. Параметры программы будут разблокированы.

Запись событий работы программы

Диагностическую информацию о событиях программы можно получить с помощью файлов дампов и файлов журналов. Эти файлы могут потребоваться Службе технической поддержки для устранения неполадок.

Файлы дампов отражают состояние рабочей памяти Kaspersky Security Element на момент создания этих файлов. Файлы дампов создаются автоматически при каждом сбое программы. Файлы дампов хранятся в папке %AllUsersProfile%\Kaspersky Lab\AntiRansom4\logs. Имена этих файлов имеют формат AntiRansom*.dmp, где * обозначает дополнительные сведения, такие как версия программы или дата и время создания файла.

Файлы журналов используются для записи подробной информации о действиях программы. По умолчанию ведение журнала событий программы отключено. Файлы журналов хранятся в папке %AllUsersProfile%\Kaspersky Lab\AntiRansom4\logs. Имена этих файлов имеют формат AntiRansom*.log, где * обозначает дополнительные сведения, такие как версия программы или дата и время создания файла.

Файлы журналов могут занимать много места на диске. Ведение журнала рекомендуется включать по запросу Службы технической поддержки. После сбора диагностической информации отключите ведение журнала, чтобы предотвратить нехватку места на диске.

Чтобы включить ведение журнала программы, выполните следующие действия:

1. Откройте главное окно программы.
2. В меню программы выберите пункт **Поддержка**.
3. Прокрутите вниз и нажмите на кнопку **Дополнительно**.
4. Установите флажок **Запись в журнал программы**.

   Когда флажок установлен, можно указать уровень детализации журналов.
5. В раскрывающемся списке **Уровень детализации** выберите одно из следующих значений:

   - **Рекомендуемый**.
   - **Все события**.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

   Kaspersky Security Element начнет запись событий программы.

Файлы дампов и журналов хранятся в незашифрованном формате и могут содержать конфиденциальные данные. Вы можете просмотреть содержимое этих файлов, открыв их в текстовом редакторе (например, Блокнот). При удалении программы файлы дампов и журналов удаляются без возможности восстановления. "Лаборатория Касперского" не осуществляет автоматический сбор файлов дампов и журналов.

Работа с программой из командной строки

В этом разделе описано, как управлять программой Kaspersky Security Element из командной строки.

Установка программы в автоматическом режиме

Программу Kaspersky Security Element можно установить в автоматическом режиме из командной строки. Перед установкой программы ознакомьтесь с условиями и положениями.

Чтобы установить программу в автоматическом режиме, выполните следующие действия:

1. Внимательно прочитайте следующие документы Лицензионное соглашение, Дополнительное положение об обработке данных и Политику конфиденциальности.

   - Если вы согласны с условиями и положениями этих документов, продолжайте установку программы.

   - Если вы не принимаете условия и положения документов, не устанавливайте и не используйте Kaspersky Security Element.

2. Запустите командную строку.

3. Введите команду `cd <путь к папке с установочным файлом>`.

4. Введите команду `<имя_установочного_файла.exe> /q AGREETOEULA=1 AGREETO_SUPPLEMENTAL_STATEMENT=1 AGREETOPRIVACYPOLICY=1 ADWARE_DETECT=1 <параметры>[=<значение>]`

   Описание параметров:

   - `/q` – включить автоматический режим.

   - `AGREETOEULA=1` – используйте этот параметр, если вы подтверждаете, что вы прочитали, понимаете и принимаете условия Лицензионного соглашения. Если вы не укажете этот параметр, программа Kaspersky Security Element не будет установлена.

- `AGREETO_SUPPLEMENTAL_STATEMENT=1` – используйте этот параметр, если вы подтверждаете, что вы прочитали, понимаете и принимаете условия Дополнительного положения об обработке данных. Если вы не укажете этот параметр, программа Kaspersky Security Element не будет установлена.

- `AGREETOPRIVACYPOLICY=1` – используйте этот параметр, если вы подтверждаете, что понимаете и соглашаетесь с тем, что ваши данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности, а также подтверждаете, что полностью прочитали и понимаете Политику конфиденциальности. Если вы не укажете этот параметр, программа Kaspersky Security Element не будет установлена.

- `ADWARE_DETECT=1` – включить обнаружение рекламных или прочих легальных программ, которые могут быть использованы для нанесения вреда вашим данным. Вы можете отключить эту функцию и обнаруживать только вредоносные программы, указав `ADWARE_DETECT=0`. Если вы не укажете этот параметр, программа Kaspersky Security Element не будет установлена.

- `<параметры>` – укажите дополнительные параметры.

> Все параметры чувствительны к регистру символов. Код ошибки `ErrorCode: 253` вместе с ошибкой MSI свидетельствует о том, что в команде использовался некорректный синтаксис. Ознакомьтесь с этими инструкциями и попробуйте снова.

5. Дождитесь окончания установки.

   После завершения установки на рабочем столе появится значок Kaspersky Security Element.

Обновление программы в автоматическом режиме

Программу Kaspersky Security Element можно обновить в автоматическом режиме из командной строки. Перед обновлением программы ознакомьтесь с условиями и положениями.

Чтобы обновить программу в автоматическом режиме, выполните следующие действия:

1. Внимательно прочитайте следующие документы Лицензионное соглашение, Дополнительное положение об обработке данных и Политику конфиденциальности.

   - Если вы согласны с условиями и положениями этих документов, продолжайте обновление программы в автоматическом режиме.

   - Если вы не принимаете условия и положения документов, не обновляйте Kaspersky Security Element.

2. Запустите командную строку.

3. Введите команду `cd <путь к папке с установочным файлом>`.

