ESET Security Ultimate

Руководство пользователя

Щелкните здесь чтобы отобразить этого документа (онлайн-справка)

Digital Security
Progress. Protected.

Авторское право ©2024 ESET, spol. s r.o.

ESET Security Ultimate разработано компанией ESET, spol. s r.o.

Дополнительные сведения можно получить на сайте https://www.eset.com.

Все права защищены. Ни одна часть этой документации не может воспроизводиться, храниться в системе получения и передаваться в любой форме или любыми средствами, в том числе электронными и механическими способами, с помощью фотокопирования, записи, сканирования, а также любыми другими способами без письменного разрешения автора.

ESET, spol. s r.o. оставляет за собой право изменять любое описанное прикладное программное обеспечение без предварительного уведомления.

Служба технической поддержки: https://support.eset.com

ПРОВ. 12.04.2024

ESET Security Ultimate

ESET Security Ultimate представляет собой новый подход к созданию действительно комплексной системы безопасности компьютера. Новейшая версия модуля сканирования ESET LiveGrid® в сочетании со специализированными модулями файервола и защиты от спама обеспечивает скорость и точность, необходимые для безопасности компьютера. Таким образом, продукт представляет собой интеллектуальную систему непрерывной защиты от атак и вредоносных программ, которые могут угрожать безопасности компьютера.

ESET Security Ultimate — это комплексное решение для обеспечения безопасности, в котором сочетается максимальная степень защиты и минимальное влияние на производительность компьютера. Наши современные технологии используют искусственный интеллект для предотвращения заражения вирусами, шпионскими, троянскими, рекламными программами, червями, руткитами и другими угрозами без влияния на производительность системы и перерывов в работе компьютера.

Возможности и преимущества

Улучшенный интерфейс	Интерфейс в этой версии значительно улучшен и упрощен с учетом результатов тестирования на предмет удобства использования. Все формулировки и уведомления, присутствующие в графическом интерфейсе пользователя, были тщательно проанализированы, и теперь интерфейс поддерживает языки с написанием справа налево, например иврит и арабский. Интернет-справка теперь интегрирована в ESET Security Ultimate и содержит динамически обновляемые статьи по поддержке.
Темный режим	Расширение, с помощью которого можно быстро включить темную тему для экрана. Предпочитаемую цветовую схему можно выбрать в разделе Элементы интерфейса.
Защита от вирусов и шпионских программ	Упреждающее обнаружение и очистка большего количества известных и неизвестных вирусов, червей, троянских программ и руткитов. Метод расширенной эвристики идентифицирует даже раннее неизвестные вредоносные программы, обеспечивая защиту вашего компьютера от неизвестных угроз и нейтрализуя их до того, как они могут причинить какой-либо вред. Функции защиты доступа в Интернет и защиты от фишинга отслеживают обмен данными между веб-браузерами и удаленными серверами (в том числе SSL). Функция защиты почтового клиента обеспечивает контроль обмена сообщениями через протоколы POP3(S) и IMAP(S).
Регулярные обновления	Регулярное обновление модуля обнаружения (ранее известного, как база данных сигнатур вирусов) и программных модулей — лучший способ обеспечить максимальный уровень безопасности компьютера.
ESET LiveGrid® (репутация на основе облака)	Вы можете проверить репутацию запущенных процессов и файлов непосредственно с помощью ESET Security Ultimate.
Контроль устройств	Автоматически сканирует все USB-устройства флэш-памяти, карты памяти, а также компакт- и DVD-диски. Блокирует съемные носители на основании типа носителя, производителя, размера и других характеристик.

Функция HIPS	Вы можете более детально настроить поведение системы, задать правила для системного реестра, активных процессов и программ, а также точно настроить проверку состояния безопасности.
Игровой режим	Откладывает все всплывающие окна, обновления или другие действия, требующие большой нагрузки на систему, чтобы обеспечить экономию системных ресурсов для игр или других полноэкранных процессов.

Возможности ESET Security Ultimate

Защита банковских операций и браузера	Функция защиты банковских операций и браузера предлагает защищенный браузер для использования при доступе к шлюзам интернет-банкинга или онлайн-платежей, чтобы все финансовые операции в Интернете осуществлялись в заслуживающей доверия и безопасной среде.
Поддержка сетевых подписей	Сетевые подписи обеспечивают быструю идентификацию и блокируют на устройствах пользователя вредоносный входящий и исходящий трафик, имеющий отношение к ботам и пакетным средствам эксплуатации уязвимостей. Эту функцию можно считать улучшением в области защиты от ботнетов.
Интеллектуальный файервол	Предотвращает несанкционированный доступ к вашему компьютеру и использование ваших личных данных пользователями, не имеющими соответствующего разрешения.
Защита почтового клиента от спама	Доля спама в общем объеме передаваемых по электронной почте сообщений составляет около 50 %. Защита почтового клиента от спама решает эту проблему.
Антивор	Антивор повышает уровень безопасности пользовательской информации на случай потери или кражи компьютера. После установки программы ESET Security Ultimate и модуля Антивор ваше устройство будет отображаться в веб-интерфейсе. С помощью веб-интерфейса можно управлять конфигурацией модуля Антивор и администрировать функции Антивор на своем устройстве.
Родительский контроль	Обеспечивает защиту семьи от потенциально нежелательного веб-содержимого, блокируя веб-сайты различных категорий.
Password Manager	Password Manager, который защищает и хранит ваши пароли и личные данные.
Secure Data	Secure Data обеспечивает шифрование данных на компьютере и съемных носителях во избежание ненадлежащего использования конфиденциальной информации.
ESET LiveGuard	Обнаруживает и останавливает никогда ранее не встречавшиеся угрозы и обрабатывает информацию для обнаружения в будущем.
VPN	Храните свои данные в безопасности, избегайте нежелательного отслеживания и повысьте свою конфиденциальность с помощью дополнительной защиты, которую обеспечивает анонимный IP-адрес.
ESET Identity Protection	Защищает вашу личную, кредитную и финансовую информацию. ESET Identity Protection выявляет незаконную продажу вашей личной информации, проводя непрерывный мониторинг.

Чтобы функции ESET Security Ultimate работали, подписка должна быть активной. Рекомендуем продлить подписку на ESET Security Ultimate за несколько недель до истечения срока ее действия.

Новые возможности

Новые возможности в ESET Security Ultimate версии 17.1

- Небольшие улучшения функции «Инспектор сети»
- Небольшие улучшения функции «Защита банковских операций и браузера»
- ESET LiveGuard — теперь отправка документов включена по умолчанию
- Другие незначительные исправления и улучшения

> Чтобы отключить **уведомления о новых возможностях**, выполните следующие действия.
> 1. Откройте Расширенные параметры > **Уведомления** > **Уведомления на рабочем столе**.
> 2. Щелкните **Изменить** рядом с элементом **Уведомления на рабочем столе**.
> 3. Снимите флажок **Отображать уведомления о новых возможностях** и щелкните **ОК**.
> Для получения дополнительных сведений об уведомлениях ознакомьтесь с разделом Уведомления.

> Подробный список изменений в ESET Security Ultimate см. в разделе Журналы изменений ESET Security Ultimate.

Какой у меня продукт

В своих новых продуктах ESET реализует средства безопасности различного уровня: от мощного и быстрого антивируса до комплексного решения по обеспечению безопасности, минимально использующего системные ресурсы. Вот эти продукты:

- **ESET NOD32 Antivirus**
- **ESET Internet Security**
- **ESET Smart Security Premium**
- **ESET Security Ultimate**

Чтобы определить, какой из продуктов установлен у вас, откройте главное окно программы. Вверху окна вы увидите имя продукта (см. статью базы знаний).

В приведенной ниже таблице описаны функции каждого из продуктов.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Модуль обнаружения	✔	✔	✔	✔
Расширенное машинное обучение	✔	✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Блокировщик эксплойтов	✔	✔	✔	✔
Защита от атак на основе сценариев	✔	✔	✔	✔
защита от фишинга;	✔	✔	✔	✔
Защита доступа в Интернет	✔	✔	✔	✔
Система HIPS (в том числе защита от программ-вымогателей)	✔	✔	✔	✔
Защита от спама		✔	✔	✔
Файервол		✔	✔	✔
Инспектор сети		✔	✔	✔
Защита веб-камеры		✔	✔	✔
Защита от сетевых атак		✔	✔	✔
Защита от ботнетов		✔	✔	✔
Защита банковских операций и браузера		✔	✔	✔
Конфиденциальность и безопасность браузера		✔	✔	✔
Родительский контроль		✔	✔	✔
Антивор		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Некоторые продукты могут быть недоступны на вашем языке или в вашем регионе.

Требования к системе

Для оптимального функционирования ESET Security Ultimate ваша система должна отвечать следующим требованиям к аппаратному и программному обеспечению:

Поддерживаемые процессоры:

Процессор Intel или AMD, 32-разрядный (x86) с набором инструкций SSE2 или 64-разрядный (x64), частотой 1 ГГц и выше
процессор ARM64, 1 ГГц и выше

Операционная система поддерживается

Microsoft® Windows® 11

Microsoft® Windows® 10

Для установки или обновления продуктов ESET, выпущенных после июля 2023 года, во всех операционных системах Windows должна быть установлена поддержка подписывания кода Azure. Дополнительные сведения.

Регулярно обновляйте операционную систему.

Требования для функций ESET Security Ultimate

В таблице ниже указаны требования к системе для определенных функций ESET Security Ultimate.

Функция	Требования
Intel® Threat Detection Technology	См. информацию о поддерживаемых процессорах.
Защита банковских операций и браузера	См. информацию о поддерживаемых веб-браузерах.
Прозрачный фон	Windows 10 версии RS4 и более поздних версий.
Специализированное средство очистки	Процессор не на архитектуре ARM64.
Средство очистки системы	Процессор не на архитектуре ARM64.
Блокировщик эксплойтов	Процессор не на архитектуре ARM64.
Глубокая поведенческая проверка	Процессор не на архитектуре ARM64.

Другое

Для активации ESET Security Ultimate и надлежащей работы обновлений необходимо подключение к Интернету.

Две программы по защите от вирусов, работающие одновременно на одном устройстве, вызывают неизбежные конфликты системных ресурсов, например замедляют работу системы до нерабочего состояния.

Устаревшая версия Microsoft Windows

Проблема

- Вы хотите установить последнюю версию ESET Security Ultimate на компьютер с Windows 7, Windows 8 (8.1) или Windows Home Server 2011
- Во время установки ESET Security Ultimate отображает ошибку **Устаревшая операционная система**

Подробности

Для последней ESET Security Ultimate требуется операционная система Windows 10 или Windows 11.

Решение

Доступны следующие решения:

Обновление до Windows 10 или Windows 11

Процесс перехода относительно прост, и во многих случаях вы можете сделать это без потери файлов. Перед переходом на Windows 10:

1. Резервное копирование важных данных.

2. Прочитайте статью Майкрософт Обновление до Windows 10: вопросы и ответы или Обновление до Windows 11: вопросы и ответы и обновите свою операционную систему Windows.

Установка ESET Security Ultimate версии 16.0

Если вы не можете повысить версию Windows, установите ESET Security Ultimate версии 16.0. Дополнительные сведения см. в интернет-справке по ESET Security Ultimate версии 16.0.

Профилактика

При использовании компьютера, особенно во время работы в Интернете, необходимо помнить, что ни одна система защиты от вирусов не способна полностью устранить опасность заражений и удаленных атак. Чтобы достигнуть наивысшей степени безопасности и комфорта, важно использовать решение для защиты от вирусов надлежащим образом и следовать нескольким полезным правилам.

Регулярно обновляйте систему защиты от вирусов

Согласно статистическим данным, полученным от системы ESET LiveGrid®, ежедневно появляются тысячи новых уникальных заражений. Они созданы для обхода существующих мер безопасности и приносят доход их авторам за счет других пользователей. Специалисты исследовательской лаборатории ESET ежедневно анализируют такие угрозы, подготавливают и выпускают обновления для непрерывного повышения уровня защиты пользователей. Для максимальной эффективности этих обновлений важно настроить их надлежащим образом на компьютере пользователя. Дополнительные сведения о настройке обновлений см. в главе Настройка обновлений.

Загружайте пакеты обновлений операционной системы и других программ

Авторы вредоносных программ часто используют различные уязвимости в системе для увеличения эффективности распространения вредоносного кода. Принимая это во внимание, компании-производители программного обеспечения внимательно следят за появлением отчетов обо всех новых уязвимостях их приложений и регулярно выпускают обновления безопасности, стараясь уменьшить количество потенциальных угроз. Очень важно загружать эти обновления безопасности сразу же после их выпуска. ОС Microsoft Windows и веб-браузеры, такие как Internet Explorer, являются примерами программ, для которых регулярно выпускаются обновления безопасности.

Резервное копирование важных данных

Авторов вредоносных программ обычно не беспокоят проблемы пользователей, а действия их продуктов зачастую приводят к полной неработоспособности операционной системы и потере важной информации. Необходимо регулярно создавать резервные копии важных конфиденциальных данных на внешних носителях, таких как DVD-диски или внешние жесткие диски. Это позволяет намного проще и быстрее восстановить данные в случае сбоя системы.

Регулярно сканируйте компьютер на наличие вирусов

Многие известные и неизвестные вирусы, черви, троянские программы и руткиты обнаруживаются модулем защиты файловой системы в режиме реального времени. Это означает, что при каждом открытии файла выполняется его сканирование на наличие признаков деятельности вредоносных программ. Рекомендуем выполнять полное сканирование компьютера по крайней мере один раз в месяц, поскольку вредоносные программы изменяются, а модуль обнаружения обновляется каждый день.

Следуйте основным правилам безопасности

Это наиболее эффективное и полезное правило — всегда будьте осторожны. На данный момент для работы многих заражений (их выполнения и распространения) необходимо вмешательство пользователя. Если соблюдать осторожность при открытии новых файлов, можно значительно сэкономить время и силы, которые в противном случае будут потрачены на устранение заражений на компьютере. Ниже приведены некоторые полезные рекомендации.

• Не посещайте подозрительные веб-сайты с множеством всплывающих окон и анимированной рекламой.

• Будьте осторожны при установке бесплатных программ, пакетов кодеков и т. п.. Используйте только безопасные программы и посещайте безопасные веб-сайты.

• Будьте осторожны, открывая вложения в сообщения электронной почты (особенно это касается сообщений, рассылаемых массово и отправленных неизвестными лицами).

• Не используйте учетную запись с правами администратора для повседневной работы на компьютере.

Страницы справочной системы

Добро пожаловать в руководство пользователя ESET Security Ultimate. Представленная здесь информация ознакомит вас с программным продуктом и сделает использование компьютера более безопасным.

Начало работы

Перед использованием программы ESET Security Ultimate вы можете ознакомиться с различными типами обнаружений и удаленных атак, с которыми может столкнуться пользователь компьютера. Мы также составили список новых функций, появившихся в ESET Security Ultimate.

Начните с установки ESET Security Ultimate. Если вы уже установили ESET Security Ultimate, см.

раздел Работа с ESET Security Ultimate.

Использование страниц справочной системы ESET Security Ultimate

Интернет-справка разделена на главы и подразделы. Для просмотра информации об открытом в данный момент окне в ESET Security Ultimate нажмите клавишу **F1**.

Программа позволяет искать тему в справочной системе по ключевым словам или выполнять поиск содержимого, вводя конкретные слова или фразы. Разница между этими двумя способами состоит в том, что ключевое слово, характеризующее содержимое справочной страницы, может отсутствовать в тексте этой страницы. Поиск по словам и фразам осуществляется в содержимом всех страниц. В результате отображаются все страницы, содержащие именно эти слова и фразы.

Для согласованности информации и во избежание путаницы в настоящем руководстве используется терминология, основанная на интерфейсе программы ESET Security Ultimate. Кроме того, для выделения особо интересных или важных тем в настоящем документе использован единый набор символов.

Примечания содержат краткие сведения о наблюдениях. Вы можете пропускать их, однако в примечаниях содержится ценная информация, например сведения о конкретных функциях или ссылки на соответствующие материалы.

Эта информация требует вашего внимания, так что рекомендуем ее не пропускать. Обычно такая информация важна, но не критически.

Это информация о том, что требует особого внимания и осторожности. Отметка «ВНИМАНИЕ!» используется для того, чтобы удержать вас от потенциально опасных ошибок. Прочитайте и поймите текст предупреждения, поскольку он содержит сведения об исключительно важных системных настройках или о возможных угрозах.

Это образец использования или практический пример, помогающий понять, как можно использовать определенную функцию или компонент.

Условное обозначение	Значение
Жирный шрифт	Названия элементов интерфейса, например флажков или переключателей.
Курсив	Заполнители для предоставляемой вами информации. Например, если текст имя файла или путь указан с использованием курсива, это означает, что путь или имя файла должны ввести вы.
`Courier New`	Образцы кода или команд.
Гиперссылка	Обеспечивает простой и быстрый доступ к связанным разделам или внешним веб-страницам. Гиперссылки выделяются синим цветом и иногда подчеркиванием.
%ProgramFiles%	Системный каталог Windows, в котором хранятся программы, установленные в этой ОС.

Интернет-справка — основной источник справочных сведений. Если подключение к Интернету установлено, автоматически открывается последняя версия интернет-справки.

Установка

Существует несколько способов установки ESET Security Ultimate на компьютере. Способы установки могут отличаться в зависимости от страны и способа получения продукта.

• Интерактивный установщик: загружается с веб-сайта ESET или компакт-/DVD-диска. Пакет для установки подходит для всех языков (выберите нужный). Интерактивный установщик представляет собой файл небольшого размера. Другие необходимые для установки ESET Security Ultimate файлы загружаются автоматически.

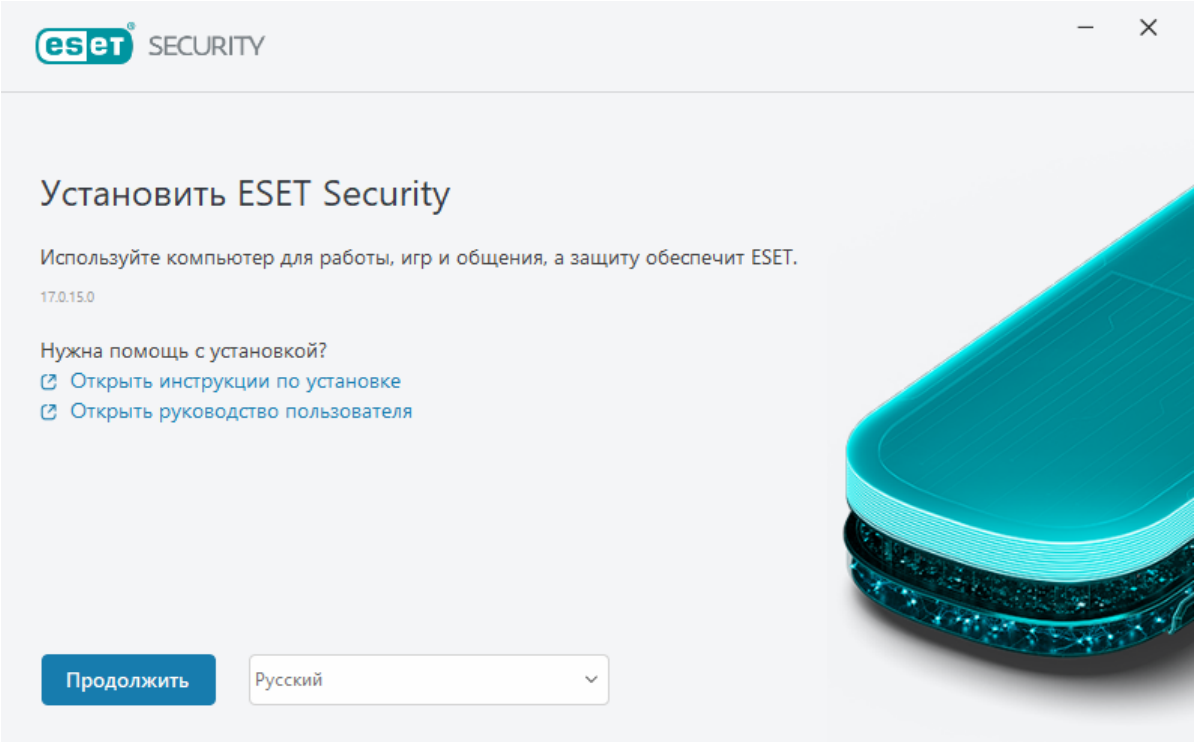
• Автономная установка: в рамках этого типа установки используется файл формата .exe, размер которого превышает размер файла интерактивного установщика. При этом для установки не требуется подключение к Интернету или дополнительные файлы.