4. Введите команду `<имя_установочного_файла.exe> /q AGREETOEULA=1 AGREETO_SUPPLEMENTAL_STATEMENT=1 AGREETOPRIVACYPOLICY=1 ADWARE_DETECT=1 REBOOTCOMPUTER=1 <параметры>[=<значение>]`

   Описание параметров:

   - `/q` – включить автоматический режим.
   - `AGREETOEULA=1` – используйте этот параметр, если вы подтверждаете, что вы прочитали, понимаете и принимаете условия Лицензионного соглашения. Если вы не укажете этот параметр, программа Kaspersky Security Element не будет установлена.
   - `AGREETO_SUPPLEMENTAL_STATEMENT=1` – используйте этот параметр, если вы подтверждаете, что вы прочитали, понимаете и принимаете условия Дополнительного положения об обработке данных. Если вы не укажете этот параметр, программа Kaspersky Security Element не будет установлена.
   - `AGREETOPRIVACYPOLICY=1` – используйте этот параметр, если вы подтверждаете, что понимаете и соглашаетесь с тем, что ваши данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности, а также подтверждаете, что полностью прочитали и понимаете Политику конфиденциальности. Если вы не укажете этот параметр, программа Kaspersky Security Element не будет установлена.
   - `ADWARE_DETECT=1` – включить обнаружение рекламных или прочих легальных программ, которые могут быть использованы для нанесения вреда вашим данным. Вы можете отключить эту функцию и обнаруживать только вредоносные программы, указав `ADWARE_DETECT=0`. Если вы не укажете этот параметр, программа Kaspersky Security Element не будет установлена.
   - `REBOOTCOMPUTER=1` – перезагрузить компьютер, чтобы завершить обновление. Чтобы перезагрузить компьютер вручную, укажите значение `REBOOTCOMPUTER=0`.
   - `<параметры>` – укажите дополнительные параметры.

   > Все параметры чувствительны к регистру символов. Код ошибки `ErrorCode: 253` вместе с ошибкой MSI свидетельствует о том, что в команде использовался некорректный синтаксис. Ознакомьтесь с этими инструкциями и попробуйте снова.

5. Перезагрузите компьютер.

   Программа будет обновлена.

Если вам необходимо сначала экспортировать параметры программы, запустите файл anti_ransom_gui.exe, находящийся в папке программы, с параметром `exportsettings`. Параметры будут экспортированы в файл c:\ProgramData\Kaspersky Lab\AntiRansom4\protected\settings_storage.xml.

При обновлении программы флаг реестра `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\AntiRansom4]` меняется на `"UpgradeFlag"=dword:00000001`.

Удаление программы в автоматическом режиме

Программу Kaspersky Security Element можно удалить в автоматическом режиме из командной строки.

Чтобы удалить программу в автоматическом режиме, выполните следующие действия:

1. Запустите командную строку.
2. Введите команду `cd <путь к папке с установочным файлом>`.
3. Введите команду `<имя_установочного_файла.exe> /q REMOVE=ALL`
4. Если вы ранее устанавливали пароль, вы должны указать его в команде с помощью параметра PROTECTION_PASSWORD.
5. Для полного удаления программы компьютер перезагрузится автоматически. Чтобы автоматическая перегрузка компьютера не выполнялась, используйте дополнительный параметр REBOOTCOMPUTER. Для этого введите команду `<имя_установочного_файла.exe> /q REMOVE=ALL REBOOTCOMPUTER=0`.

   Все параметры чувствительны к регистру символов. Код ошибки `ErrorCode: 253` вместе с ошибкой MSI свидетельствует о том, что в команде использовался некорректный синтаксис. Ознакомьтесь с этими инструкциями и попробуйте снова.

   Программа будет удалена.

Настройка параметров программы из командной строки

При установке и обновлении программы в автоматическом режиме вы можете использовать в командах перечисленные в следующей таблице параметры.

Используйте следующий формат: `<параметры>[=<значение>]`. Например, `POSITION=Admin`

Если значения параметров содержат пробелы, заключите эти значения в двойные кавычки. Например, `POSITION="Младший разработчик"`

Настройка параметров программы из командной строки

Имя	Описание	Доп
AGREETOEULA	Принять условия Лицензионного соглашения.	0 – о 1 – пр
AGREETO_SUPPLEMENTAL_STATEMENT	Принять условия Дополнительного положения об обработке данных.	0 – о 1 – пр
AGREETOPRIVACYPOLICY	Принять условия Политики конфиденциальности.	0 – о 1 – пр
ADWARE_DETECT	Включить обнаружение рекламных программ и подозрительных процессов.	0 – о 1 – пр
USER_MODE	Выбрать режим работы.	0 – П отчет элект 1 – По 2 – А,
USER	Имя пользователя.	Прои
POSITION	Должность пользователя.	Прои
ADMIN_EMAIL	Адрес электронной почты для отправки отчетов.	Адре почты
SENDER_EMAIL	Адрес электронной почты, с которого будут отправляться отчеты.	Адре почты
SMTP_SERVER	Адрес SMTP-сервера.	IP-ад серве
SMTP_PORT	Порт SMTP-сервера.	Допу – 655 умол
CONNECTION_SECURITY	Тип зашифрованного соединения для отправки сообщений электронной почты.	0 – не соеди умол 1 – ST