Перед установкой ESET Security Ultimate убедитесь, что на компьютере не установлены другие программы защиты от вирусов. Если на одном компьютере установлено два и более решения для защиты от вирусов, между ними может возникнуть конфликт. Рекомендуется удалить все прочие программы защиты от вирусов с компьютера. Список инструментов для удаления популярных антивирусных программ см. в статье базы знаний ESET (доступна на английском и на нескольких других языках).

Интерактивный установщик

После загрузки пакета для установки интерактивного установщика дважды щелкните файл установки и следуйте пошаговым инструкциям мастера установки.

Для использования этого типа установки необходимо подключение к Интернету.



1. Выберите нужный язык в раскрывающемся меню и щелкните **Продолжить**.

Если вы устанавливаете более новую версию поверх предыдущей версии с защищенными паролем настройками, введите свой пароль. Вы можете конфигурировать пароль для настроек в разделе Настройка доступа.

2. Выберите настройки для следующих функций, прочитайте Лицензионное соглашение с конечным пользователем и Политику конфиденциальности и щелкните **Продолжить** или **Разрешить все и продолжить**, чтобы включить все функции:

- Система обратной связи ESET LiveGrid®
- Потенциально нежелательные приложения
- Программа улучшения пользовательского опыта

Нажимая **Продолжить** или **Разрешить все и продолжить**, вы принимаете Лицензионное соглашение с конечным пользователем и соглашаетесь с Политикой конфиденциальности.

3. Чтобы активировать безопасность устройства, управлять ею и просматривать о ней сведения с помощью ESET HOME, подключите устройство к учетной записи ESET HOME. Щелкните **Пропустить вход**, чтобы продолжить без подключения к ESET HOME. Вы сможете подключить устройство к учетной записи ESET HOME позже.

4. В случае продолжения без подключения к ESET HOME выберите опцию активации. Если вы устанавливаете более новую версию поверх старой, ваш **ключ активации** будет введен автоматически.

5. Мастер установки определяет, какой продукт ESET устанавливается, согласно вашей подписки. Всегда предварительно выбрана версия с максимальным количеством функций безопасности. Щелкните **Изменить продукт**, если нужно установить другую версию продукта ESET. Щелкните **Продолжить**, чтобы начать процесс установки. Он может занять некоторое время.

При наличии каких-либо остатков (файлов или папок) продуктов ESET, которые были удалены в прошлом, вам будет предложено разрешить их удаление. Щелкните **Установить**, чтобы продолжить.

6. Нажмите кнопку **Готово**, чтобы закрыть мастер установки.

Устранение неполадок при установке.

После установки и активации программы начнется загрузка модулей. Выполняется инициализация защиты, и до завершения загрузки некоторые функции могут еще не быть полностью функциональными.

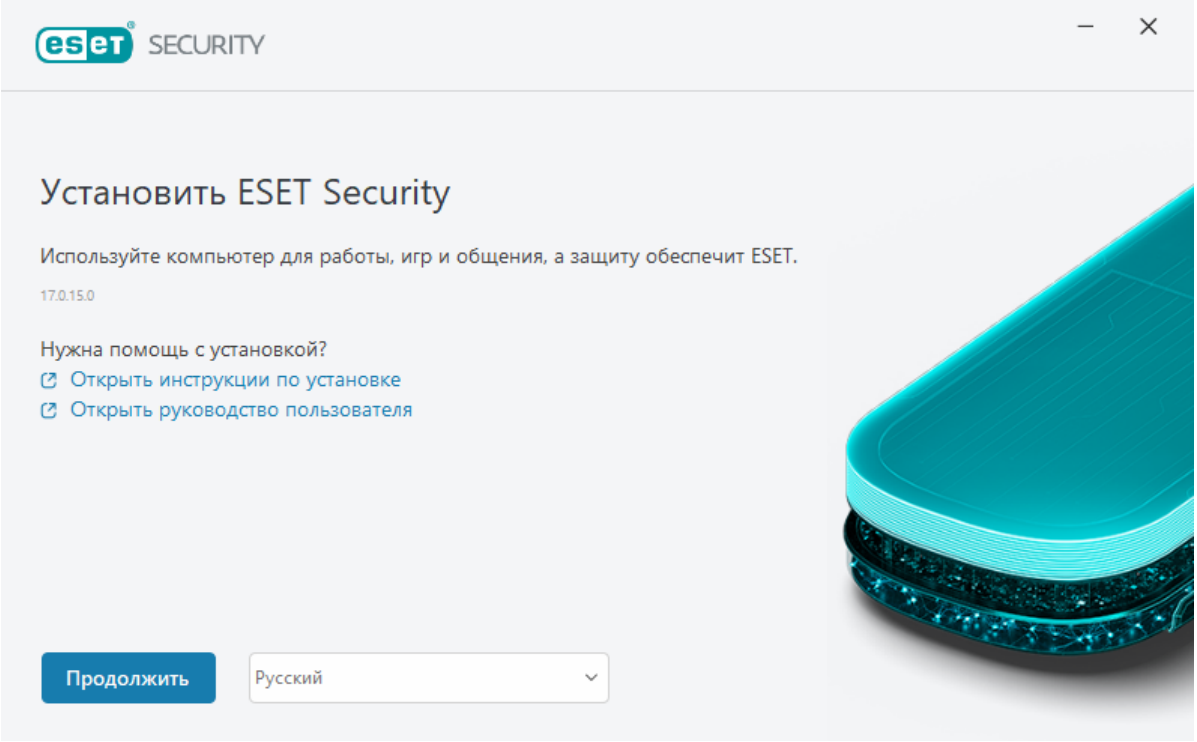
Автономная установка

Загрузите и установите продукт ESET для Windows для домашнего использования с помощью автономного установщика (.exe) ниже. Выберите, какую версию продукта ESET HOME загрузить (32-разрядную, 64-разрядную или ARM).

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Загрузить 64-разрядную версию Загрузить 32-разрядную версию Загрузить версию ARM	Загрузить 64-разрядную версию Загрузить 32-разрядную версию Загрузить версию ARM	Загрузить 64-разрядную версию Загрузить 32-разрядную версию Загрузить версию ARM	Загрузить 64-разрядную версию Загрузить 32-разрядную версию Загрузить версию ARM

Если у вас активное подключение к Интернету, установите продукт ESET с помощью интерактивного установщика.

Когда вы запустите автономный установщик (.exe), мастер установки поможет установить программу.



1. Выберите нужный язык в раскрывающемся меню и щелкните **Продолжить**.

Если вы устанавливаете более новую версию поверх предыдущей версии с защищенными паролем настройками, введите свой пароль. Вы можете конфигурировать пароль для настроек в разделе Настройка доступа.

2. Выберите настройки для следующих функций, прочитайте Лицензионное соглашение с конечным пользователем и Политику конфиденциальности и щелкните **Продолжить** или **Разрешить все и продолжить**, чтобы включить все функции:

- Система обратной связи ESET LiveGrid®
- Потенциально нежелательные приложения
- Программа улучшения пользовательского опыта

Нажимая **Продолжить** или **Разрешить все и продолжить**, вы принимаете Лицензионное соглашение с конечным пользователем и соглашаетесь с Политикой конфиденциальности.

3. Щелкните **Пропустить вход**. Если у вас есть подключение к Интернету, вы можете подключить устройство к своей учетной записи ESET HOME.

4. Щелкните **Пропустить активацию**. Для полноценной работы решение ESET Security Ultimate должно быть активировано после установки. Для активации программы требуется активное подключение к Интернету.

5. Мастер установки показывает, какой продукт ESET будет установлен, в зависимости от загруженного автономного установщика. Щелкните **Продолжить**, чтобы начать процесс установки. Он может занять некоторое время.

При наличии каких-либо остатков (файлов или папок) продуктов ESET, которые были удалены в прошлом, вам будет предложено разрешить их удаление. Щелкните **Установить**, чтобы продолжить.

6. Нажмите кнопку **Готово**, чтобы закрыть мастер установки.

Устранение неполадок при установке.

Повышение уровня подписки

Это окно уведомления появляется, когда была изменена подписка, используемая для активации вашего продукта ESET. Измененная подписка позволяет активировать продукт, который имеет больше функций безопасности. Если никаких изменений сделано не было, в ESET Security Ultimate один раз отобразится окно предупреждения **Переход к использованию продукта с большим количеством функций**.

Да (рекомендуется): будет автоматически установлен продукт с дополнительными функциями безопасности.

Нет, спасибо: никаких изменений не будет, и уведомление больше не появится.

Сведения о том, как изменить продукт позже, см. в статье базы знаний ESET. Дополнительные сведения о подписке ESET см. в разделе Вопросы и ответы о подписке.

В приведенной ниже таблице описаны функции каждого из продуктов.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Модуль обнаружения	✔	✔	✔	✔
Расширенное машинное обучение	✔	✔	✔	✔
Блокировщик эксплойтов	✔	✔	✔	✔
Защита от атак на основе сценариев	✔	✔	✔	✔
защита от фишинга;	✔	✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Защита доступа в Интернет	✔	✔	✔	✔
Система HIPS (в том числе защита от программ-вымогателей)	✔	✔	✔	✔
Защита от спама		✔	✔	✔
Файервол		✔	✔	✔
Инспектор сети		✔	✔	✔
Защита веб-камеры		✔	✔	✔
Защита от сетевых атак		✔	✔	✔
Защита от ботнетов		✔	✔	✔
Защита банковских операций и браузера		✔	✔	✔
Конфиденциальность и безопасность браузера		✔	✔	✔
Родительский контроль		✔	✔	✔
Антивор		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Повышение уровня продукта

Вы загрузили установщик по умолчанию и решили изменить активируемый продукт, или вы желаете заменить установленный продукт на продукт с дополнительными функциями безопасности.

Изменение продукта во время установки.

В приведенной ниже таблице описаны функции каждого из продуктов.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Модуль обнаружения	✔	✔	✔	✔
Расширенное машинное обучение	✔	✔	✔	✔
Блокировщик эксплойтов	✔	✔	✔	✔
Защита от атак на основе сценариев	✔	✔	✔	✔
защита от фишинга;	✔	✔	✔	✔
Защита доступа в Интернет	✔	✔	✔	✔
Система HIPS (в том числе защита от программ-вымогателей)	✔	✔	✔	✔
Защита от спама		✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Файервол		✔	✔	✔
Инспектор сети		✔	✔	✔
Защита веб-камеры		✔	✔	✔
Защита от сетевых атак		✔	✔	✔
Защита от ботнетов		✔	✔	✔
Защита банковских операций и браузера		✔	✔	✔
Конфиденциальность и безопасность браузера		✔	✔	✔
Родительский контроль		✔	✔	✔
Антивор		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Понижение уровня подписки

Это диалоговое окно появляется, когда была изменена подписка, используемая для активации вашего продукта ESET. Измененная подписка может использоваться только с другим продуктом ESET, который имеет меньше функций безопасности. Продукт был изменен автоматически, чтобы предотвратить потерю защиты.

Дополнительные сведения о подписке ESET см. в разделе Вопросы и ответы о подписке.

В приведенной ниже таблице описаны функции каждого из продуктов.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Модуль обнаружения	✔	✔	✔	✔
Расширенное машинное обучение	✔	✔	✔	✔
Блокировщик эксплойтов	✔	✔	✔	✔
Защита от атак на основе сценариев	✔	✔	✔	✔
защита от фишинга;	✔	✔	✔	✔
Защита доступа в Интернет	✔	✔	✔	✔
Система HIPS (в том числе защита от программ-вымогателей)	✔	✔	✔	✔
Защита от спама		✔	✔	✔
Файервол		✔	✔	✔
Инспектор сети		✔	✔	✔
Защита веб-камеры		✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Защита от сетевых атак		✔	✔	✔
Защита от ботнетов		✔	✔	✔
Защита банковских операций и браузера		✔	✔	✔
Конфиденциальность и безопасность браузера		✔	✔	✔
Родительский контроль		✔	✔	✔
Антивор		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Понижение уровня продукта

Установленный сейчас продукт имеет больше функций по обеспечению безопасности, чем продукт, который вы собираетесь активировать. Функции VPN, «Защита идентификационных данных», Secure Data и Password Manager не входят в состав этого продукта. Вы не сможете создавать зашифрованные файлы.

В приведенной ниже таблице описаны функции каждого из продуктов.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Модуль обнаружения	✔	✔	✔	✔
Расширенное машинное обучение	✔	✔	✔	✔
Блокировщик эксплойтов	✔	✔	✔	✔
Защита от атак на основе сценариев	✔	✔	✔	✔
защита от фишинга;	✔	✔	✔	✔
Защита доступа в Интернет	✔	✔	✔	✔
Система HIPS (в том числе защита от программ-вымогателей)	✔	✔	✔	✔
Защита от спама		✔	✔	✔
Файервол		✔	✔	✔
Инспектор сети		✔	✔	✔
Защита веб-камеры		✔	✔	✔
Защита от сетевых атак		✔	✔	✔
Защита от ботнетов		✔	✔	✔
Защита банковских операций и браузера		✔	✔	✔
Конфиденциальность и безопасность браузера		✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Родительский контроль		✔	✔	✔
Антивор		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Устранение неполадок при установке

Если во время установки возникают проблемы, мастер установки предоставляет решение для устранения неполадок, которое поможет с ними справиться, если это возможно.

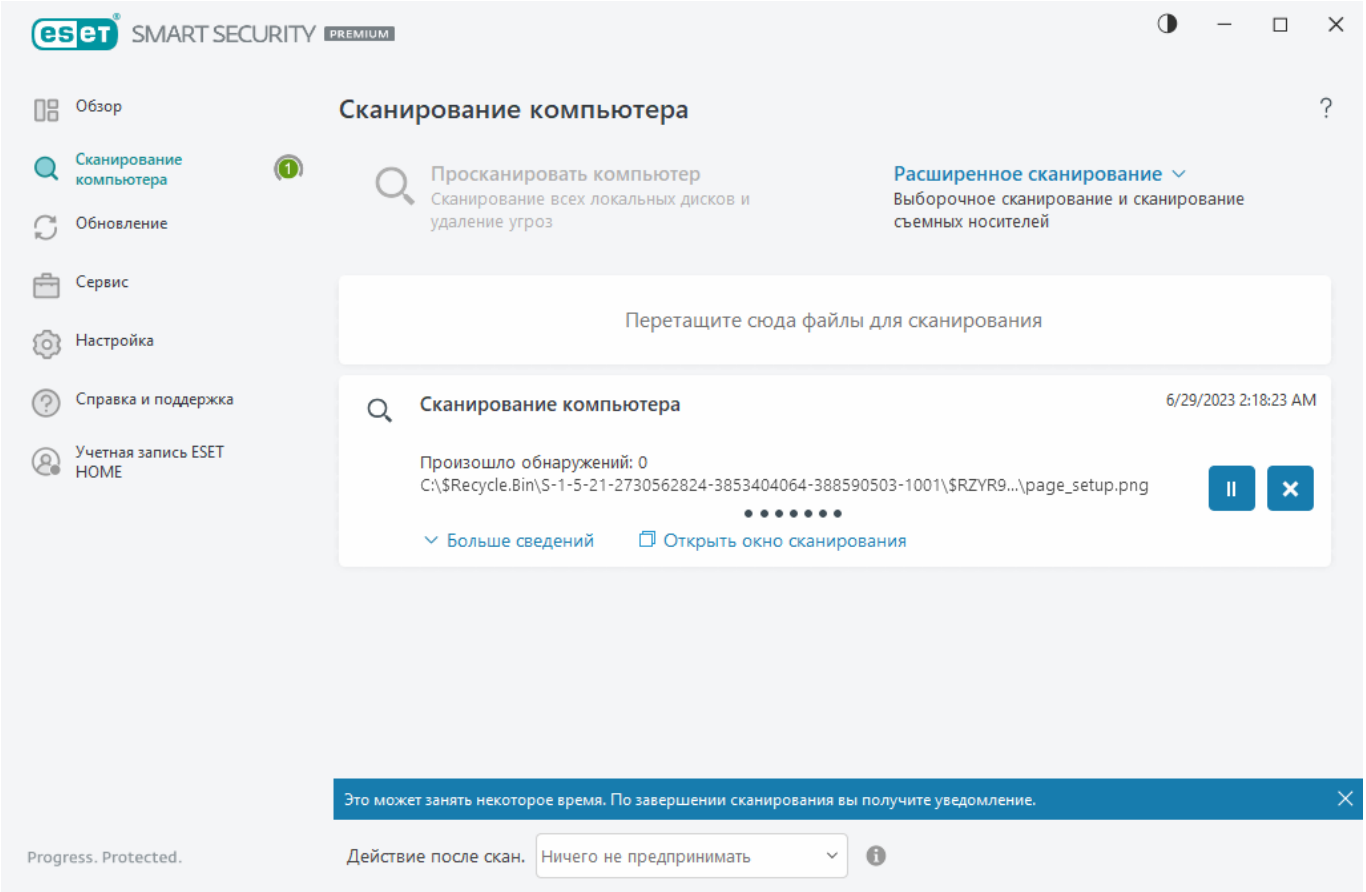
Щелкните **Запустить устранение неполадок**. Когда решение для устранения неполадок завершит работу, выполните рекомендуемые действия.

Если проблема не будет устранена, см. список распространенных ошибок установки и решений для них.

Первое сканирование после установки

После установки ESET Security Ultimate и первого успешного обновления автоматически начинается сканирование компьютера на наличие вредоносного кода.

Сканирование компьютера также можно запустить вручную в главном окне программы > **Сканирование компьютера** > **Сканировать компьютер**. Для получения дополнительных сведений о сканировании компьютера см. раздел Сканирование компьютера.



Обновление до новой версии

Новые версии ESET Security Ultimate выпускаются для реализации улучшений или исправления проблем, которые не могут быть устранены автоматическим обновлением модулей программы. Обновление до более новой версии можно выполнить одним из нескольких способов.

1. Автоматически путем обновления программы.
Поскольку обновления программы распространяются среди всех пользователей и могут повлиять на некоторые системные конфигурации, они выпускаются только после длительного тестирования с целью обеспечения бесперебойной работы на всех возможных конфигурациях. Чтобы перейти на новую версию сразу после ее выпуска, воспользуйтесь одним из перечисленных ниже способов.
Убедитесь, что включен параметр **Обновление функций приложения** в разделе Расширенные параметры > **Обновление** > **Профили** > **Обновления**.

2. Вручную в главном окне программы с помощью кнопки **Проверить наличие обновлений** в разделе **Обновление**

3. Вручную путем загрузки и установки новой версии поверх предыдущей.

Дополнительные сведения и иллюстрированные инструкции см. в разделах:

- Обновление продуктов ESET — проверка на наличие новейших версий модулей продукта
- Различные типы выпусков и обновлений продуктов ESET

Автоматическое обновление устаревшей версии продукта

Версия продукта ESET больше не поддерживается. Ваш продукт был обновлен до последней версии.

⚠ Распространенные проблемы, возникающие при установке

> i Каждая новая версия продуктов ESET содержит множество исправлений ошибок и улучшений. Имеющиеся клиенты с действующей подпиской для продукта ESET могут бесплатно перейти на последнюю версию того же продукта.

Чтобы завершить установку, выполните следующие действия.

1. Нажмите **Принять и продолжить**, чтобы принять лицензионное соглашение с конечным пользователем и подтвердить свое согласие с политикой конфиденциальности. Если вы не согласны с лицензионным соглашением, нажмите **Удалить**. Восстановить предыдущую версию невозможно.

2. Щелкните **Разрешить все и продолжить**, чтобы разрешить как Систему обратной связи ESET LiveGrid®, так и Программу улучшения пользовательского опыта, или нажмите **Продолжить**, если вы не хотите участвовать.

3. После активации нового продукта ESET с помощью ключа активации откроется страница «Обзор». Если сведения о вашей подписке не будут найдены, воспользуйтесь бесплатной пробной версией. Если подписка, используемая в предыдущем продукте, недействительна, активируйте продукт ESET.

4. Для завершения установки необходимо перезагрузить устройство.

Будет выполнена установка ESET Security Ultimate

Это диалоговое окно может отобразиться:

- В процессе установки — щелкните **Продолжить**, чтобы установить ESET Security Ultimate.
- При изменении подписки в ESET Security Ultimate — щелкните **Активировать**, чтобы изменить подписку и активировать ESET Security Ultimate.

С помощью опции **Изменить продукт** можно переключаться между Windows-продуктами ESET для домашнего использования, доступными в соответствии с вашей подпиской ESET. Подробнее см. в статье Какой у меня продукт.

Переход к использованию другой линейки продуктов

Вы можете переключаться между различными Windows-продуктами ESET для домашнего использования, доступными в соответствии с вашей подпиской ESET. Подробнее см. в статье Какой у меня продукт.

Регистрация

Зарегистрируйте подписку, заполнив поля регистрационной формы и нажав **Активировать**. Обязательны к заполнению поля, рядом с которыми в скобках дано соответствующее указание. Данная информация будет использоваться только в целях, связанных с вашей подпиской ESET.

Ход выполнения активации

Процесс активации займет несколько секунд (необходимое время может отличаться в зависимости от скорости подключения к Интернету или характеристик компьютера).

Активация выполнена

Процесс активации завершен. Чтобы завершить настройку ESET Security Ultimate, следуйте указаниям послеустановочного мастера.

Обновление модуля начнется через несколько секунд. Регулярные обновления ESET Security Ultimate начнутся сразу после этого.

Первое сканирование начнется автоматически в течение 20 минут после обновления модуля.

> Процесс активации может быть прерван, если предложение не связано с ESET HOME. Авторизуйтесь в ESET HOME или создайте учетную запись.

Руководство для начинающих

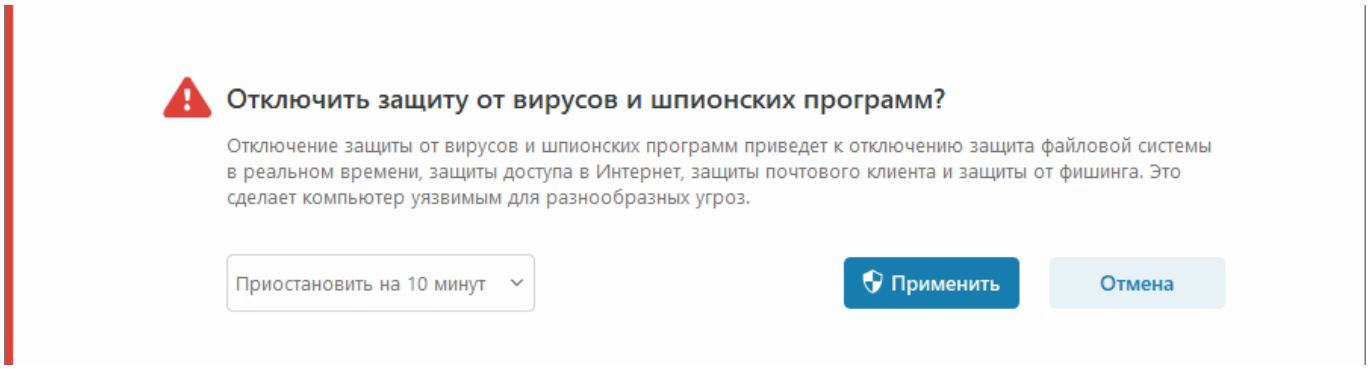
В этом разделе приводятся общие сведения о программном обеспечении ESET Security Ultimate и его основных параметрах.

Значок на панели задач

К некоторым наиболее важным функциям и настройкам можно получить доступ, щелкнув правой кнопкой мыши значок на панели задач .

Приостановить защиту. На экран выводится диалоговое окно для подтверждения. В нем можно отключить модуль обнаружения, который контролирует обмен файлами и данными через Интернет и электронную почту, предотвращая тем самым атаки на систему. С помощью

раскрывающегося меню **Интервал времени** можно указать, на какое время отключается защита.



Приостановить работу файервола (разрешить весь трафик): файервол переводится в неактивное состояние. Для получения дополнительных сведений см. раздел Сеть.

Блокировать весь сетевой трафик: весь сетевой трафик будет заблокирован. Чтобы разблокировать трафик, щелкните **Остановить блокировку всего сетевого трафика**.

Расширенные параметры: вызов расширенных параметров ESET Security Ultimate. Чтобы открыть расширенные параметры в главном окне продукта, нажмите клавишу F5 на клавиатуре или выберите **Настройка** > **Расширенные параметры**.

Файлы журнала: файлы журнала содержат информацию о важных программных событиях и предоставляют общие сведения об обнаружениях.

Открыть ESET Security Ultimate: открывает главное окно программы ESET Security Ultimate.

Сбросить настройки макета окна: для окна ESET Security Ultimate восстанавливаются размер и положение на экране по умолчанию.

Режим цвета: открывает настройки интерфейса, с помощью которых можно изменить цвет графического интерфейса.

Проверить наличие обновлений: запуск обновления программы или модуля, чтобы обеспечить защиту. ESET Security Ultimate автоматически проверяет наличие обновлений несколько раз в день.

О программе: отображение информации о системе, сведений об установленной версии ESET Security Ultimate и установленных модулях программы, а также данных об операционной системе и системных ресурсах.

Сочетания клавиш

Для более удобной навигации в ESET Security Ultimate можно использовать следующие сочетания клавиш:

Сочетания клавиш	Действие
F1	вызов справки
F5	вызов окна расширенных параметров

Сочетания клавиш	Действие
Стрелка вверх или стрелка вниз	навигация в пунктах раскрывающегося меню
TAB	переход к следующему элементу графического интерфейса пользователя в окне
Shift+TAB	переход к предыдущему элементу графического интерфейса пользователя в окне
ESC	закрытие активного диалогового окна
Ctrl+U	отображение сведений о подписке ESET и вашем компьютере (информация для службы технической поддержки)
Ctrl+R	восстановление размеров окна продукта и его положения на экране по умолчанию
ALT + стрелка влево	переход назад
ALT + стрелка вправо	переход вперед
ALT+Home	переход на домашнюю страницу

Для навигации также можно использовать кнопки мыши назад или вперед.

Профили

Диспетчер профилей используется в двух разделах ESET Security Ultimate: в разделе **Сканирование по требованию** и в разделе **Обновление**.

Сканирование компьютера

В ESET Security Ultimate есть четыре предварительно заданных профиля сканирования:

• **Интеллектуальное сканирование** — это профиль расширенного сканирования по умолчанию. Для профиля интеллектуального сканирования используется технология интеллектуальной оптимизации, исключающая файлы, которые во время предыдущего сканирования были определены как чистые и с того времени не изменялись. Это обеспечивает сокращение времени сканирования при минимальном влиянии на безопасность системы.

• **Сканирование через контекстное меню** — вы можете запустить в контекстном меню сканирование по требованию для любого файла. Профиль «Сканирование через контекстное меню» позволяет определить конфигурацию сканирования, которая будет использоваться при запуске сканирования таким способом.

• **Глубокое сканирование** — Для профиля глубокого сканирования интеллектуальная оптимизация по умолчанию не используется, поэтому при использовании этого профиля никакие файлы из сканирования не исключаются.

• **Сканирование компьютера** — этот профиль по умолчанию используется при стандартном сканировании компьютера.

Предпочтительные параметры сканирования можно сохранить для использования в дальнейшем. Рекомендуется создать отдельный профиль для каждого регулярно

используемого сканирования (с различными объектами, методами сканирования и прочими параметрами).

Чтобы создать профиль, откройте раздел Расширенные параметры > **Модуль обнаружения** > **Процессы сканирования вредоносных программ** > **Сканирование по требованию** > **Список профилей** > **Изменить**. В окне **Диспетчер профилей** доступно раскрывающееся меню **Выбранный профиль** со списком существующих профилей сканирования и опцией для создания нового. Для создания профиля сканирования в соответствии с конкретными потребностями см. раздел ThreatSense, где описывается каждый параметр, используемый для настройки сканирования.

> Предположим, вам требуется создать собственный профиль сканирования. Хотя конфигурация **Сканировать компьютер** частично подходит, сканировать программы-упаковщики или потенциально опасные приложения не требуется и нужно применить **Всегда исправлять обнаружение**. Введите имя нового профиля в окне **Диспетчер профилей** и нажмите кнопку **Добавить**. Выберите новый профиль в раскрывающемся меня **Выбранный профиль** и настройте остальные параметры в соответствии со своими требованиями, а затем нажмите кнопку **ОК**, чтобы сохранить новый профиль.

Обновление

Редактор профилей, расположенный в разделе «Настройка обновлений», дает пользователям возможность создавать новые профили обновления. Создавать и использовать собственные пользовательские профили (т. е. профили, отличные от профиля по умолчанию **Мой профиль**) следует только в том случае, если компьютер подключается к серверам обновлений разными способами.

В качестве примера можно привести ноутбук, который обычно подключается к локальному серверу (зеркалу) в локальной сети, но также загружает обновления непосредственно с серверов обновлений ESET, когда находится не в локальной сети (например, во время командировок). На таком ноутбуке можно использовать два профиля: первый настроен на подключение к локальному серверу, а второй — к одному из серверов ESET. После настройки профилей перейдите в раздел **Служебные программы** > **Планировщик** и измените параметры задач обновления. Назначьте один из профилей в качестве основного, а другой — в качестве вспомогательного.

Профиль обновления: текущий профиль обновления. Для изменения профиля выберите нужный из раскрывающегося меню.

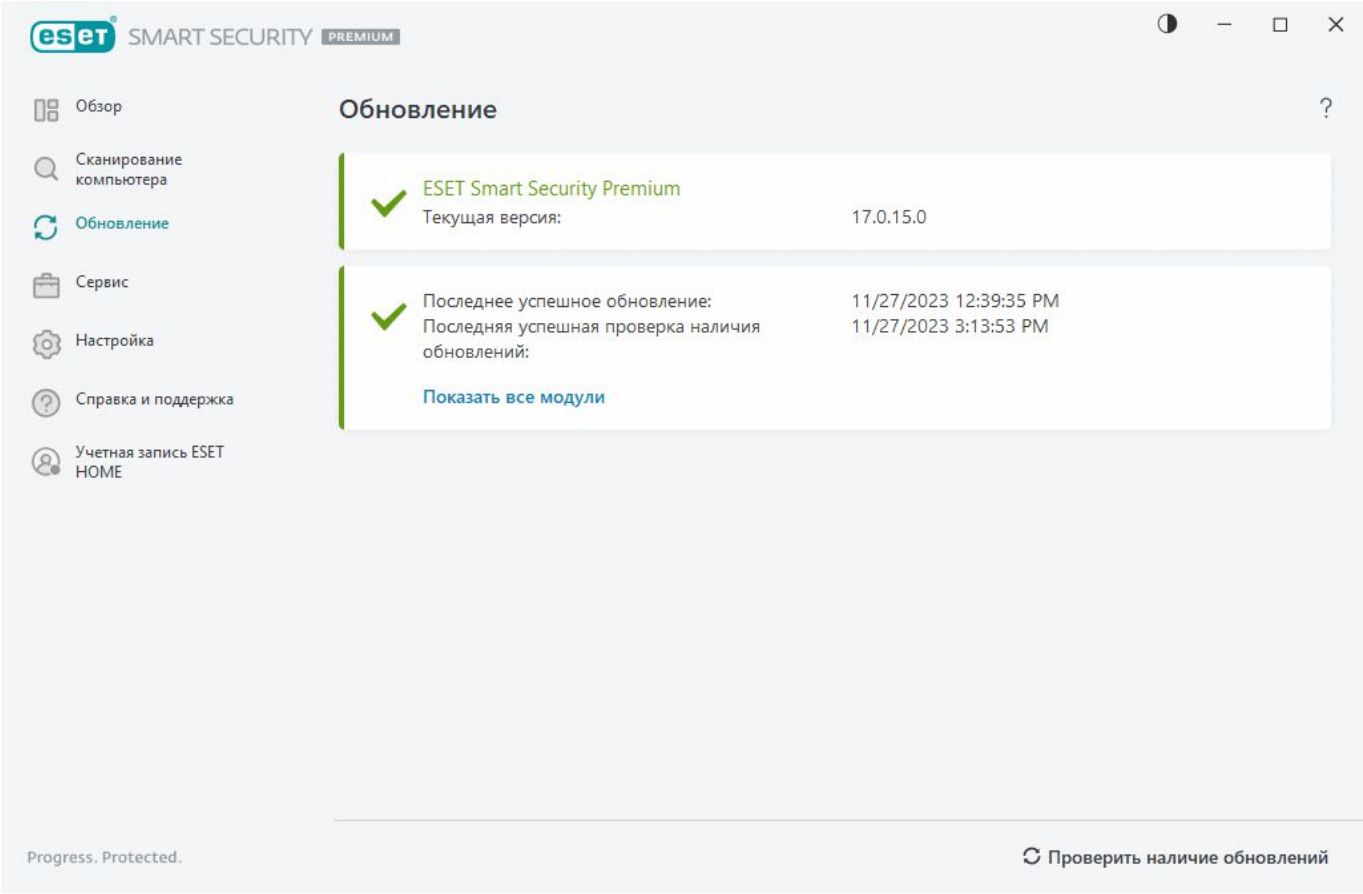
Список профилей: создание или редактирование профилей обновления.

Обновления

Регулярное обновление ESET Security Ultimate — лучший способ обеспечить максимальный уровень безопасности компьютера. Модуль обновления поддерживает актуальность программных модулей и компонентов системы.

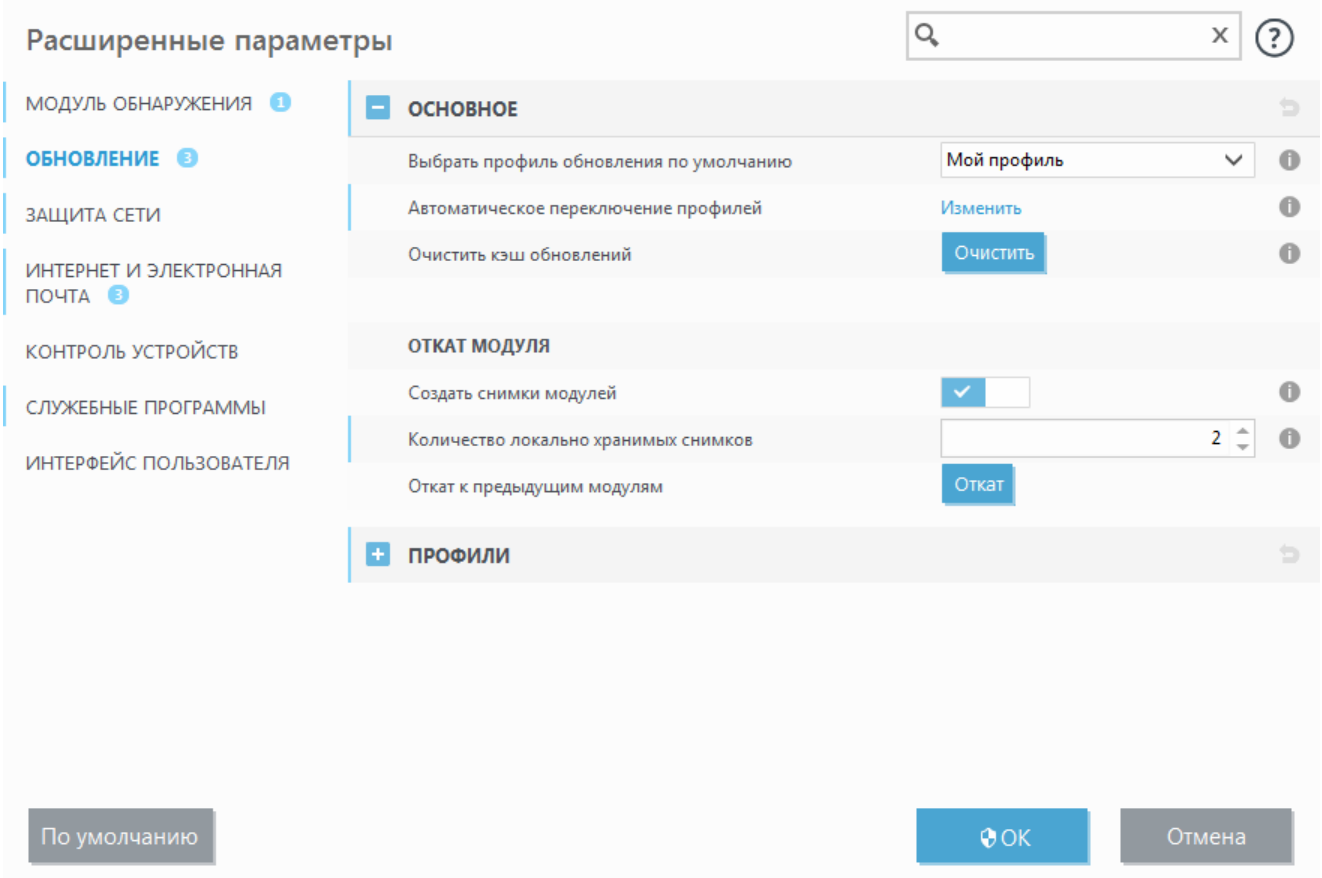
Выбрав пункт **Обновление** в главном окне программы, можно просмотреть информацию о текущем состоянии обновления, в том числе дату и время последнего успешно выполненного обновления, а также сведения о необходимости обновления.

Кроме автоматического обновления, можно выполнить обновление вручную, нажав кнопку **Проверить наличие обновлений**.