		2 – S
NEED_AUTHENTICATION	Требуется ли аутентификация на SMTP-сервере.	0 – ау треб умол 1 – тр аутен
EMAIL_USER	Имя пользователя для аутентификации на SMTP-сервере.	Прои
EMAIL_USER_PASSWORD	Пароль для аутентификации на SMTP-сервере.	Прои
REPORTS_TYPE	Тип расписания отчетов.	manu автом отпра откл week отпра автом в нед умол mont отпра автом в мес daily - отпра автом день
REPORTS_DAY	День, в который выполняется автоматическая отправка отчетов.	[1-7], значе REPC [1-31] значе REPC
REPORTS_TIME	Время, когда выполняется автоматическая отправка отчетов (в 24-часовом формате).	[00-2 По ум отпра
PROXY_TYPE	Тип использования прокси-сервера.	auto -

	Если задано значение PROXY_TYPE = manually, необходимо указать параметры PROXY_HOST и PROXY_PORT.	прок опре авто умол manu прок необ вруч none не ис
PROXY_HOST	Адрес прокси-сервера.	Прои
PROXY_PORT	Порт, используемый для подключения к прокси-серверу.	[0-65
PROXY_AUTH_LOGIN	Имя пользователя для подключения к прокси-серверу.	Прои
PROXY_AUTH_PASSWORD	Пароль для подключения к прокси-серверу.	Прои
PROXY_LOCAL_ADDRESS	Будет ли использоваться прокси-сервер для локальных адресов.	0 – пр испол 1 – пр испол умол
MIGRATE_SETTINGS	Включить или отключить перенос настроенных параметров из предыдущей версии программы. Если перенос параметров включен (или значение не указано), то при обновлении программы в автоматическом режиме для команды будут использоваться только параметры, которые всегда обязательно указывать (AGREETOEULA, AGREETO_SUPPLEMENTAL_STATEMENT, AGREETOPRIVACYPOLICY, ADWARE_DETECT). Необязательные и относительно-обязательные значения параметров будут скопированы из установленной ранее версии программы.	0 – от 1 – вк умол
REBOOTCOMPUTER	Перезагрузить компьютер после удаления или обновления программы.	0 – не 1 – пе

PROTECTION_PASSWORD	Защита параметров программы паролем. Пароль не должен быть пустым и содержать кавычки.	Прои строк
PROTECTION_PASSWORD_PATH	Локальный или сетевой путь к TXT-файлу с паролем для защиты параметров программы.	Прои строк

В следующей таблице описаны конкретные значения параметров, предназначенные для внутреннего использования в "Лаборатории Касперского". При изменении заданных по умолчанию значений этих параметров корректная установка и работа программы не гарантируется.

Параметры программы для внутреннего использования

Имя	Описание	Значение по умолчанию
INSTALLDIR	Внутренний параметр для изменения заданного по умолчанию пути установки программы.	По умолчанию для 64-разрядной операционной системы используется путь: C:\Program Files (x86)\Kaspersky Lab\Kaspersky Anti-Ransomware Tool for Business 4.0.
SELFPROTECTION	1 – включить / 0 – выключить самозащиту.	По умолчанию самозащита включена.
RUNAPP	1 – запустить / 0 – не запускать программу после установки в автоматическом режиме.	По умолчанию программа запускается.
/log <путь к папке>	Создать файлы журналов установщика программы и установщика MSI в указанной папке. Используются следующие имена файлов: "kart_installer_%m.%d_%H.%M.INST.log"; "kart_installer_%m.%d_%H.%M.MSI.log"; m – месяц, d – день, H – часы, M – минуты.	Не задано

Все параметры чувствительны к регистру символов. Код ошибки `ErrorCode: 253` вместе с ошибкой MSI свидетельствует о том, что в команде использовался некорректный синтаксис. Ознакомьтесь с этими инструкциями и попробуйте снова.

Параметр IS_ADMIN больше не поддерживается. Вместо этого используйте параметр USER_MODE.

Если вы не укажете необязательные параметры, программа Kaspersky Security Element будет установлена со значениями этих параметров, заданными по умолчанию.

Просмотр справки из командной строки

Если вы используете некорректный синтаксис команд при работе с программой из командной строки, например, если вы не указали обязательные параметры, программа вернет код ошибки `ErrorCode: 253` вместе с ошибкой MSI и ссылкой на соответствующую статью в справке.

Чтобы вызвать справку из командной строки

1. Запустите командную строку.
2. Введите команду `cd <путь к папке с установочным файлом>`.
3. Введите команду `<имя_установочного_файла.exe> /q`

   Отобразится ссылка на справку.

Получение технической поддержки

Если у вас возникли проблемы при работе с программой Kaspersky Security Element, вы можете выбрать один из следующих вариантов поддержки, предоставляемых "Лабораторией Касперского":

- Расширенная поддержка
- Сообщество
- База знаний
- Онлайн-справка

Чтобы открыть список вариантов поддержки, выполните следующие действия:

1. Откройте главное окно программы.
2. В меню программы выберите пункт **Поддержка**.

   В результате откроется окно, содержащее варианты поддержки.

Оставить отзыв

Поделитесь, что вы думаете о программе Kaspersky Security Element, или просто оцените программу. У нас может не быть возможности немедленно ответить вам или решить вашу проблему, но мы ценим любые отзывы и стремимся сделать наши продукты лучше.

Чтобы оставить отзыв,

перейдите по ссылке **Оставить отзыв** в главном окне программы и заполните форму обратной связи.

Пожалуйста, заполните также Опрос удовлетворенности клиентов. Ссылка на опрос находится в окне отзыва.

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

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

Internet Explorer, Microsoft, Windows и Windows Server – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

JavaScript – зарегистрированный товарный знак компании Oracle и/или аффилированных компаний.