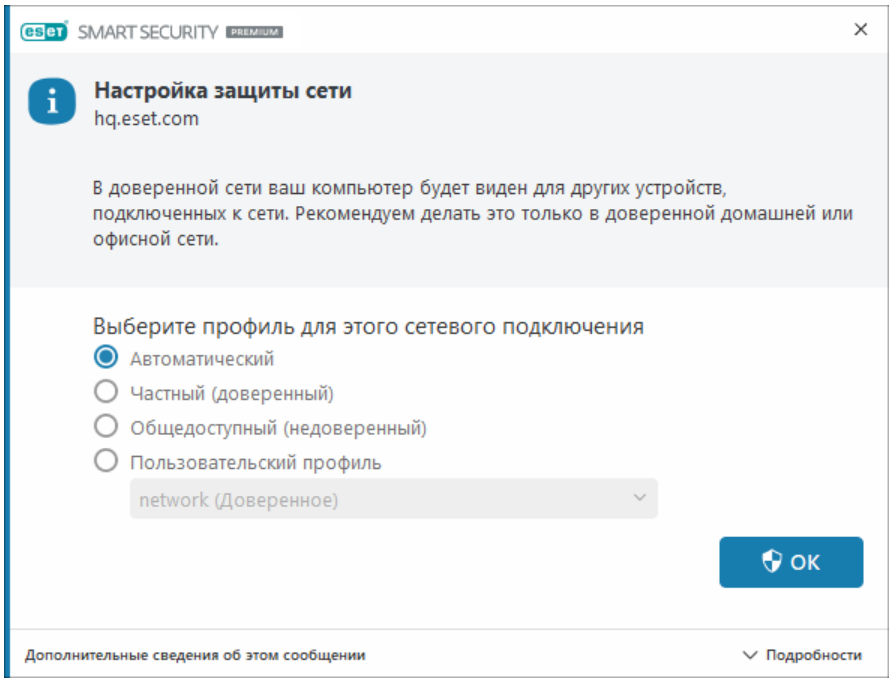
Раздел Расширенные параметры > **Обновление** содержит дополнительные опции обновления, такие как режим обновления, доступ к прокси-серверу и подключения к локальной сети.

Если при обновлении возникнут проблемы, щелкните **Очистить**, чтобы удалить кэш обновления. Если обновить модули программы все равно не удается, см. раздел Устранение неполадок при получении сообщения «Обновление модулей не выполнено».



Настройка защиты сети

По умолчанию ESET Security Ultimate использует параметры Windows при обнаружении новой сети. Чтобы при обнаружении новой сети отображалось диалоговое окно, установите для параметра Назначение профиля защиты сети значение **Запросить**. Конфигурация защиты сети отображается при каждом подключении вашего компьютера к новой сети.



Можно выбрать один из следующих профилей сетевых подключений.

Автоматический: ESET Security Ultimate автоматически выберет профиль согласно активаторам, настроенным для каждого профиля.

Конфиденциально — для доверенной сети (домашней или офисной сети). Ваш компьютер и общие файлы, хранящиеся на нем, видны для других пользователей сети, а также другим пользователям сети доступны системные ресурсы (доступ к общим файлам и принтерам включен, входящее подключение RPC включено, общий доступ к удаленному рабочему столу предоставлен). Этот параметр рекомендуется использовать при доступе к безопасной локальной сети. Этот профиль автоматически назначается сетевому подключению, если оно настроено как доменная или частная сеть в Windows.

Общедоступная — для недоверенных (общедоступных) сетей. Файлы и папки в вашей системе не являются общими для других пользователей в сети, и другие пользователи сети их не видят, а общий доступ к системным ресурсам отключен. Этот параметр рекомендуется использовать при доступе к беспроводным сетям. Этот профиль автоматически назначается любому сетевому подключению, которое не настроено как доменная или частная сеть в Windows.

Пользовательский профиль: в раскрывающемся меню можно выбрать созданный вами профиль. Эта опция доступна только в том случае, если вы создали хотя бы один пользовательский профиль.

Неправильная конфигурация сети может представлять угрозу безопасности вашего компьютера.

Включить Антивор

Персональные устройства постоянно подвергаются риску потери или кражи в наших повседневных поездках из дома на работу или в другие общественные места. Антивор — это функция, которая расширяет безопасность на уровне пользователя в случае потери или кражи устройства. Антивор позволяет мониторить использование устройства и отслеживать ваше потерянное устройство с помощью локализации по IP-адресу в ESET HOME, помогая восстановить устройство и защитить личные данные.

Благодаря использованию в модуле Антивор таких современных технологий, как определение географического местоположения по IP-адресу, захват изображений с помощью веб-камеры, защита учетной записи пользователя и мониторинг устройства, пользователи и правоохранительные органы имеют возможность находить потерянные или украденные компьютеры или устройства. В ESET HOME вы можете увидеть, какие действия выполняются на вашем компьютере или устройстве.

Дополнительные сведения о Антивор в ESET HOME см. в интерактивной справке ESET HOME.

Антивор может работать неправильно на компьютерах в доменах из-за ограничений в управлении учетными записями пользователей.

Чтобы включить Антивор и защитить свое устройство в случае потери или кражи, выберите одну из следующих опций:

- В главном окне программы в разделе **Обзор** щелкните **НАСТРОИТЬ** рядом с элементом **Антивор**.

• Если в главном окне программы > **Обзор** экране отображается сообщение «Антивор доступен», щелкните **Включить Антивор**.

• В главном окне программы щелкните **Настройка** > **Средства безопасности**. Включите переключатель  **Антивор** и следуйте инструкциям на экране.

Если ваше устройство не подключено к ESET HOME, необходимо сделать следующее:
1. Войдите в свою учетную запись ESET HOME при включении Антивор.
2. Задать имя устройства.

Приложение Антивор не поддерживает Microsoft Windows Home Server.

После включения Антивор вы сможете оптимизировать безопасность вашего устройства в главном окне программы > **Параметры** > **Средства безопасности**> **Антивор**.

Родительский контроль

Если вы уже включили родительский контроль в ESET Security Ultimate, необходимо также настроить эту функцию для всех связанных учетных записей пользователя.

Если родительский контроль включен, но учетные записи пользователя не настроены, в ESET Security Ultimate на экране **Обзор** отображается уведомление «Функция родительского контроля не настроена». Щелкните **Настроить правила** и для получения дополнительных сведений прочитайте раздел Родительский контроль.

Активация программы

Существует несколько способов активации программы. Доступность того или иного варианта в окне активации может зависеть от страны и способа получения программы (на компакт- или DVD-диске, с веб-страницы ESET и т. д.).

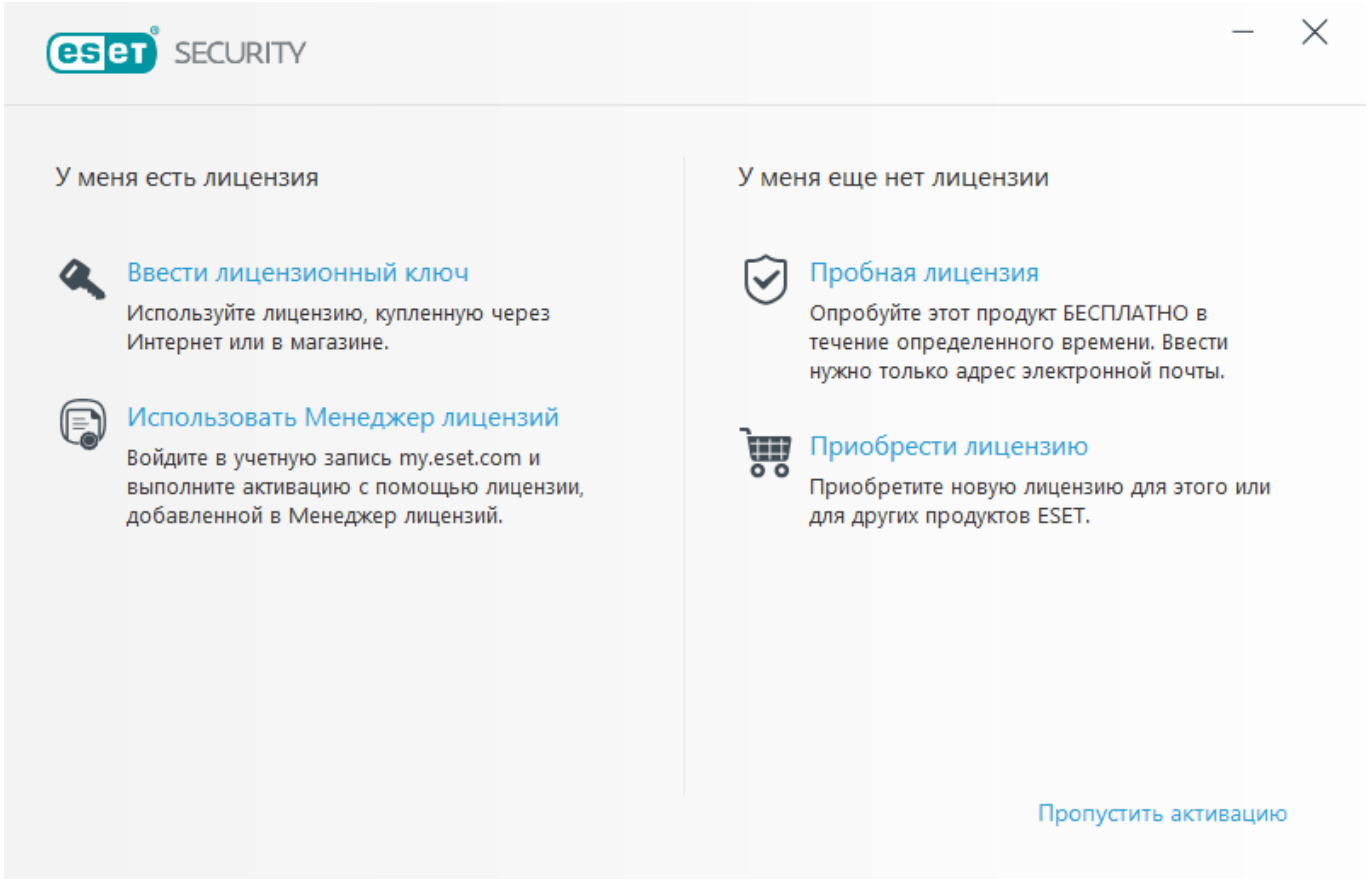
• Если вы приобрели розничную коробочную версию продукта или получили электронное письмо с информацией о подписке, активируйте продукт, щелкнув **Использовать приобретенный ключ активации**. Для успешного выполнения активации ключ активации необходимо ввести в том виде, в котором он предоставлен. Ключ активации — это уникальная строка в формате XXXX-XXXX-XXXX-XXXX-XXXX или XXXX-XXXXXXXX, которая используется для идентификации владельца и активации подписки. Ключ активации, как правило, расположен внутри упаковки продукта или на ее тыльной стороне.

• После выбора параметра Использование учетной записи ESET HOME вам будет предложено авторизоваться в учетной записи ESET HOME.

• Если у вас нет подписки, но вы хотите купить ее, щелкните **Приобрести подписку**. В результате откроется веб-сайт местного дистрибьютора ESET. Подписки на Windows-продукты ESET для домашнего использования не бесплатны.

Изменить подписку на продукт можно в любое время. Для этого щелкните **Справка и поддержка** > **Изменить подписку** в главном окне программы. Отобразится открытый идентификатор, предназначенный для идентификации подписки в службе поддержки ESET.

⚠ Не удалось активировать программу?



Ввод ключа активации во время активации

Автоматические обновления являются важным компонентом вашей безопасности. ESET Security Ultimate будет получать обновления после активации.

При вводе **ключа активации** важно указывать его именно в том виде, в котором он получен. Ключ активации — это уникальная строка в формате XXXX-XXXX-XXXX-XXXX-XXXX, которая используется для идентификации владельца и активации подписки.

Во избежание неточностей рекомендуется скопировать ключ активации из электронного письма с регистрационными данными и вставить его в нужное поле.

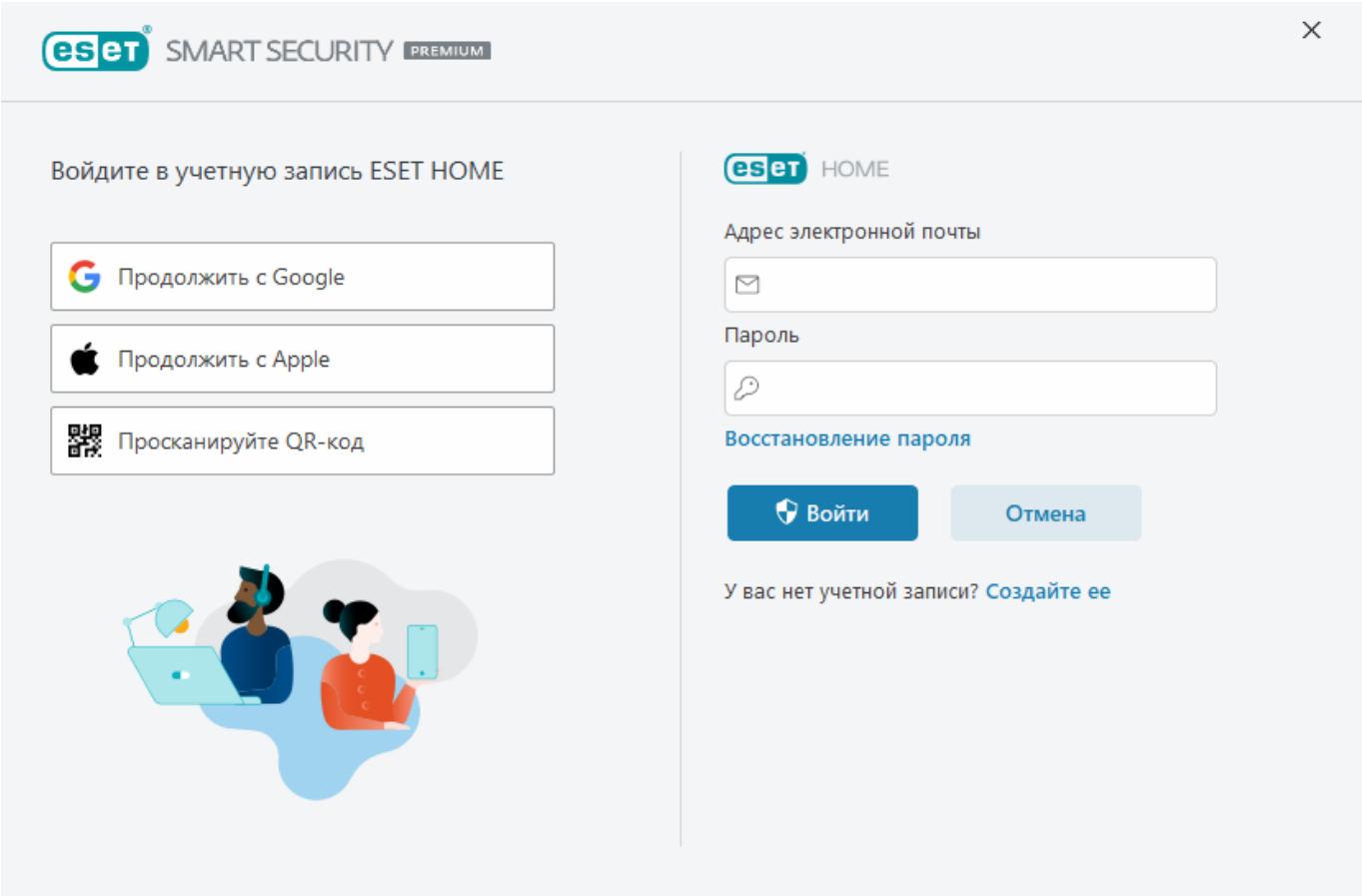
Если не ввести ключ активации после установки, продукт активирован не будет. ESET Security Ultimate Можно активировать в главном окне программы > **Справка и поддержка** > **Активировать подписку**.

Подписки на Windows-продукты ESET для домашнего использования не бесплатны.

Использование учетной записи ESET HOME

Подключите свое устройство к ESET HOME, чтобы получить возможность просматривать все активированные подписки и устройства ESET и управлять ими. Подписку можно продлить, расширить или повысить ее уровень, а также просмотреть важные сведения о ней. На портале управления или в мобильном приложении ESET HOME можно добавлять различные подписки,

загружать продукты на свои устройства, проверять состояние безопасности продукта и делиться подписками по электронной почте. Дополнительные сведения можно найти на онлайн-справке ESET HOME.



После выбора варианта **Использование учетной записи ESET HOME** в качестве способа активации или при подключении к учетной записи ESET HOME во время установки:

1. Вход в учетную ESET HOME запись.

> Если у вас нет учетной записи ESET HOME, щелкните **Создать учетную запись**, чтобы зарегистрироваться, или ознакомьтесь с инструкциями в онлайн-справке ESET HOME. Если вы забыли пароль, щелкните **Я не помню пароль** и следуйте инструкциям на экране или ознакомьтесь с инструкциями в онлайн-справке ESET HOME.

2. Задайте **имя устройства**, которое будет использоваться во всех службах ESET HOME, а затем щелкните **Продолжить**.

3. Выберите подписку для активации или добавьте новую подписку. Щелкните **Продолжить**, чтобы активировать ESET Security Ultimate.

Бесплатный ключ активации ESET

Подписка на ESET Security Ultimate не бесплатна.

Ключ активации ESET представляет собой уникальную последовательность разделенных дефисами букв и цифр. Он предоставляется компанией ESET и обеспечивает легальное использование ESET Security Ultimate в соответствии с лицензионным соглашением с конечным

пользователем. Каждый конечный пользователь имеет право использовать ключ активации только в пределах, в которых он имеет право использовать ESET Security Ultimate в соответствии с количеством лицензий, предоставленных компанией ESET. Ключ активации считается конфиденциальным и не может быть передан третьим лицам. Однако вы можете предоставить общий доступ к подписке с помощью ESET HOME.

Некоторые источники в Интернете могут предоставить вам «бесплатные» ключи активации ESET, но следует учитывать следующее.

- Переход по рекламной ссылке «Бесплатная подписка ESET» может подвергнуть опасности ваш компьютер или устройство и привести к заражению вредоносными программами. Вредоносные программы могут скрываться в неофициальном веб-содержимом (например, в видеороликах), на веб-сайтах, которые зарабатывают деньги, показывая рекламу посетителям, и т. д. Обычно это ловушка.

- ESET имеет право отключать пиратские подписки и делает это.

- Использование пиратского ключа активации нарушает условия лицензионного соглашения с конечным пользователем, которое вы должны принять, чтобы установить ESET Security Ultimate.

- Покупайте подписку ESET только через официальные каналы, например на сайте www.eset.com, у дистрибьюторов или посредников ESET (не покупайте подписку на неофициальных сторонних веб-сайтах, таких как eBay, и подписки с общим доступом у третьих лиц).

- Загрузка продукта ESET Security Ultimate является бесплатной, но для активации во время установки требуется действительный ключ активации ESET (вы можете загрузить и установить продукт, но без активации он не будет работать).

- Не делитесь своей подпиской в Интернете или социальных сетях (она может стать широко доступной).

Чтобы распознать пиратскую подписку ESET и сообщить о ней, воспользуйтесь инструкциями, которые приведены в статье нашей базы знаний.

Если вы не уверены в необходимости покупать продукт безопасности ESET, для принятия решения можно воспользоваться пробной версией:

1. Активация ESET Security Ultimate с помощью бесплатной пробной версии

2. Участие в программе бета-тестирования ESET

3. Установите ESET Mobile Security, если вы используете мобильное устройство Android, это решение является условно-бесплатным.

Чтобы получить скидку или продлить лицензию, продлите продукт ESET.

Активация не выполнена: распространенные сценарии

Если активация ESET Security Ultimate завершилась неудачей, наиболее распространенными сценариями являются:

- Ключ активации уже используется.
- Введен недопустимый ключ активации.
- В форме активации отсутствует или указана недопустимая информация.
- Ошибка обмена данными с сервером активации.
- Подключение к серверам активации ESET отсутствует или отключено.

Убедитесь, что введен правильный ключ активации и есть подключение к Интернету. Попробуйте активировать ESET Security Ultimate еще раз. Если для активации вы используете учетную запись ESET HOME, см. статью Подписка ESET HOME и управление подпиской — интернет-справка.

> Если вы получили сообщение об ошибке (например, «Подписка приостановлена» или «Превышен порог использования подписки»), следуйте инструкциям в разделе Состояние подписки.

Если вам все равно не удается выполнить активацию ESET Security Ultimate, воспользуйтесь средством ESET по устранению неполадок активации, которое содержит ответы на часто задаваемые вопросы, сведения об ошибках и способы решения проблем с активацией и лицензированием (доступно на английском и нескольких других языках).

Состояние подписки

У подписки могут быть разные состояния. Состояние подписки можно увидеть в ESET HOME. Чтобы добавить подписку в учетную запись ESET HOME, ознакомьтесь с разделом Добавление подписки.

> Если у вас нет учетной записи ESET HOME, можно создать новую учетную запись ESET HOME.

При любом состоянии подписки, кроме **активного**, отобразится сообщение об ошибке во время активации или уведомление в главном окне программы.

Чтобы отключить уведомления о состоянии подписки, откройте раздел Расширенные параметры > **Уведомления** > **Состояния приложения**. Щелкните **Изменить** рядом с элементом **Состояния приложения**, разверните элемент **Лицензирование** и снимите флажок рядом с уведомлением, которое нужно отключить. Отключение уведомления не решит проблему.

В таблице ниже приведены описания и рекомендуемые решения для разных состояний подписки.

Состояние подписки	Описание	Решение
Активный	Подписка действительна, и никаких действий пользователя не требуется. Программу ESET Security Ultimate можно активировать. Сведения о подписке можно найти в главном окне программы > **Справка и поддержка**.	
Превышен порог использования	Эта подписка используется на большем количестве устройств, чем она предусматривает. Отобразится сообщение об ошибке при активации.	Для получения дополнительных сведений см. раздел Активация не выполнена из-за превышения порога использования подписки.
Приостановлена	Подписка приостановлена из-за проблем с оплатой. Чтобы использовать подписку, убедитесь, что в ESET HOME указаны ваши актуальные платежные данные, или обратитесь к посреднику, у которого была приобретена подписка. Эта ошибка может отобразиться во время активации или в главном окне программы.	Установленный продукт: если у вас есть учетная запись ESET HOME, в уведомлении, отображаемом в главном окне программы, щелкните **Управлять подпиской в ESET HOME** и проверьте свои платежные данные. В противном случае обратитесь к посреднику, у которого была приобретена подписка. Ошибка при активации: если у вас есть учетная запись ESET HOME, в окне сообщения об ошибке при активации щелкните **Открыть ESET HOME** и просмотрите свои платежные данные. В противном случае обратитесь к посреднику, у которого была приобретена подписка.
Срок действия истек	Срок действия подписки истек, и вы не можете активировать ESET Security Ultimate с помощью этой подписки. Эта ошибка может отобразиться во время активации или в главном окне программы. Если программа ESET Security Ultimate уже установлена, компьютер не защищен и не обновляется.	Установленный продукт: в уведомлении, отображаемом в главном окне программы, щелкните **Продлить подписку** и следуйте инструкциям в разделе Как продлить подписку? или щелкните **Активировать продукт** и выберите способ активации. Ошибка при активации: в окне «Ошибка при активации» щелкните **Продлите свою подписку** и следуйте инструкциям в разделе Как продлить подписку? или введите новый либо продленный ключ активации и щелкните **Продлить подписку**.

Состояние подписки	Описание	Решение
Отменена	Ваша подписка была отменена компанией ESET или посредником, у которого была приобретена подписка.	Если отображается сообщение об ошибке «Подписка отменена» в главном окне программы или во время активации, но ваша подписка должна работать правильно, обратитесь к посреднику, у которого была приобретена подписка.

Активация не выполнена из-за превышения порога использования подписки

Проблема

- Возможно, превышен порог использования вашей подписки, или она используется не по назначению
- Активация не выполнена из-за превышения порога использования подписки

Решение

Эта подписка используется на большем количестве устройств, чем она предусматривает. Возможно, вы стали жертвой пиратства или подделки программного обеспечения. Эта подписка не может быть использована для активации какого-либо другого продукта ESET. Вы можете решить эту проблему непосредственно, если у вас есть право на управление подпиской в учетной записи ESET HOME или если вы приобрели подписку в законном источнике. Если у вас еще нет учетной записи, создайте ее.

Если вы являетесь владельцем подписки и не получили запрос на ввод адреса электронной почты:

1. Чтобы управлять подпиской ESET, откройте веб-браузер и перейдите на веб-сайт https://home.eset.com. Откройте ESET License Manager и удалите либо деактивируйте рабочие места. Более подробные сведения см. в разделе Что делать в случае превышения порога использования подписки.

2. Чтобы распознать пиратскую подписку ESET и сообщить о ней, воспользуйтесь инструкциями в нашей статье.

3. Если вы не уверены в том, что происходит, нажмите кнопку **«Назад»** и свяжитесь со службой технической поддержки ESET по электронной почте.

Если вы не владелец подписки, сообщите владельцу этой подписки о том, что вы не можете активировать продукт ESET из-за превышения порога использования подписки. Владелец может решить эту проблему на портале ESET HOME.

Если вы получите запрос на подтверждение адреса электронной почты (он отображается

только в некоторых случаях), введите адрес электронной почты, который вы изначально использовали для покупки или активации ESET Security Ultimate.

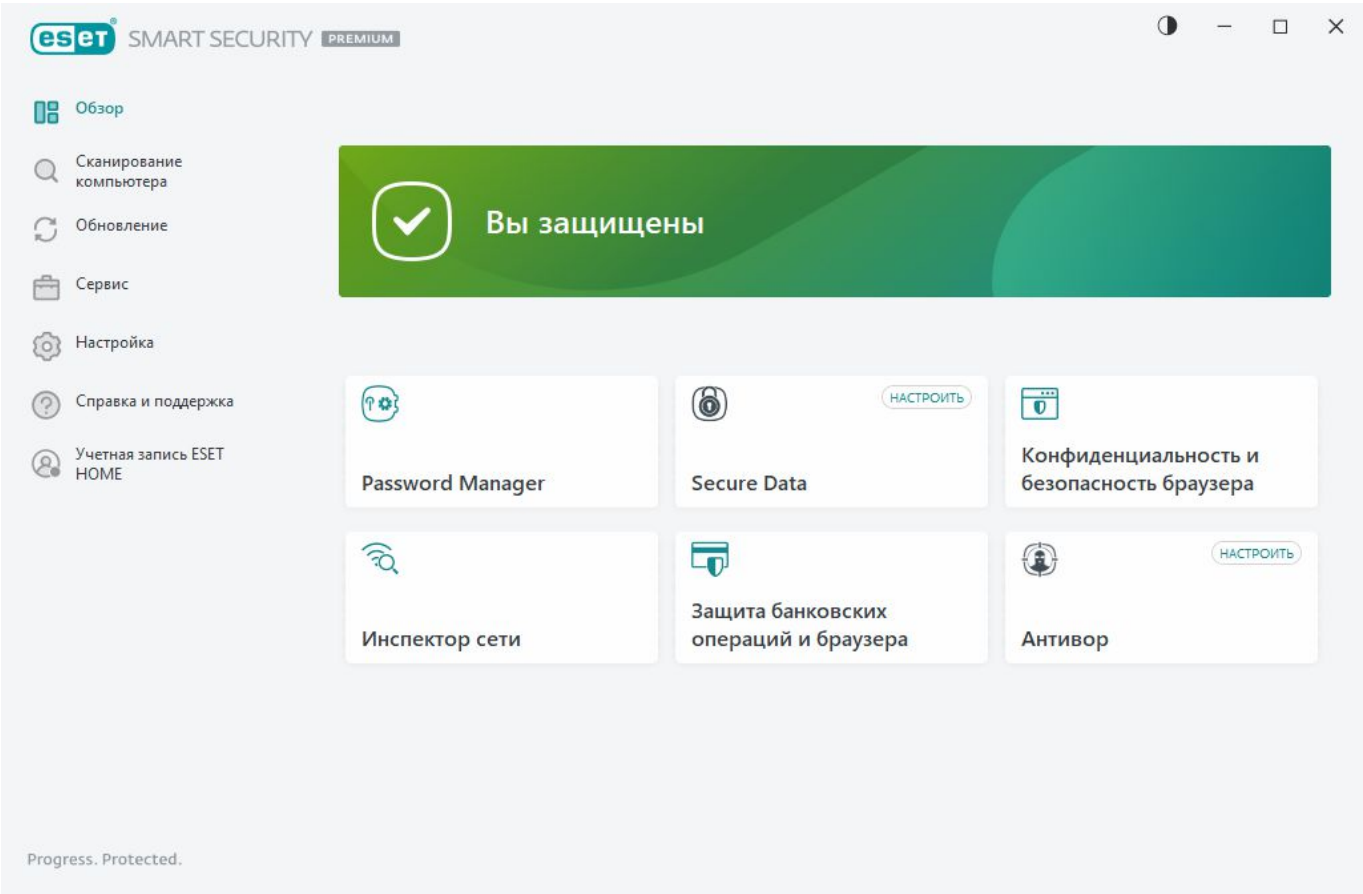
Работа с ESET Security Ultimate

Главное окно программы ESET Security Ultimate разделено на две части. Основное окно справа содержит информацию, относящуюся к параметру, выбранному в главном меню слева.

> **Иллюстрированные инструкции**
> Иллюстрированные инструкции на английском и еще нескольких языках можно найти в разделе Открытие главного окна программы в продуктах ESET для Windows.

Цветовую схему графического интерфейса ESET Security Ultimate можно выбрать в правом верхнем углу главного окна программы. Щелкните значок **Цветовая схема** (значок изменяется в зависимости от выбранной в данный момент цветовой схемы) рядом со значком **Свернуть** и выберите цветовую схему в раскрывающемся меню:

- **Соответствовать цвету системы**: цветовая схема ESET Security Ultimate задается согласно настройкам операционной системы.
- **Темная**: выбор темной цветовой схемы для ESET Security Ultimate (темный режим).
- **Светлая**: выбор стандартной (светлой) цветовой схемы для ESET Security Ultimate.



Опции главного меню:

Обзор: этот пункт предоставляет информацию о состоянии защиты ESET Security Ultimate.

Сканирование компьютера: настройка и запуск сканирования компьютера или создание выборочного сканирования.

Обновление: отображение информации об обновлении модуля и модуля обнаружения.

Сервис: обеспечивает доступ к Инспектору сети и другим функциям, которые помогают упростить администрирование программы и содержат дополнительные возможности для опытных пользователей.

Настройка: содержит опции конфигурации для функций защиты ESET Security Ultimate («Защита компьютера», «Защита Интернета», «Защита сети» и «Средства безопасности») и обеспечивает доступ к расширенным параметрам.

Справка и поддержка: информация о вашей подписки, установленном продукте ESET, а также ссылки на интернет-справку, базу знаний ESET и службу технической поддержки.

Учетная запись ESET HOME: подключение устройства к ESET HOME или просмотр состояния подключения к учетной записи ESET HOME. Используйте ESET HOME для просмотра настроек Антивор, активированной подписки ESET и устройств, а также управления ими.

Обзор

В окне **Обзор** отображается информация о текущем состоянии защиты компьютера и быстрые ссылки на функции безопасности в ESET Security Ultimate.

В окне **Обзор** отображаются уведомления с подробной информацией и рекомендуемыми решениями для повышения безопасности ESET Security Ultimate, включения дополнительных функций и обеспечения максимальной защиты. При наличии дополнительных уведомлений щелкните **Еще X уведомлений**, чтобы развернуть все.

Password Manager — открывает инструкции о том, как настроить Password Manager.

Инспектор сети — Проверьте безопасность своей сети.

Secure Data — открывает средства безопасности. Щелкните переключатель  рядом с **Secure Data**, чтобы включить это решение. Если вы уже включили Secure Data, с помощью быстрой ссылки открывается страница Secure Data.

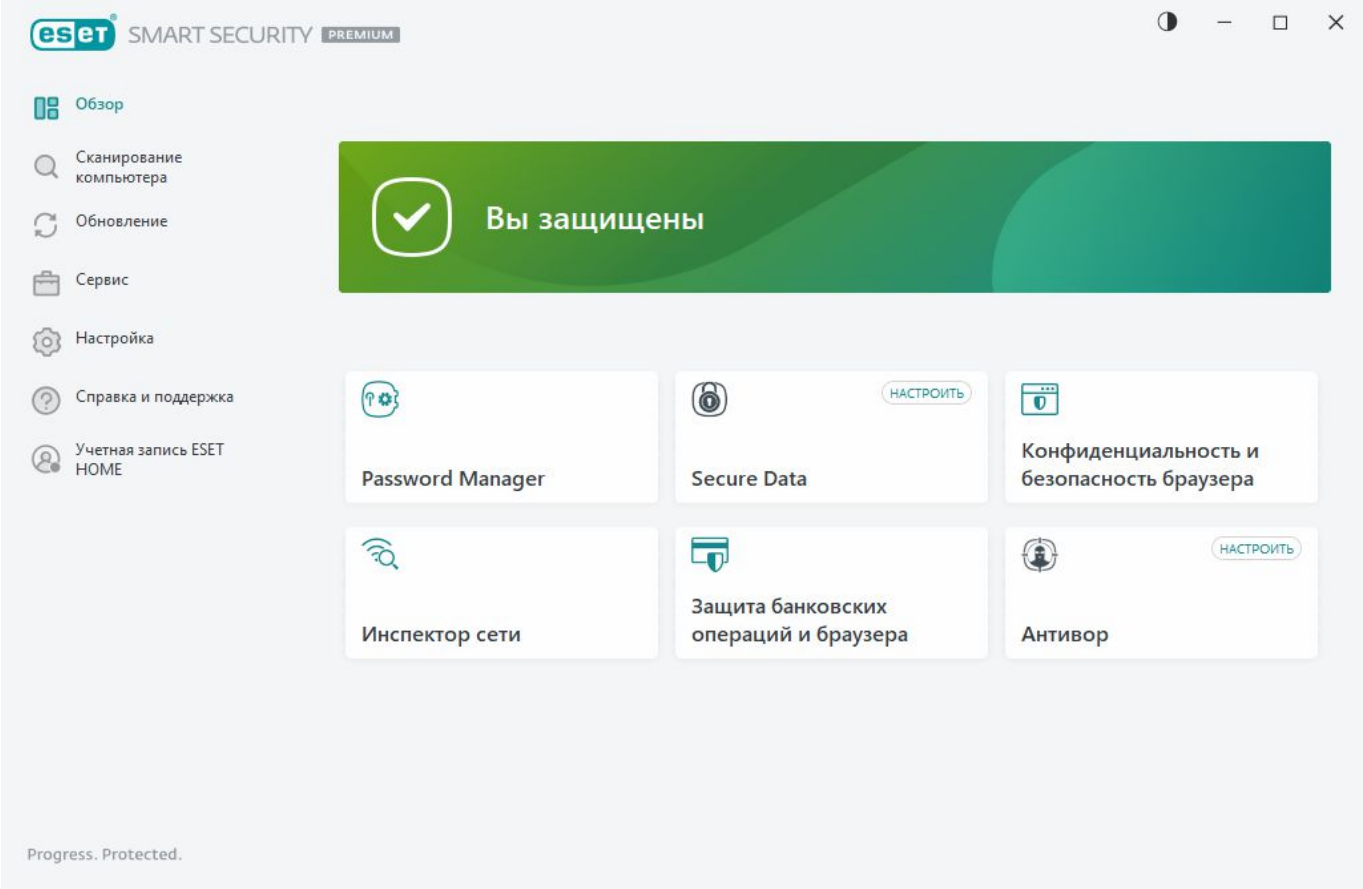
Защита банковских операций и браузера — запускает в защищенном режиме браузер, используемый по умолчанию в Windows.

Конфиденциальность и безопасность браузера: вы можете выбрать, какие расширения разрешено устанавливать в браузере, который защищен с помощью ESET.

Антивор — запускает настройку Антивор. Если вы уже настроили Антивор, с помощью быстрой ссылки открывается страница Антивор.

VPN — Храните свои данные в безопасности, избегайте нежелательного отслеживания и повысьте свою конфиденциальность с помощью дополнительной защиты, которую обеспечивает анонимный IP-адрес.

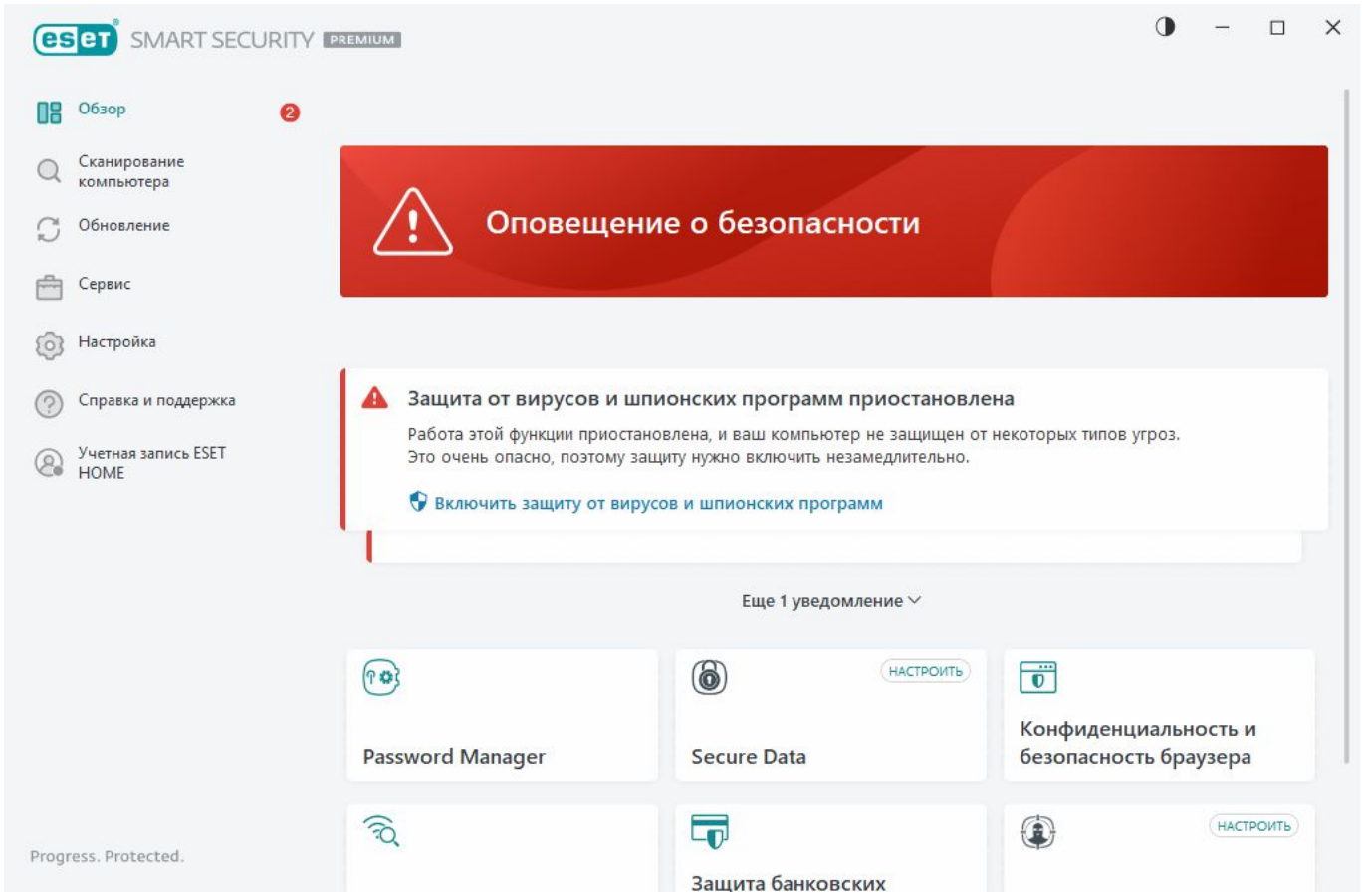
Identity Protection — защищает вашу личную, кредитную и финансовую информацию. Identity Protection выявляет незаконную продажу вашей личной информации, проводя непрерывный мониторинг.