ДОПОЛНИТЕЛЬНОЕ ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ ДАННЫХ (ДОПОЛНИТЕЛЬНОЕ ПОЛОЖЕНИЕ)

ДОПОЛНИТЕЛЬНОЕ ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ ДАННЫХ (ДОПОЛНИТЕЛЬНОЕ ПОЛОЖЕНИЕ)

Дополнительное Положение (далее – Положение) относится к программному обеспечению Kaspersky Security Element (далее – ПО).

Все используемые в настоящем Положении определения имеют значения, указанные в Разделе «Определения» Лицензионного соглашения.

Настоящее Положение совместно с Лицензионным соглашением для ПО, в частности в разделе «Условия обработки данных», определяют условия, ответственность и порядок передачи и обработки данных, указанных в настоящем Положении.

Внимательно ознакомьтесь с условиями Положения, а также со всеми документами, ссылки на которые содержит Положение, перед тем, как принять его.

Если Пользователь использует ПО, то Пользователь несет ответственность за обеспечение законности обработки персональных данных Субъектов данных, которая определена в применимых законах о конфиденциальной информации, персональных данных, защите данных или аналогичных законах.

Защита и обработка данных

Все данные, получаемые и обрабатываемые Правообладателем при использовании Вами ПО, защищаются и обрабатывается в соответствии с Политикой конфиденциальности Правообладателя, опубликованной по адресу: https://www.kaspersky.com/Products-and-Services-Privacy-Policy.

Цели обработки данных

Использование ПО позволяет защищать Пользователя от известных угроз информационной безопасности, как указано в Руководстве Пользователя. Обработка данных, указанных в настоящем Положении, может повысить эффективность защиты, предоставляемой ПО, от угроз информационной и сетевой безопасности.

Заявленная цель достигается посредством:

- определения репутации проверяемых объектов;

- выявления новых и сложных для обнаружения угроз информационной и сетевой безопасности, а также их источников;

- оперативного принятия мер по повышению уровня защиты информации, хранимой и обрабатываемой Пользователем с использованием Компьютера;

- уменьшения вероятностей ложных срабатываний;

- повышения эффективности работы компонентов ПО;

- предотвращения инцидентов информационной безопасности и расследования возникших инцидентов;

- улучшения качества работы продуктов Правообладателя;

- получения справочной информации о количестве объектов с известной репутацией.

Обрабатываемые данные

При использовании ПО Правообладатель будет получать и обрабатывать следующие данные в автоматическом режиме:

- содержимое фрагмента в обрабатываемом объекте;

- дата и время истечения сертификата;

- дата и время выдачи сертификата;

- версия списка отозванных заключений службы ПО;

- количество циклов обновления и применения антивирусных баз;

- дата и время последнего обновления и применения антивирусных баз;

- версия записи в базе данных ПО;

- идентификатор сработавшей записи в антивирусных базах ПО;

- временная метка сработавшей записи в антивирусных базах ПО;

- тип сработавшей записи в антивирусных базах ПО;

- дата и время выпуска баз ПО;

- идентификатор устройства;

- информация о потреблении ПО системной памяти;

- версия ОС, номер сборки ОС, номер обновления ОС, редакция ОС, расширенная информация о редакции ОС;

- идентификатор ОС;

- версия пакета обновления ОС;

- дата и время запуска ОС;

- признак включения компонента Device Guard (windows);

- IP-адрес;

- разрядность операционной системы;

- версия установленной операционной системы на компьютере пользователя;

- идентификатор ключа из хранилища ключей, используемого для шифрования;

- протокол, используемый для передачи данных в KSN;

- характеристики шифрования пакета данных, отправляемых в KSN;

- идентификатор пакета данных, отправляемых в KSN;

- идентификатор языка ПО;

- порядковый номер фрагмента в обрабатываемом объекте;

- данные внутреннего журнала, сформированного антивирусным компонентом ПО для обрабатываемого объекта;

- содержимое обрабатываемого цифрового сертификата;

- наименование эмитента сертификата;

- публичный ключ сертификата;

- алгоритм вычисления публичного ключа сертификата;

- серийный номер сертификата;

- дата и время подписи объекта;

- имя и параметры владельца сертификата;

- отпечаток цифрового сертификата проверяемого объекта и алгоритм хеширования;

- дата и время последней модификации обрабатываемого объекта;

- дата и время создания обрабатываемого объекта;

- характеристики обнаружения;

- обрабатываемые объекты или их части;

- описание обрабатываемого объекта, указанное в его свойствах;

- формат обрабатываемого объекта;

- тип контрольной суммы обрабатываемого объекта;

- контрольная сумма (MD5) обрабатываемого объекта;

- имя обрабатываемого объекта;

- название ПО;

- контрольная сумма (SHA256) обрабатываемого объекта;

- размер обрабатываемого объекта;

- название обнаруженной вредоносной программы или легальной программы, которая может быть использована для нанесения вреда устройству или данным пользователя;

- название продавца ПО;

- заключение ПО по обрабатываемому объекту;

- версия обрабатываемого объекта;

- источник заключения по обрабатываемому объекту;

- контрольная сумма обрабатываемого объекта;

- имя приложения, частью которого является обрабатываемый объект;

- результат проверки подписи модуля, целостность которого проверяется ПО;

- путь к обрабатываемому объекту;

- код каталога файлов;

- информация о результатах проверки подписи файла;

- разрядность ОС;

- редакция ОС;

- дата и время запуска компонента мониторинг активности;

- версия компонента ПО;

- полная версия ПО;

- идентификатор обновления ПО;

- дата и время установки ПО;

- идентификатор установки ПО (PCID);

- статус работоспособности ПО после обновления;

- тип установленного ПО;

- формат данных в запросе к инфраструктуре Правообладателя;

- идентификатор компонента ПО;