Зеленый значок и зеленый статус **Вы под защитой** свидетельствуют о максимальном уровне защиты.

Устранение неполадок программы

Если модуль активной защиты работает правильно, значок состояния защиты будет зеленым. Красный восклицательный знак или оранжевый значок уведомления означает, что максимальная степень защиты не обеспечивается. Дополнительные сведения о состоянии защиты каждого модуля, а также предлагаемые решения для восстановления полной защиты отображаются в виде уведомления в окне **Обзор**. Для изменения состояния отдельного модуля щелкните **Настройка** и выберите необходимый модуль.



Красный значок и красный значок **оповещения по безопасности** указывают на критические проблемы.
Для отображения такого состояния может быть несколько причин.

- **Продукт не активирован**, или **Срок действия подписки истек** — об этом сигнализирует красный значок состояния защиты. После истечения срока действия подписки программа больше не сможет обновляться. Для продления подписки следуйте инструкциям в окне предупреждения.

- **Модуль обнаружения устарел**: эта ошибка появляется после нескольких неудачных попыток обновить модуль обнаружения. Рекомендуется проверить параметры обновлений. Наиболее частая причина этой ошибки — неправильно введенные данные для аутентификации или неверно настроенные параметры подключения.

- **Защита файловой системы в реальном времени отключена**: защита в реальном времени отключена пользователем. Компьютер не защищен от угроз. Нажмите **Включить защиту файловой системы в реальном времени**, чтобы повторно включить эту функцию.

- **Модули защиты от вирусов и шпионских программ отключены**: можно снова включить защиту от вирусов и шпионских программ, щелкнув **Включить защиту от вирусов и шпионских программ**.

- **Файервол ESET отключен**: об этой проблеме сигнализирует уведомление о защите на рабочем столе рядом с элементом **Сеть**. Чтобы повторно включить защиту сети, щелкните элемент **Включить файервол**.

Оранжевый цвет значка указывает на то, что действует ограниченная защита. Например, существуют проблемы с обновлением программы или заканчивается срок действия подписки.

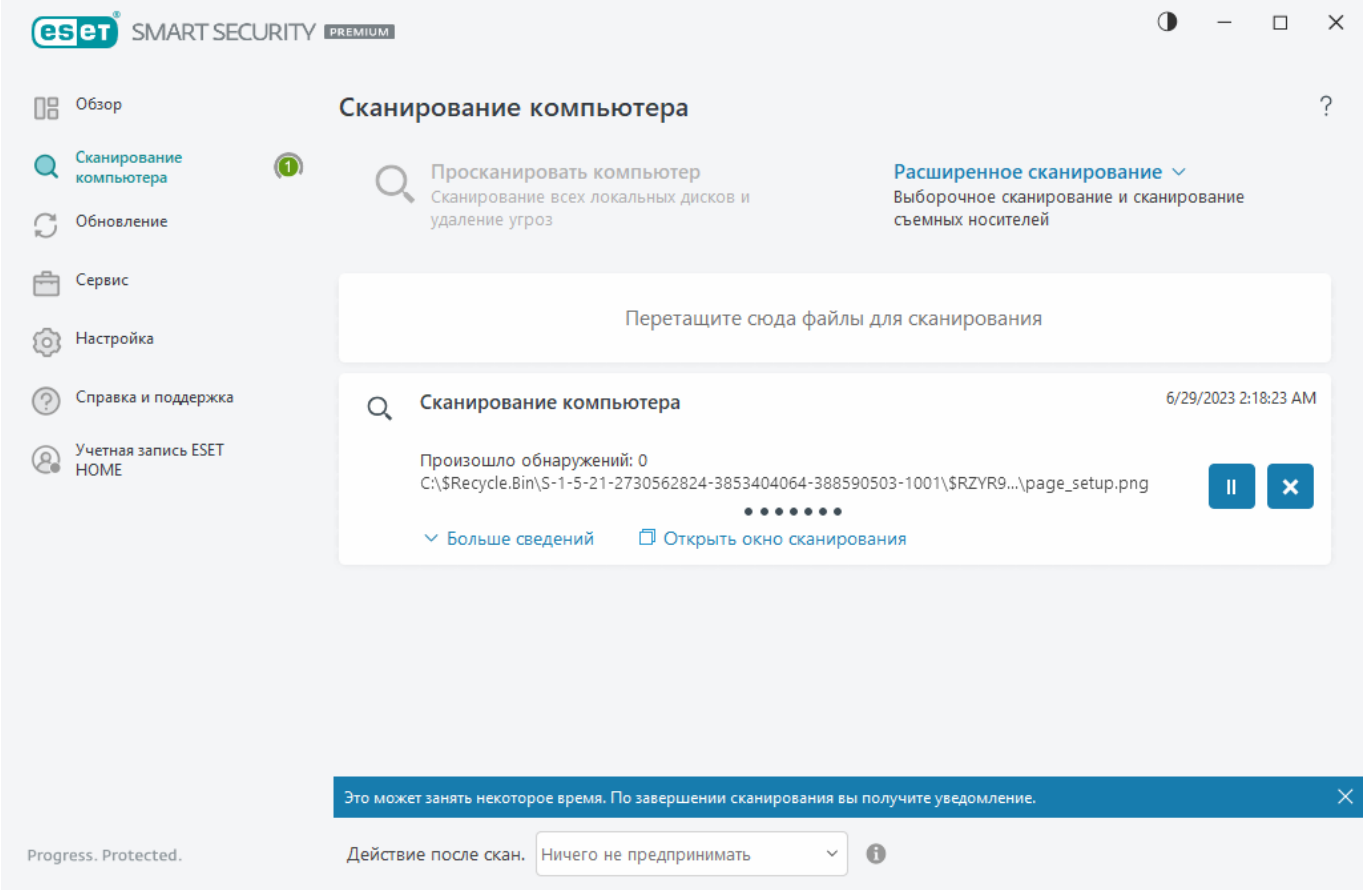
Для отображения такого состояния может быть несколько причин.

- **Предупреждение об оптимизации модуля «Антивор»**: это устройство не оптимизировано для модуля Антивор. Например, на вашем компьютере может быть не создана фантомная учетная запись (функция системы защиты, автоматически включаемая, когда устройство помечается как отсутствующее). Фантомную учетную запись можно создать с помощью функции Оптимизация в веб-интерфейсе Антивор.
- **Игровой режим активен**: включение игрового режима представляет потенциальный риск для безопасности. При включении этой функции блокируются все окна уведомлений или предупреждений и останавливаются все запланированные задачи.
- **Срок действия подписки скоро истечет/Срок действия подписки истекает сегодня**: признаком наличия этой проблемы является появление восклицательного знака в значке состояния защиты рядом с системными часами. После окончания срока действия подписки программа больше не сможет выполнять обновления, а значок состояния защиты станет красным.

Если предложенные решения не позволяют устранить проблему, выберите элемент **Справка и поддержка** и просмотрите файлы справки или поищите нужную информацию в базе знаний ESET. Если вам по-прежнему нужна помощь, отправьте свой запрос в службу технической поддержки ESET. Ее специалисты оперативно ответят на ваши вопросы и помогут найти решение.

Сканирование компьютера

Модуль сканирования компьютера по требованию является важной частью решения, обеспечивающего защиту от вирусов. Он используется для сканирования файлов и папок на компьютере. С точки зрения обеспечения безопасности принципиально важно выполнять сканирование компьютера регулярно, а не только при возникновении подозрений о заражении. Рекомендуется регулярно выполнять полное сканирование компьютера для обнаружения вирусов, которые не были найдены защитой файловой системы в режиме реального времени при записи на диск. Это может произойти, если в тот момент защита файловой системы в режиме реального времени была отключена, модуль обнаружения был устаревшим или же файл не был распознан как вирус при сохранении на диск.



Доступно два типа **сканирования компьютера**. **Сканирование компьютера** быстро сканирует систему без указания параметров сканирования. **Выборочное сканирование** (в разделе «Расширенное сканирование») позволяет выбрать один из предварительно определенных профилей сканирования, предназначенных для определенных местоположений и выбора определенных целей сканирования.

См. главу Ход сканирования для получения дополнительных сведений о процессе сканирования.

По умолчанию ESET Security Ultimate пытается автоматически очищать или удалять все опасные элементы, обнаруженные при сканировании компьютера. В некоторых случаях, когда не удается выполнить ни одно из действий, пользователь получает интерактивное уведомление, в котором нужно выбрать действие (например, удалить или проигнорировать). Изменить уровень очистки и получить более подробные сведения можно в разделе Очистка. Информацию о предыдущих сеансах сканирования см. в файлах журнала.

Просканировать компьютер

Функция **Просканировать компьютер** позволяет быстро запустить сканирование компьютера и очистить зараженные файлы без вмешательства пользователя. Преимущество функции **Просканировать компьютер** заключается в том, что оно удобно в выполнении и не требует тщательной настройки сканирования. При таком сканировании проверяются все файлы на локальных жестких дисках, а также автоматически очищаются или удаляются обнаруженные заражения. При этом автоматически используется уровень очистки по умолчанию. Дополнительную информацию о типах очистки см. в разделе Очистка.

Кроме того, можно использовать функцию **сканирования с использованием перетаскивания**, чтобы вручную сканировать файлы или папки: для этого наведите указатель мыши на нужный файл или папку, щелкните и, удерживая нажатой клавишу мыши, переместите выделенный элемент в отмеченную область, после чего отпустите кнопку мыши. После этого приложение будет переведено в фоновый режим.

В разделе **расширенных параметров сканирования** доступны следующие варианты сканирования.

 Выборочное сканирование

Выборочное сканирование позволяет указать параметры сканирования, такие как объекты и методы. Преимущество **выборочного сканирования** заключается в том, что вы можете детально конфигурировать параметры. Конфигурации можно сохранять в пользовательских профилях сканирования, которые удобно применять, если регулярно выполняется сканирование с одними и теми же параметрами.

 Сканирование съемных носителей

Подобно **сканированию компьютера** данная функция быстро запускает сканирование съемных носителей (например, CD/DVD/USB-дисков), которые подключены к компьютеру в данный момент. Это может быть удобно при подключении к компьютеру USB-устройства флэш-памяти, содержимое которого необходимо просканировать на наличие вредоносных программ и других потенциальных угроз.

Данный тип сканирования также можно запустить, выбрав вариант **Выборочное сканирование** и пункт **Съемные носители** в раскрывающемся меню **Объекты сканирования**, а затем нажав кнопку **Сканировать**.

 Повторить последнее сканирование

Позволяет быстро запустить последнее выполненное сканирование с использованием тех же настроек.

В раскрывающемся меню **Действие после сканирования** можно настроить действие, которое будет выполняться автоматически после завершения сканирования:

- **Ничего не предпринимать**: после сканирования действия предприниматься не будут.
- **Выключить**: после сканирования компьютер отключается.
- **Перезапуск при необходимости**: компьютер перезапускается, только если нужно завершить очистку обнаруженных угроз.
- **Перезагрузить**: после сканирования открытые программы закрываются, а компьютер перезагружается.
- **Принудительный перезапуск при необходимости**: компьютер принудительно перезапускается, только если нужно завершить очистку обнаруженных угроз.
- **Принудительная перезагрузка**: все открытые программы принудительно

закрываются, не дожидаясь вмешательства пользователя, и компьютер перезапускается после завершения сканирования.

• **Спящий режим**: сеанс сохраняется, и компьютер переходит в режим пониженного энергопотребления (т. е. пользователь может быстро возобновить работу).

• **Режим гибернации**: все компоненты, использующие ОЗУ, переносятся в специальный файл на жестком диске. Компьютер выключается, и при следующем включении вернется в предыдущее состояние.

Доступность действий **Сон** и **Гибернация** зависит от параметров питания и спящего режима операционной системы и возможностей вашего ноутбука или компьютера. Не забывайте, что компьютер в спящем режиме все же работает. Компьютер выполняет основные функции и потребляет электричество, когда работает от аккумулятора. Чтобы сохранить время работы батареи (например, если вы находитесь в пути), рекомендуется перевести компьютер в режим гибернации.

Выбранное действие будет запущено после того, как все запущенные процессы сканирования будут завершены. При выборе **Завершение работы** или **Перезагрузка** в диалоговом окне подтверждения будет отображаться 30-секундный обратный отсчет (щелкните **Отмена**, чтобы деактивировать запрошенное действие).

Сканирование компьютера рекомендуется запускать не реже одного раза в месяц. Его можно сконфигурировать в качестве запланированной задачи в разделе **Сервис** > **Планировщик**. Планирование еженедельного сканирования компьютера

Средство запуска выборочного сканирования

Выборочное сканирование позволяет сканировать оперативную память, сеть или определенные части диска (а не диск целиком). Для этого щелкните **Расширенное сканирование** > **Выборочное сканирование** и выберите конкретные объекты сканирования в древовидной структуре папок.

В раскрывающемся меню **Профиль** можно выбрать профиль, который будет использоваться для сканирования указанных объектов. По умолчанию используется профиль **Интеллектуальное сканирование**. Существует еще три предварительно заданных профиля сканирования: **Глубокое сканирование**, **Сканирование через контекстное меню** и **Сканирование компьютера**. В этих профилях сканирования используются другие параметры ThreatSense. Чтобы ознакомиться с доступными параметрами, последовательно выберите Расширенные параметры > **Модуль обнаружения** > **Сканирование на наличие вредоносных программ** > **Сканирование по требованию** > ThreatSense.

Структура папок (дерево) также содержит определенные объекты сканирования.

• **Оперативная память**: сканирование всех процессов и данных, которые в данный момент используются оперативной памятью.

• **Загрузочные секторы/UEFI**: сканирование загрузочных секторов и UEFI на наличие вредоносных программ. Дополнительные сведения о модуле сканирования UEFI приведены

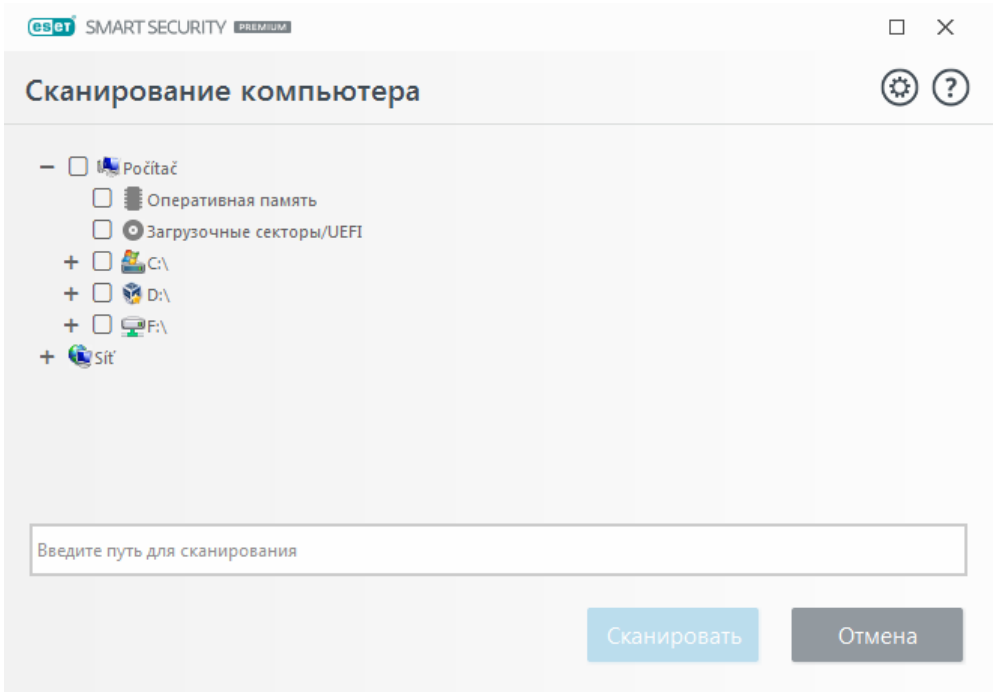
в глоссарии.

• **База данных WMI**: сканирование всей базы данных Windows Management Instrumentation (WMI), всех пространств имен, экземпляров классов и всех свойств. Поиск ссылок на зараженные файлы или вредоносные программы, внедренные в виде данных.

• **Системный реестр**: сканирование всего системного реестра, всех разделов и подразделов. Поиск ссылок на зараженные файлы или вредоносные программы, внедренные в виде данных. При очистке обнаружений ссылка остается в реестре во избежание потери каких-либо важных данных.

Чтобы быстро перейти к объекту сканирования (файлу или папке), введите его путь в текстовом поле под древовидной структурой. Путь вводится с учетом регистра. Чтобы включить объект в сканирование, установите его флажок в древовидной структуре.

> **Планирование еженедельного сканирования компьютера**
> Чтобы узнать, как запланировать регулярную задачу, см. раздел Планирование еженедельного сканирования компьютера.



Параметры очистки для сканирования можно настроить в разделе Расширенные параметры > **Модуль обнаружения** > **Процессы сканирования вредоносных программ** > **Сканирование по требованию** > **ThreatSense** > **Очистка**. Чтобы выполнить сканирование без очистки, щелкните **Дополнительные параметры** и выберите **Сканировать без очистки**. История сканирования сохраняется в журнале сканирования.

Если выбран параметр **Пропустить исключения**, файлы с ранее исключенными расширениями будут просканированы без исключений.

Нажмите кнопку **Сканировать**, чтобы выполнить сканирование с выбранными параметрами.

Кнопка **Сканировать с правами администратора** позволяет выполнять сканирование под учетной записью администратора. Воспользуйтесь этой функцией, если у текущего пользователя нет прав на доступ к файлам, которые следует просканировать. Данная кнопка

недоступна, если текущий пользователь не может вызывать операции контроля учетных записей в качестве администратора.

> Журнал сканирования можно просмотреть по завершении сканирования, нажав кнопку Показать журналы.

Ход сканирования

В окне хода сканирования отображается текущее состояние сканирования и информация о количестве файлов, в которых обнаружен злонамеренный код.

> Нормальной ситуацией является невозможность сканирования некоторых файлов, например защищенных паролем файлов или файлов, используемых исключительно операционной системой (обычно *pagefile.sys* и некоторых файлов журналов). Более подробную информацию можно найти в статье нашей базы знаний.

> **Планирование еженедельного сканирования компьютера**
> Чтобы узнать, как запланировать регулярную задачу, см. раздел Планирование еженедельного сканирования компьютера.

Ход сканирования: индикатор выполнения показывает состояние текущего сканирования.

Объект: имя объекта, который сканируется в настоящий момент, и его расположение.

Произошли обнаружения: отображается общее количество просканированных файлов и угроз, обнаруженных и удаленных во время сканирования.

Щелкните элемент «Дополнительные сведения», чтобы отобразить следующую информацию:

- **Пользователь**: имя учетной записи пользователя, который запустил сканирование.
- **Просканировано объектов**: количество уже просканированных объектов.
- **Продолжительность**: прошедшее время.

Значок паузы: приостановка сканирования.

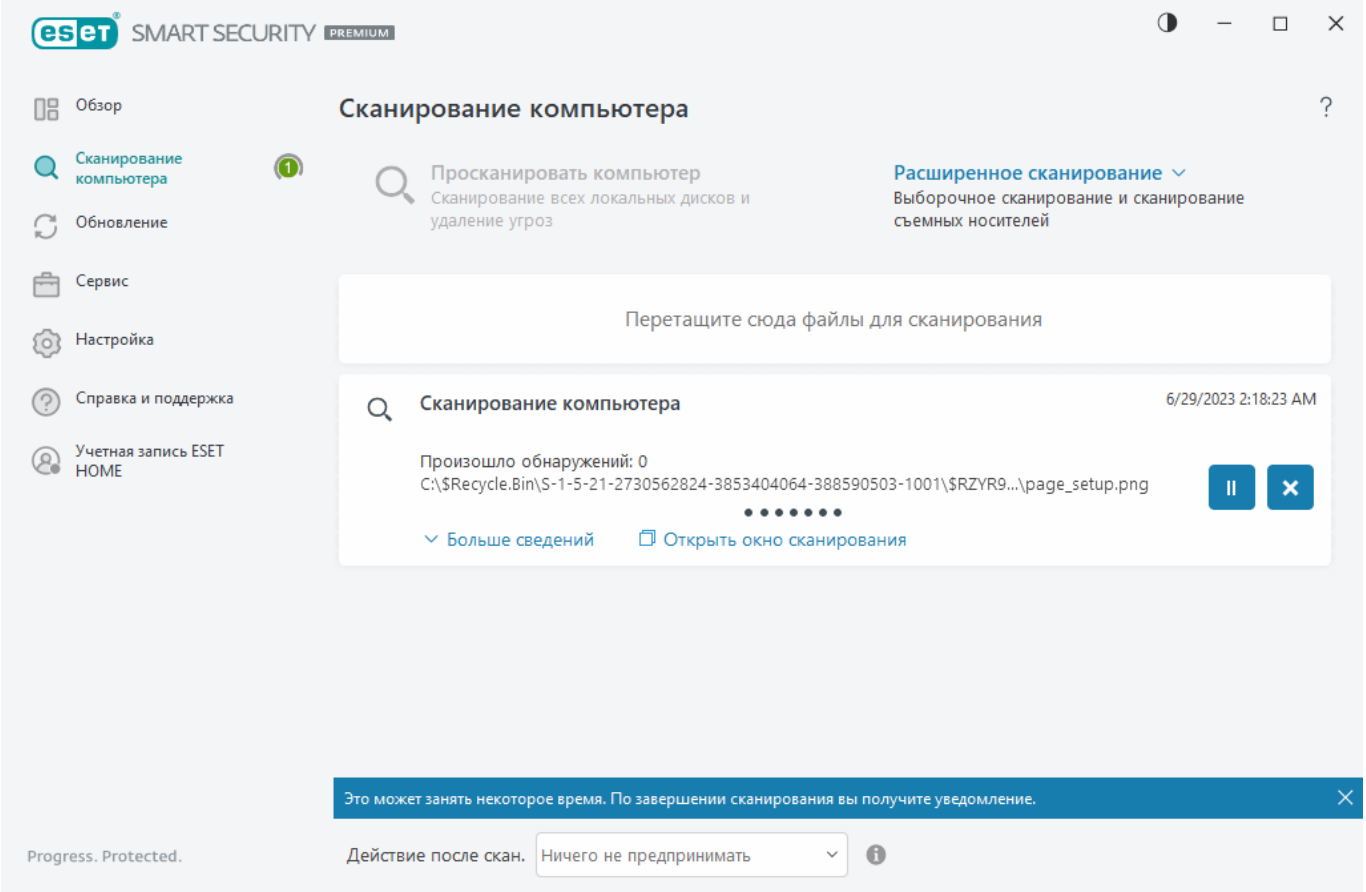
Значок возобновления: эта опция отображается, когда сканирование приостановлено. Щелкните этот значок, чтобы продолжить сканирование.

Значок остановки: завершение сканирования.

Щелкните элемент **Открыть окно сканирования**, чтобы открыть журнал сканирования компьютера с более подробной информацией о сканировании.

Прокрутить журнал сканирования: если этот параметр активирован, журнал сканирования будет прокручиваться автоматически при добавлении новых записей, чтобы отображались самые свежие элементы.

Щелкните экранную лупу или стрелку, чтобы просмотреть сведения о текущем сканировании. Можно параллельно запустить другое сканирование, щелкнув **Сканировать компьютер** или **Расширенное сканирование** > **Выборочное сканирование**.



В раскрывающемся меню **Действие после сканирования** можно настроить действие, которое будет выполняться автоматически после завершения сканирования:

- **Ничего не предпринимать**: после сканирования действия предприниматься не будут.
- **Выключить**: после сканирования компьютер отключается.
- **Перезапуск при необходимости**: компьютер перезапускается, только если нужно завершить очистку обнаруженных угроз.
- **Перезагрузить**: после сканирования открытые программы закрываются, а компьютер перезагружается.
- **Принудительный перезапуск при необходимости**: компьютер принудительно перезапускается, только если нужно завершить очистку обнаруженных угроз.
- **Принудительная перезагрузка**: все открытые программы принудительно закрываются, не дожидаясь вмешательства пользователя, и компьютер перезапускается после завершения сканирования.
- **Спящий режим**: сеанс сохраняется, и компьютер переходит в режим пониженного энергопотребления (т. е. пользователь может быстро возобновить работу).
- **Режим гибернации**: все компоненты, использующие ОЗУ, переносятся в специальный

файл на жестком диске. Компьютер выключается, и при следующем включении вернется в предыдущее состояние.

Доступность действий **Сон** и **Гибернация** зависит от параметров питания и спящего режима операционной системы и возможностей вашего ноутбука или компьютера. Не забывайте, что компьютер в спящем режиме все же работает. Компьютер выполняет основные функции и потребляет электричество, когда работает от аккумулятора. Чтобы сохранить время работы батареи (например, если вы находитесь в пути), рекомендуется перевести компьютер в режим гибернации.

Выбранное действие будет запущено после того, как все запущенные процессы сканирования будут завершены. При выборе **Завершение работы** или **Перезагрузка** в диалоговом окне подтверждения будет отображаться 30-секундный обратный отсчет (щелкните **Отмена**, чтобы деактивировать запрошенное действие).

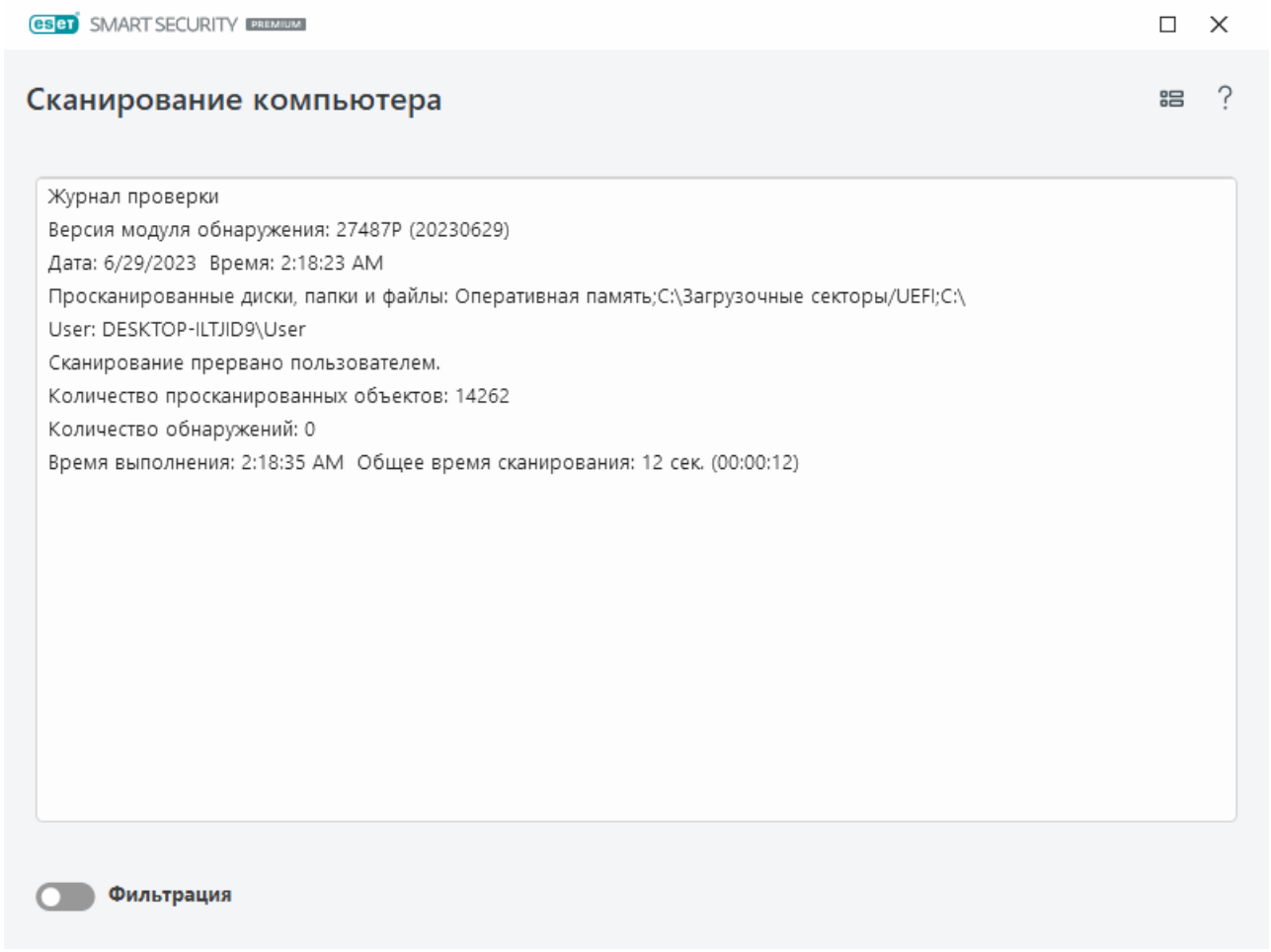
Журнал проверки сканирования компьютера

В разделе Файлы журнала можно просмотреть подробную информацию, связанную с конкретным сканированием. Журнал сканирования содержит следующие сведения:

- Версия модуля обнаружения
- дата и время начала;
- список просканированных дисков, папок и файлов;
- Имя сканирования по расписанию (только сканирование по расписанию)
- пользователь, запустивший сканирование;
- Состояние сканирования
- число просканированных объектов;
- количество обнаружений;
- время завершения;
- общее время сканирования.

Новый запуск задания сканирования компьютера по расписанию пропускается, если все еще выполняется то же задание по расписанию, которое выполнялось ранее. В случае пропуска задания сканирования по расписанию будет создан журнал проверки компьютера с просканированными объектами в количестве 0 и статусом **Сканирование не началось, поскольку все еще выполнялось предыдущее сканирование**.

Чтобы найти предыдущие журналы сканирования, в главном окне программы выберите **Сервис** > **Файлы журнала**. В раскрывающемся меню выберите **Сканирование компьютера** и дважды щелкните нужную запись.



Дополнительные сведения о записях «Не удается открыть», «Ошибка открытия» и/или «Архив поврежден» см. в статье базы знаний ESET.

Щелкните значок переключателя **Фильтрация**, чтобы открыть окно Фильтрация журнала, где можно уточнить поиск, задав пользовательские критерии. Чтобы просмотреть контекстное меню, щелкните правой кнопкой мыши запись в журнале:

Действие	Использование
Фильтрация одинаковых записей	Активирует фильтрацию журнала. В журнале будут отображаться только записи того же типа, что у выбранной записи.
Фильтр	При выборе этого параметра отображается окно «Фильтрация журнала», в котором можно задать критерии фильтрации для определенных записей журнала. Сочетание клавиш: `Ctrl+Shift+F`.
Включить фильтр	Активирует параметры фильтра. Если вы активируете фильтр в первый раз, нужно установить параметры, и откроется окно «Фильтрация журнала».
Отключить фильтр	Выключает фильтр (то же самое, что щелкнуть переключатель внизу).
Копировать	Копирует выделенные записи в буфер обмена. Сочетание клавиш: `Ctrl+C`.
Копировать все	Копирует все записи в окне.
Экспорт	Экспортирует выделенные записи в XML-файл.
Экспортировать все	Экспортирует все записи в окне в XML-файл.

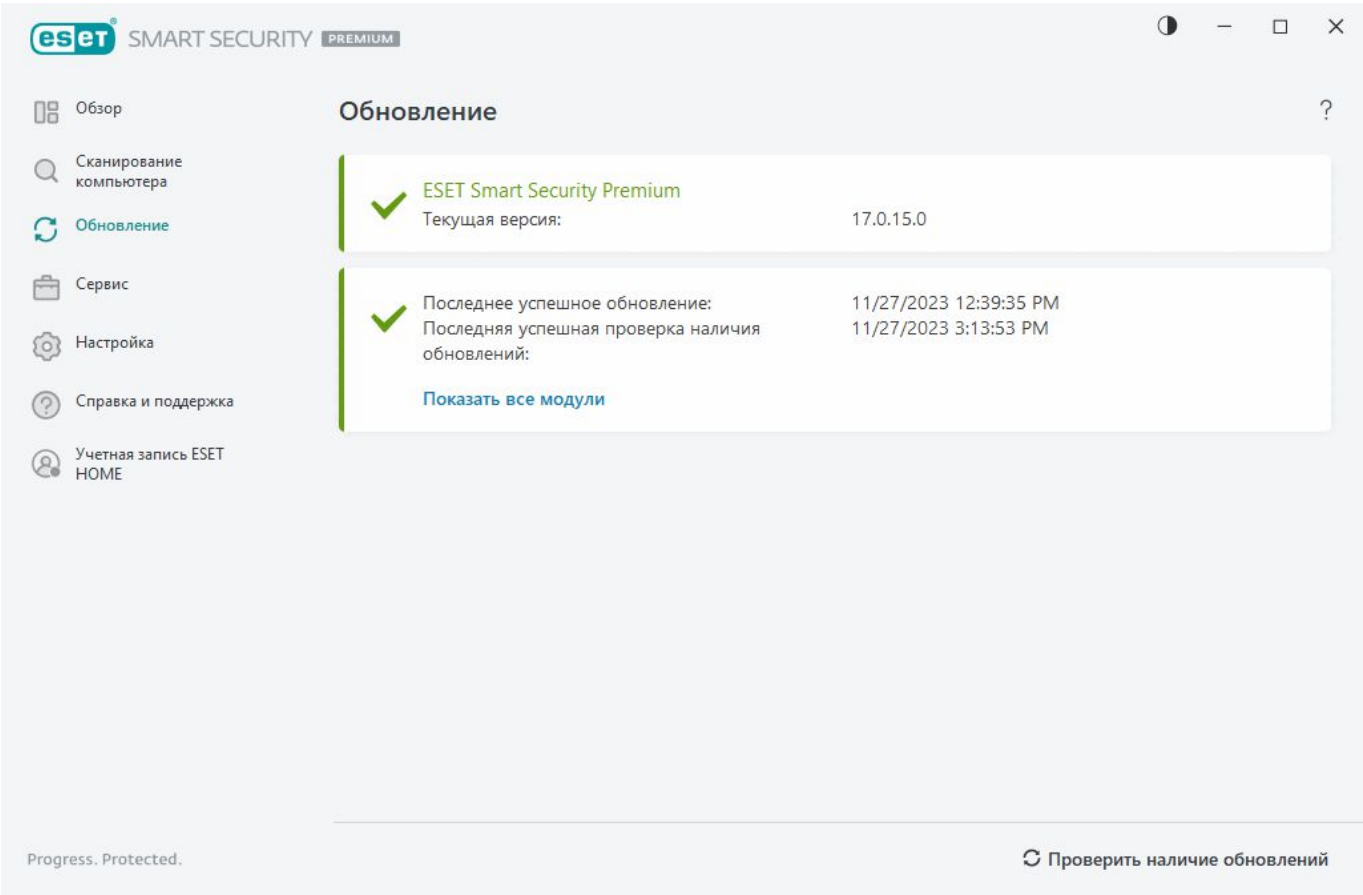
Действие	Использование
Описание обнаружения	Открывает энциклопедию угроз ESET, которая содержит подробную информацию об опасностях и симптомах выделенного заражения.

Обновление

Регулярное обновление ESET Security Ultimate — лучший способ обеспечить максимальный уровень безопасности компьютера. Модуль обновления поддерживает актуальность программных модулей и компонентов системы.

Выбрав пункт **Обновление** в главном окне программы, можно просмотреть информацию о текущем состоянии обновления, в том числе дату и время последнего успешно выполненного обновления, а также сведения о необходимости обновления.

Кроме автоматического обновления, можно выполнить обновление вручную, нажав кнопку **Проверить наличие обновлений**. Регулярное обновление программных модулей и компонентов является важным аспектом обеспечения полной защиты от вредоносного кода. Уделите особое внимание конфигурированию и работе программных модулей. Для получения обновлений необходимо активировать продукт с помощью вашего ключа активации. Если это не было сделано во время установки, вам потребуется активировать ESET Security Ultimate, чтобы получить доступ к серверам обновления ESET. Компания ESET отправила вам ключ активации по электронной почте после приобретения ESET Security Ultimate.



Текущая версия: отображается номер текущей установленной версии продукта.

Последнее успешное обновление: отображается дата последнего успешного обновления.

Если не отображается недавняя дата, возможно, ваши модули продукта неактуальны.