- ключ сеанса входа;

- алгоритм шифрования ключа сеанса входа;

- признак принятия пользователем условий юридического соглашения в ходе использования ПО;

- тип юридического соглашения, условия которого были приняты пользователем в ходе использования ПО;

- дата и время согласия пользователя с условиями юридического Соглашения в ходе использования ПО;

- версия юридического соглашения, условия которого были приняты пользователем в ходе использования ПО;

- имя модуля, в котором предположительно произошел сбой;

- код ребрендинга ПО;

- вероятность отправки статистики компонентом мониторинг активности;

- код события, обрабатываемого компонентом мониторинг активности дольше стандартного времени обработки;

- время обработки события в базах, обработка которого компонентом мониторинг активности длилась дольше стандартного времени;

- время задержки обработки события о совершении действия в ОС в подсистеме поведенческого анализа;

- количество задержанных событий текущего типа, совершенных в ОС;

- максимально допустимое время обработки события компонентом мониторинг активности;

- время задержки обработки события о совершении действия в ОС в подсистеме проактивной защиты;

- количество обработанных событий, совершенных в ОС;

- количество обработанных синхронных событий, совершенных в ОС;

- суммарная задержка всех событий текущего типа, совершенных в ОС;

- время задержки обработки события о совершении действия в ОС в подсистеме постоянного хранения событий;

- время обработки события, обработка которого компонентом мониторинг активности длилась дольше стандартного времени;

- общее количество событий, обработка которых компонентом мониторинг активности длилась дольше стандартного времени;

- суммарная задержка всех событий, совершенных в ОС;

- количество ожидающих синхронных событий, совершенных в ОС;

- дата и время обнаружения стороннего ПО компонентом мониторинг активности;

- номер обнаруженного ПО в контексте компонента мониторинг активности;

- причина обнаружения стороннего ПО компонентом мониторинг активности;

- дата и время получения события о совершении действия в ОС;

- код события, обрабатываемого компонентом мониторинг активности, которое переполнило очередь событий;

- количество событий, обрабатываемых компонентом мониторинг активности, которые переполнили очередь событий;

- общее количество переполнений очереди событий, обрабатываемых компонентом мониторинг активности;

- разница во времени между наступлением первого события в очереди и текущим событием на момент отправки пакета статистики компонентом мониторинг активности;

- тип события, обработка которого была прервана по тайм-ауту (klif-событие/swmon-событие);

- старший и младший номер фильтра перехвата, осуществившего перехват, обработка которого компонентом мониторинг активности была прервана по тайм-ауту;

- идентификатор перехвата, обработка которого была прервана по тайм-ауту в подсистеме мониторинг активности;

- количество klif-событий, которые наступили по тайм-ауту на момент отправки пакета статистики компонентом мониторинг активности;

- размер очереди событий, обрабатываемых компонентом мониторинг активности, обработка которых была прервана по тайм-ауту;

- количество событий компонента Монитор Активности, которые наступили по тайм-ауту на момент отправки пакета статистики компонентом мониторинг активности;

- время работы стороннего ПО до сбоя;

- адрес памяти со смещением, в котором произошёл сбой стороннего ПО;

- информация о сбое в стороннем ПО;

- название ошибки из системного журнала, произошедшей в стороннем ПО;

- время хранения обрабатываемого объекта;

- алгоритм расчета отпечатка цифрового сертификата;

- число неуспешеных завершений установки обновления для компонента обновления;

- число ошибок установки обновления для компонента обновления;

- код ошибки задачи обновления;

- тип задачи обновления;

- версия компонента обновления;

- адрес веб-службы, на который осуществлялось обрабатываемое обращение (веб-адрес, IP);

- номер порта;

- веб-адрес источника запроса к веб-службе (referer);

- обрабатываемый веб-адрес.

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», ОПРЕДЕЛЯЮЩЕЕ УСЛОВИЯ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (ПО)

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ для Kaspersky Security Element

ВНИМАНИЕ! ВНИМАТЕЛЬНО ОЗНАКОМЬТЕСЬ С УСЛОВИЯМИ ЛИЦЕНЗИОННОГО СОГЛАШЕНИЯ ПЕРЕД НАЧАЛОМ РАБОТЫ С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ.

НАЖАТИЕ ВАМИ КНОПКИ ПОДТВЕРЖДЕНИЯ СОГЛАСИЯ В ОКНЕ С ТЕКСТОМ ЛИЦЕНЗИОННОГО СОГЛАШЕНИЯ ПРИ УСТАНОВКЕ ПО ИЛИ ВВОД СООТВЕТСТВУЮЩЕГО СИМВОЛА(-ОВ) ОЗНАЧАЕТ ВАШЕ БЕЗОГОВОРОЧНОЕ СОГЛАСИЕ С УСЛОВИЯМИ НАСТОЯЩЕГО ЛИЦЕНЗИОННОГО СОГЛАШЕНИЯ. ЕСЛИ ВЫ НЕ СОГЛАСНЫ С УСЛОВИЯМИ НАСТОЯЩЕГО ЛИЦЕНЗИОННОГО СОГЛАШЕНИЯ, ВЫ ДОЛЖНЫ ПРЕРВАТЬ УСТАНОВКУ ПО.

1. Определения

1.1. ПО – программное обеспечение, сопроводительные материалы, обновления, описанные в Руководстве Пользователя, Правообладателем которых является АО «Лаборатория Касперского».

1.2. Правообладатель (обладатель исключительного права на ПО) – АО «Лаборатория Касперского».

1.3. Компьютер(ы) — операционная система, виртуальная машина или оборудование, для работы на котором предназначено ПО, на которое устанавливается ПО и/или на котором используется ПО.

1.4. Пользователь (Вы) — юридическое лицо, для которого ПО было загружено или приобретено, и которое поручило отдельному физическому лицу принять данное соглашение от своего имени.

1.5. Обновление(-я) — все улучшения, исправления, расширения, пакеты обновлений, копии и/или модификации ПО.

1.6. Руководство Пользователя – сопроводительные печатные и иные материалы, руководство пользователя, руководство администратора, справочник, файл справки и аналогичные им печатные и электронные документы.

Электронная версия Руководства Пользователя доступна на веб-сайте Правообладателя: https://help.kaspersky.ru. Правообладатель оставляет за собой право обновлять электронную версию Руководства Пользователя на вышеуказанном сайте в случае необходимости.

2. Предоставление лицензии

2.1. Правообладатель предоставляет Вам неисключительную лицензию на использование ПО в пределах функциональности описанной в Руководстве Пользователя.

2.2. Вы имеете право изготовить копию ПО при условии, что эта копия предназначена только для архивных целей и для замены правомерно приобретенного экземпляра в случаях, когда оригинал утерян, уничтожен или стал непригоден для использования. Такая копия не может быть использована для иных целей и должна быть уничтожена в случае, если владение экземпляром ПО перестанет быть правомерным.

2.3. После установки ПО Вам предоставляется возможность в течение указанного Срока получать от Правообладателя:

- новые версии ПО по мере их выхода (через Интернет). Все получаемые Вами обновления становятся частью ПО, и к ним применяются положения и условия настоящего Соглашения;

- техническую поддержку, указанную в п.4;

- доступ к информационным и вспомогательным ресурсам Правообладателя.

3. Срок и его истечение

3.1. ПО может быть использовано после принятия условий данного Лицензионного соглашения в течение периода, указанного по адресу: https://support.kaspersky.com/corporate/lifecycle.

3.2. В случае нарушения Вами какого-либо из условий данного Лицензионного соглашения Правообладатель вправе прервать действие данного Лицензионного соглашения на использование ПО в любое время без Вашего уведомления.

3.3. Вы соглашаетесь, что при использовании ПО и использовании любого отчета или информации, полученной в результате использования данного ПО, вы будете соблюдать все применимые международные, национальные, государственные, региональные и местные законы и правила, включая, без ограничений, закон о конфиденциальности, авторском праве, экспортном контроле и непристойном поведении.

4. Техническая поддержка

4.1. Техническая поддержка, указанная в п. 2.3 настоящего Лицензионного соглашения, предоставляется в соответствии с правилами оказания Технической поддержки.

Адрес службы технической поддержки и правила ее оказания: https://support.kaspersky.com.

5. Условия обработки данных

5.1. В рамках данного Раздела вводятся дополнительные определения:

Субъект данных – физическое лицо, которое использует или будет использовать ПО напрямую или косвенно при осуществлении Пользователем своей деятельности, в том числе работник, подрядчик, сотрудник, клиент или представитель Пользователя, и в отношении которого осуществляется передача и обработка данных, включая данные, имеющие статус персональных по законодательству некоторых стран. Субъектами данных могут также выступать любые физические лица, которые сообщают или передают свои данные Пользователю.

5.2. Правообладатель осуществляет обработку всех полученных от Пользователя данных в соответствии с Лицензионным соглашением, в частности положениями раздела 5 «Условия обработки данных», а также в соответствии с функциональностью ПО, которую Пользователь может использовать, если иное не указано в отдельном письменном соглашении между Пользователем и Правообладателем или его Партнерами.

5.3. Пользователь принимает на себя обязательство за полное ознакомление с Руководством Пользователя, особенно в отношении обработки данных, с Политикой конфиденциальности Правообладателя, которая описывает обработку данных (https://www.kaspersky.com/Products-and-Services-Privacy-Policy), и принятие решения о соответствии ПО требованиям Пользователя.

5.4. При использовании ПО Пользователь должен соблюдать применимые законы, включая законы о конфиденциальной информации, персональных данных и о защите данных. При использовании компонентов ПО, которые обрабатывают данные без их передачи Правообладателю, Пользователь несет ответственность за обеспечение и поддержание конфиденциальности и мер безопасности в отношении данных. Пользователь должен определить соответствующие технические и организационные меры для защиты данных и обеспечения их конфиденциальности при использовании таких компонентов ПО.

5.5. Во время использования ПО Пользователь несет ответственность за обеспечение законности обработки персональных данных Субъектов данных, которая определена в применимых законах о конфиденциальной информации, персональных данных, защите данных или аналогичных законах.

5.6. В том случае, если Пользователь принимает решение получать согласие от Субъектов данных для обеспечения законности обработки, Пользователь должен перед началом использования ПО получить согласие каждого Субъекта данных в соответствии со всеми требованиями применимого законодательства. Пользователь должен получать согласие от каждого Субъекта данных до начала обработки персональных данных такого Субъекта данных.

5.7. В отношении п. 5.6 настоящего Лицензионного соглашения Пользователь должен иметь подтверждения наличия согласия на обработку персональных данных. Пользователь обязуется предоставить подтверждения наличия такого согласия каждого Субъекта данных по запросу Правообладателя в течение 5 (пяти) рабочих дней после получения запроса.

5.8. В отношении п. 5.6 настоящего Лицензионного соглашения, до начала использования ПО Пользователь обязуется и несет полную ответственность за предоставление каждому отдельному Субъекту данных всей информации, требуемой в соответствии с применимым законодательством, для получения согласия на обработку персональных данных. В частности, Пользователь до начала использования ПО обязан предоставить каждому Субъекту данных Политику конфиденциальности Правообладателя (https://www.kaspersky.com/Products-and-Services-Privacy-Policy).

5.9. Пользователь несет полную ответственность по отношению к Правообладателю за любой ущерб, причиненный в результате нарушения настоящего Лицензионного соглашения, в частности, в случае неспособности Пользователя получить согласие Субъекта данных, если это применимо, и/или в случае отсутствия подтверждений, и/или позднего предоставления подтверждений наличия согласия, полученного от Субъекта данных, и/или любого другого нарушения обязательств по настоящему Лицензионному соглашению.

5.10. Пользователь обязуется возместить Правообладателю ущерб в результате претензий, выдвинутых третьими сторонами, в частности контролирующими органами по надзору за соблюдением законодательства о защите данных, против Правообладателя в связи с невыполнением Пользователем обязательств, указанных в разделе 5 «Условия обработки данных».

6. Получение информационных и рекламных материалов

6.1. Вы соглашаетесь получать от Правообладателя и его Партнеров информационные и рекламные сообщения посредством ПО, направленные на повышение уровня безопасности.

7. Ограничения

7.1. Вы не вправе декомпилировать, дизассемблировать, модифицировать или выполнять производные работы, основанные на ПО, целиком или частично, за исключением случаев, предусмотренных законодательством.

7.2. Запрещается передавать право на использование ПО третьей стороне.

7.3. Запрещается сдавать ПО в аренду, прокат или во временное пользование.

7.4. Запрещается использовать ПО с целью создания данных или кода, или программного обеспечения, предназначенных для обнаружения, блокирования или удаления угроз, описанных в Руководстве Пользователя.

7.5. Нарушение интеллектуальных прав на ПО ведет к гражданской, административной или уголовной ответственности в соответствии с законодательством.

8. Ограниченная гарантия и отказ от предоставления гарантий

8.1. Правообладатель гарантирует работу ПО в соответствии со спецификациями и описаниями, изложенными в Руководстве Пользователя.

8.2. Вы соглашаетесь с тем, что никакое программное обеспечение не свободно от ошибок, и поэтому рекомендуется регулярно создавать резервные копии файлов на Вашем компьютере.

8.3. Правообладатель не гарантирует работоспособность ПО при нарушении условий, описанных в Руководстве Пользователя или в настоящем Лицензионном соглашении.

8.4. Правообладатель не гарантирует работоспособность ПО, если Вы не осуществляете регулярные обновления ПО, указанные в п. 2.3 настоящего Лицензионного соглашения.

8.5. Правообладатель не гарантирует защиту от угроз, описанных в Руководстве Пользователя, по окончании срока, указанного в п. 3.1, или после прекращения действия лицензии на использование ПО по какой-либо причине.

8.6. Вы соглашаетесь с тем, что ПО предоставляется со стандартными настройками, применяемыми по умолчанию, и ответственность за вносимые Вами изменения в настройки ПО лежит на Вас.

8.7. ЗА ИСКЛЮЧЕНИЕМ УСТАНАВЛИВАЕМОЙ В НАСТОЯЩЕМ ПУНКТЕ ОГРАНИЧЕННОЙ ГАРАНТИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПОСТАВЛЯЕТСЯ «КАК ЕСТЬ». ПРАВООБЛАДАТЕЛЬ И ЕГО ПАРТНЕРЫ НЕ ДАЮТ НИКАКИХ ГАРАНТИЙ НА ЕГО ИСПОЛЬЗОВАНИЕ ИЛИ ПРОИЗВОДИТЕЛЬНОСТЬ. ЗА ИСКЛЮЧЕНИЕМ ГАРАНТИЙ, УСЛОВИЙ, ПРЕДСТАВЛЕНИЙ ИЛИ ПОЛОЖЕНИЙ, СТЕПЕНЬ КОТОРЫХ НЕ МОЖЕТ БЫТЬ ИСКЛЮЧЕНА ИЛИ ОГРАНИЧЕНА В СООТВЕТСТВИИ С ПРИМЕНИМЫМ ЗАКОНОДАТЕЛЬСТВОМ, ПРАВООБЛАДАТЕЛЬ И ЕГО ПАРТНЕРЫ НЕ ДАЮТ НИКАКИХ ГАРАНТИЙ, УСЛОВИЙ, ПРЕДСТАВЛЕНИЙ ИЛИ ПОЛОЖЕНИЙ (ВЫРАЖАЕМЫХ В ЯВНОЙ ИЛИ В ПОДРАЗУМЕВАЕМОЙ ФОРМЕ) НА ВСЕ, ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЙ НЕНАРУШЕНИЕ ПРАВ ТРЕТЬИХ ЛИЦ, КОММЕРЧЕСКОЕ КАЧЕСТВО, ИНТЕГРАЦИЮ ИЛИ ПРИГОДНОСТЬ ДЛЯ ОПРЕДЕЛЕННЫХ ЦЕЛЕЙ. ВЫ СОГЛАШАЕТЕСЬ С ТЕМ, ЧТО ВЫ НЕСЕТЕ ОТВЕТСТВЕННОСТЬ ЗА ВЫБОР ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ДОСТИЖЕНИЯ НУЖНЫХ РЕЗУЛЬТАТОВ, ЗА УСТАНОВКУ И ИСПОЛЬЗОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, А ТАКЖЕ ЗА РЕЗУЛЬТАТЫ, ПОЛУЧЕННЫЕ С ЕГО ПОМОЩЬЮ. БЕЗ ОГРАНИЧЕНИЯ ВЫШЕИЗЛОЖЕННЫХ ПОЛОЖЕНИЙ, ПРАВООБЛАДАТЕЛЬ НЕ ДЕЛАЕТ НИКАКИХ ЗАЯВЛЕНИЙ И НЕ ДАЕТ НИКАКИХ ГАРАНТИЙ, ЧТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НЕ БУДЕТ СОДЕРЖАТЬ ОШИБОК ИЛИ БУДЕТ РАБОТАТЬ БЕЗ СБОЕВ ИЛИ ДРУГИХ НЕИСПРАВНОСТЕЙ, ИЛИ ЧТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ БУДЕТ СООТВЕТСТВОВАТЬ КАКИМ-ЛИБО ИЛИ ВСЕМ ВАШИМ ТРЕБОВАНИЯМ, НЕЗАВИСИМО ОТ ТОГО, СООБЩИЛИ ЛИ ВЫ ПРАВООБЛАДАТЕЛЮ О ТАКОВЫХ ИЛИ НЕТ.

9. Исключения и ограничение ответственности

9.1. В МАКСИМАЛЬНОЙ СТЕПЕНИ, ДОПУСКАЕМОЙ ПРИМЕНИМЫМ ЗАКОНОДАТЕЛЬСТВОМ, ПРАВООБЛАДАТЕЛЬ И/ИЛИ ЕГО ПАРТНЕРЫ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА КАКИЕ-ЛИБО УБЫТКИ И/ИЛИ УЩЕРБ (В ТОМ ЧИСЛЕ УБЫТКИ В СВЯЗИ С НЕДОПОЛУЧЕННОЙ КОММЕРЧЕСКОЙ ПРИБЫЛЬЮ, ПРЕРЫВАНИЕМ ДЕЯТЕЛЬНОСТИ, УТРАТОЙ ИНФОРМАЦИИ ИЛИ ИНОЙ ИМУЩЕСТВЕННЫЙ УЩЕРБ), ВОЗНИКАЮЩИЕ В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ИЛИ НЕВОЗМОЖНОСТЬЮ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ДАЖЕ ЕСЛИ ПРАВООБЛАДАТЕЛЬ И/ИЛИ ЕГО ПАРТНЕРЫ БЫЛИ УВЕДОМЛЕНЫ О ВОЗМОЖНОМ ВОЗНИКНОВЕНИИ ТАКИХ УБЫТКОВ И/ИЛИ УЩЕРБА. В ЛЮБОМ СЛУЧАЕ ОТВЕТСТВЕННОСТЬ ПРАВООБЛАДАТЕЛЯ И/ИЛИ ЕГО ПАРТНЕРОВ ПО ЛЮБОМУ ИЗ ПОЛОЖЕНИЙ НАСТОЯЩЕГО ЛИЦЕНЗИОННОГО СОГЛАШЕНИЯ ОГРАНИЧИВАЕТСЯ СУММОЙ, ФАКТИЧЕСКИ УПЛАЧЕННОЙ ВАМИ ЗА ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ. НАСТОЯЩИЕ ОГРАНИЧЕНИЯ НЕ МОГУТ БЫТЬ ИСКЛЮЧЕНЫ ИЛИ ОГРАНИЧЕНЫ В СООТВЕТСТВИИ С ПРИМЕНИМЫМ ЗАКОНОДАТЕЛЬСТВОМ.

10. Открытое (свободное) программное обеспечение

10.1. Данный продукт содержит или может содержать программы, которые лицензируются (или сублицензируются) Пользователю в соответствии с общедоступной лицензией GNU или иными аналогичными лицензиями Open Source, которые помимо прочих прав разрешают Пользователю копировать, модифицировать, перераспределять определенные программы или их части и получать доступ к исходному коду («ПО с открытым исходным кодом»). Если такая лицензия предусматривает предоставление исходного кода Пользователям, которым предоставляется ПО в формате исполняемого двоичного кода, исходный код делается доступным при осуществлении запроса на адрес source@kaspersky.com или сопровождается с продуктом. Если какая-либо лицензия на ПО с открытым исходным кодом требует, чтобы Правообладатель предоставлял права на использование, копирование или модификацию ПО с открытым исходным кодом, выходящие за рамки прав, предоставляемых настоящим Лицензионным соглашением, такие права имеют преимущественную силу над правами и ограничениями, оговоренными в настоящем Лицензионном соглашении.

11. Права на интеллектуальную собственность

11.1. Вы соглашаетесь с тем, что ПО, документация, как и все другие объекты авторского права, а также системы, идеи и методы работы, другая информация, которая содержится в ПО, товарные знаки - являются объектами интеллектуальной собственности Правообладателя или его Партнеров. Данное Лицензионное соглашение не дает Вам никаких прав на использование объектов интеллектуальной собственности, включая товарные знаки и знаки обслуживания Правообладателя или его Партнеров, за исключением переданных Вам прав Правообладателем или его Партнерами.

11.2. Вы соглашаетесь с тем, что не будете модифицировать или изменять ПО никаким способом. Запрещается удалять или изменять уведомления об авторских правах или другие проприетарные уведомления на любой копии ПО.

12. Применимое законодательство

12.1. Настоящее Лицензионное соглашение регулируется в соответствии с законодательством Российской Федерации.

13. Контактная информация Правообладателя

Если у Вас есть какие-либо вопросы в отношении настоящего Соглашения, или если Вы хотите связаться с Правообладателем по любой причине, обратитесь в Отдел обслуживания клиентов по адресу:

АО «Лаборатория Касперского», Ленинградское шоссе, д. 39А, стр. 3

Москва, 125212

Российская Федерация

Адрес электронной почты: info@kaspersky.com

Веб-сайт: https://www.kaspersky.ru/