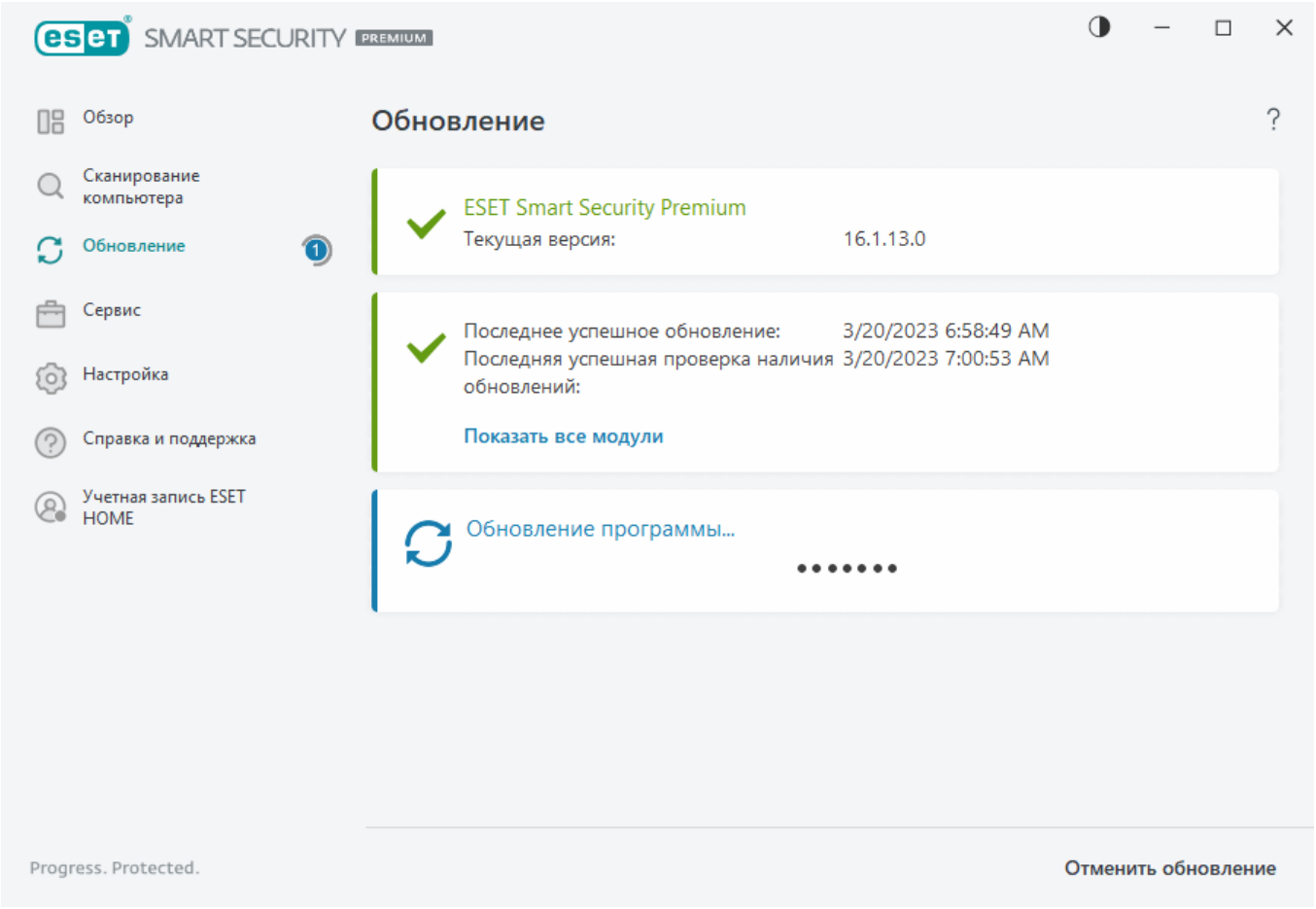
Последняя успешная проверка на наличие обновлений: отображается дата последней успешной проверки на наличие обновлений.

Показать все модули: отображается список установленных программных модулей.

Щелкните **Проверить наличие обновлений**, чтобы проверить наличие последней доступной версии ESET Security Ultimate.

Процесс обновления

После нажатия кнопки **Проверить наличие обновлений** начинается загрузка. На экран будут выведены индикатор выполнения загрузки и время до ее окончания. Чтобы прервать обновление, нажмите кнопку **Отменить обновление**.



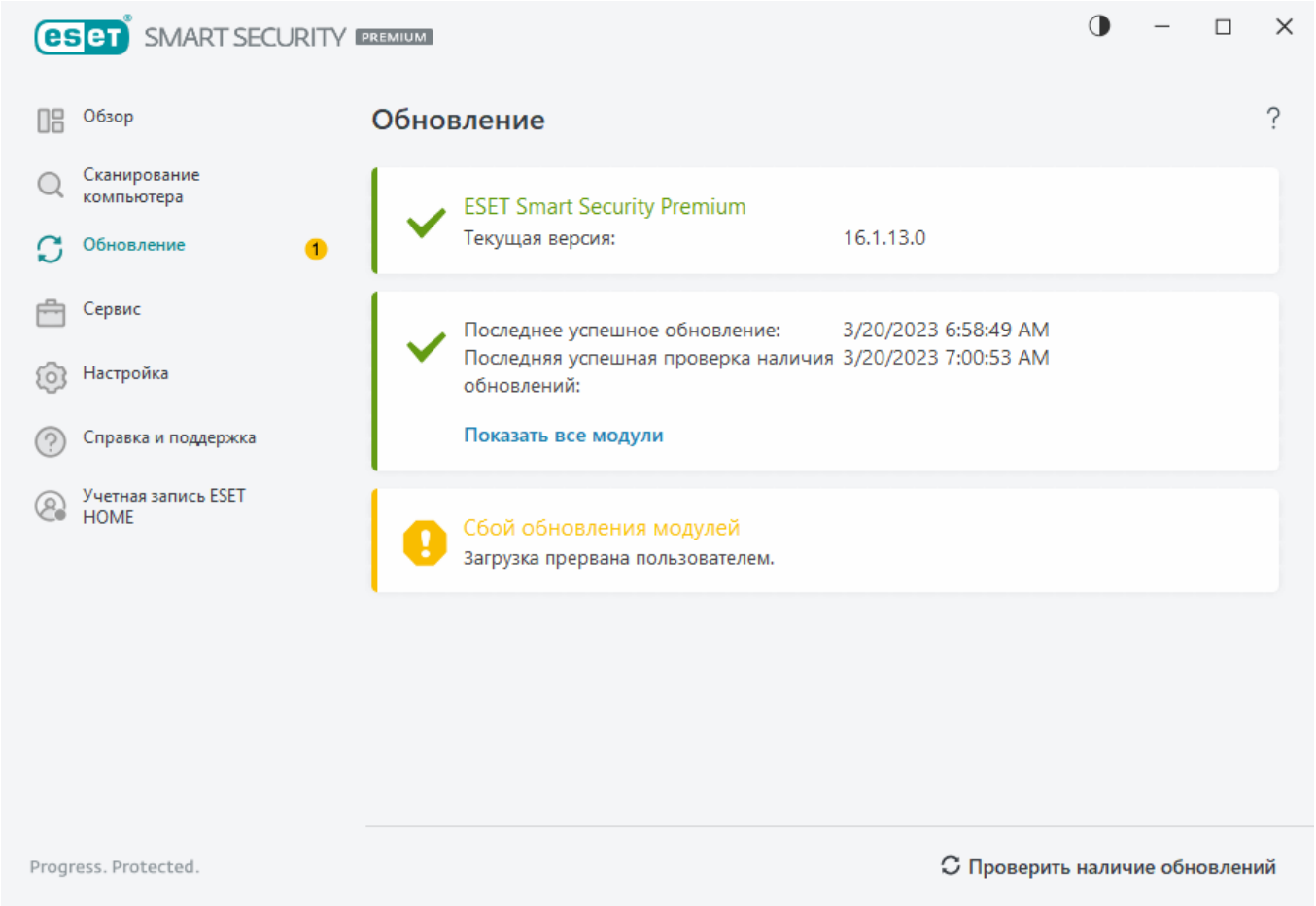
Обычно в окне **Обновление** отображается зеленый флажок, указывающий на то, что установлена актуальная версия программы. Если вы не видите этот флажок, программа устарела. При этом повышается риск заражения. Обновите модули программы как можно скорее.

Ошибка обновления

Если вы получили сообщение о том, что обновить модули не удалось, у этого может быть несколько причин.

1. **Недействительная подписка**: используемая для активации подписка недействительна, или срок ее действия истек. В главном окне программы щелкните **Справка и поддержка** > **Изменить подписку** и активируйте свой продукт.

2. **При загрузке файлов обновлений произошла ошибка**: возможная причина этой ошибки — неправильные параметры подключения к Интернету. Рекомендуется проверить наличие подключения к Интернету (например, попробуйте открыть любой веб-сайт в браузере). Если веб-сайт не открывается, возможно, не установлено подключение к Интернету или на компьютере возникли какие-либо проблемы с подключением к сети. Обратитесь к своему поставщику услуг Интернета, чтобы выяснить, есть ли у вас активное подключение к Интернету.



Перезапустите компьютер после обновления продукта ESET Security Ultimate до более новой версии, чтобы убедиться, что все модули программы обновлены надлежащим образом. При регулярном обновлении модулей выполнять перезагрузку нет необходимости.

Дополнительные сведения можно найти в статье Устранение проблемы с сообщением «Не удалось обновить модули».

Диалоговое окно — требуется перезапуск

После обновления ESET Security Ultimate до новой версии требуется перезапуск компьютера. Новые версии ESET Security Ultimate выпускаются для реализации улучшений или исправления проблем, которые не могут быть устранены автоматическими обновлениями модулей программы.

Новую версию ESET Security Ultimate можно установить автоматически на основе настроек обновления программы или вручную путем загрузки и установки более новой версии поверх предыдущей.

Нажмите кнопку **Перезапустить сейчас**, чтобы перепустить компьютер. Если вы планируете перезапустить компьютер позже, нажмите кнопку **«Напомнить позже»**. Позже можно будет перезапустить компьютер вручную из раздела **Обзор** в главном окне программы.

Создание задач обновления

Обновление можно запустить вручную, нажав **Проверить наличие обновлений** в основном окне, которое появляется после выбора пункта **Обновление** в главном меню.

Обновления также можно выполнять как запланированную задачу. Для конфигурирования запланированной задачи щелкните **Сервис** > **Планировщик**. По умолчанию в ESET Security Ultimate активированы указанные ниже задачи обновления:

- **Регулярное автоматическое обновление**
- **Автоматическое обновление после входа пользователя в систему**

Каждую задачу обновления можно изменить в соответствии с конкретными требованиями. Кроме задач по умолчанию можно создать другие задачи обновления с пользовательскими настройками. Дополнительную информацию о создании и настройке задач обновления см. в разделе Планировщик.

Служебные программы

В меню **Инструменты** доступны функции, которые обеспечивают дополнительную защиту и упрощают администрирование ESET Security Ultimate. Доступны следующие средства:

 Файлы журналов

 Запущенные процессы (если использование системы ESET LiveGrid® включено в ESET Security Ultimate)

 Отчет по безопасности

 Сетевые подключения (если Файервол включен в программе ESET Security Ultimate)

ESET SysInspector

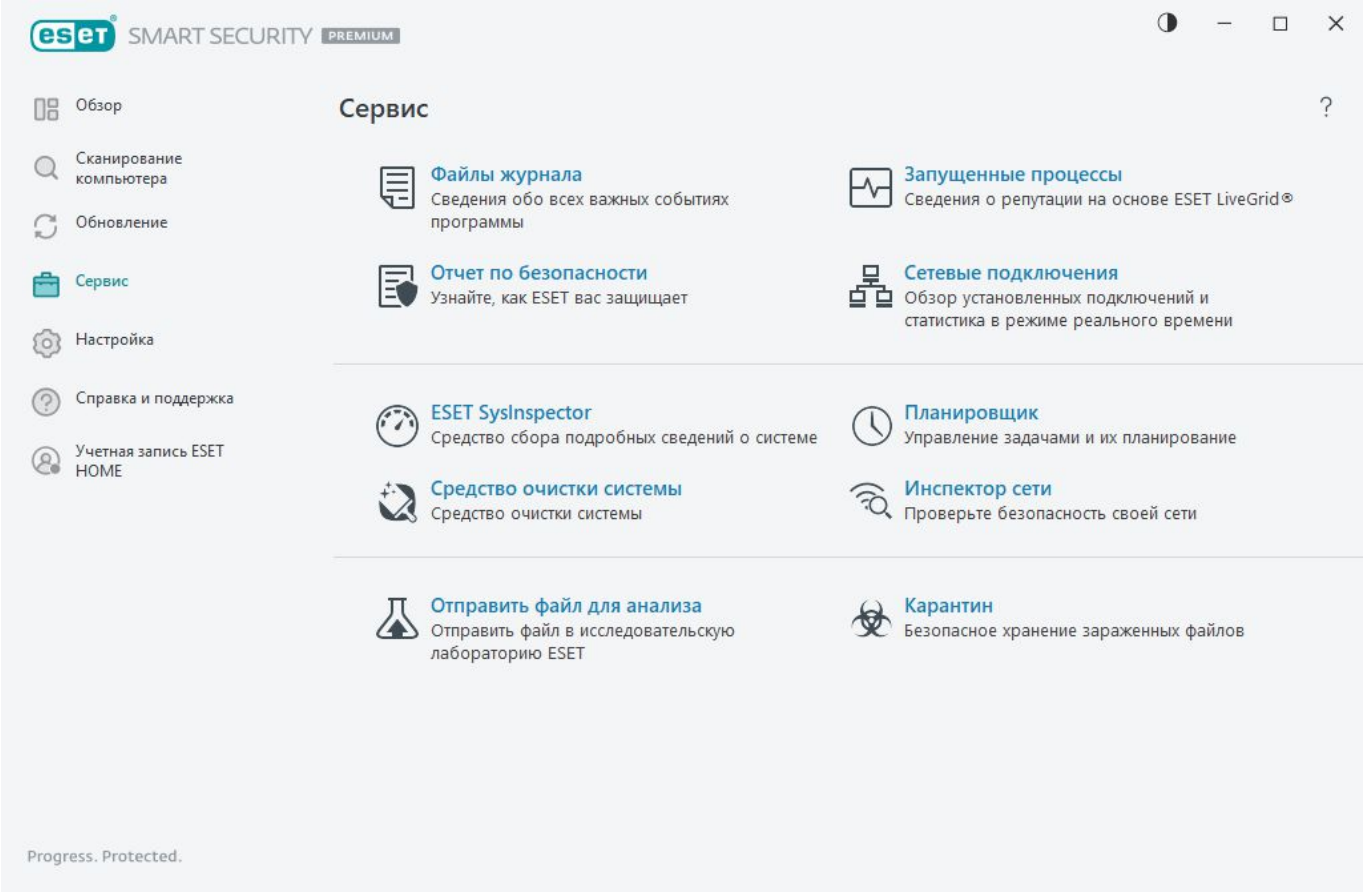
Планировщик

Средство очистки системы

Инспектор сети

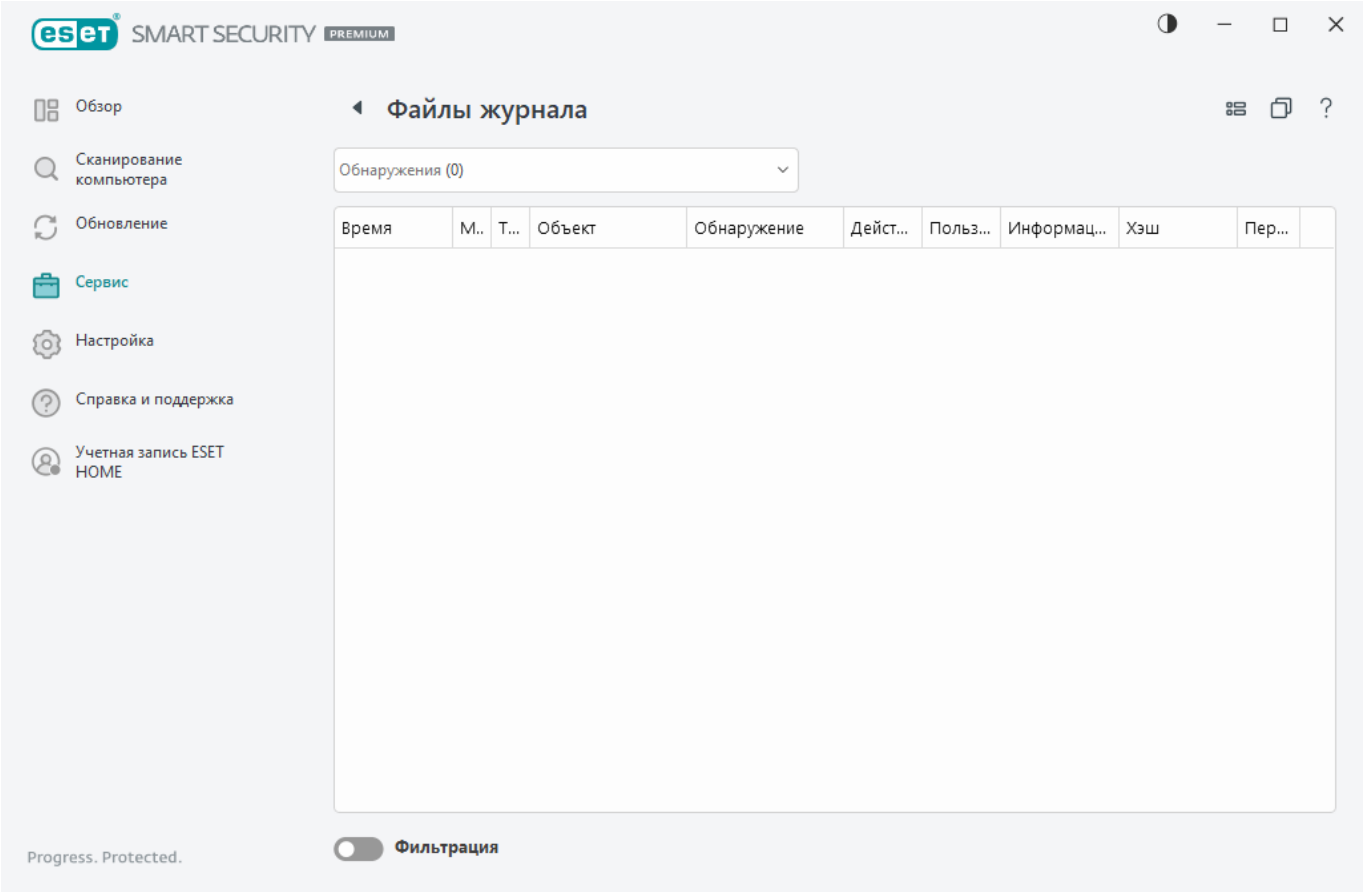
Отправка образца на анализ (функция может быть недоступна в зависимости от конфигурации ESET LiveGrid®).

Карантин



Файлы журнала

Файлы журналов содержат информацию о важных программных событиях и сводные сведения об обнаруженных угрозах. Ведение журнала является важнейшим элементом анализа системы, обнаружения угроз и устранения проблем. Оно выполняется в фоновом режиме без вмешательства пользователя. Данные сохраняются в соответствии с текущими параметрами степени детализации журнала. Просматривать текстовые сообщения и файлы журналов, а также архивировать их можно непосредственно в среде ESET Security Ultimate.



Получить доступ к файлам журнала можно из главного окна программы с помощью команды **Служебные программы** > **Файлы журнала**. Выберите нужный тип журнала в раскрывающемся меню Журнал.

• **Обнаружения**: этот журнал содержит подробную информацию об угрозах и заражениях, обнаруженных программой ESET Security Ultimate. Регистрируется время обнаружения, тип модуля сканирования, тип объекта, расположение объекта, название обнаружения, выполненное действие, имя пользователя, который находился в системе при обнаружении заражения, хеш и первое появление. Неочищенные заражения всегда отмечены красным текстом на розовом фоне. Очищенные заражения отмечаются желтым текстом на белом фоне. Неочищенные потенциально опасные приложения (PUA) отмечаются желтым текстом на белом фоне.

• **События**: в журнале событий регистрируются все важные действия, выполняемые программой ESET Security Ultimate. Он содержит информацию о событиях и ошибках, которые произошли во время работы программы. Он должен помогать системным администраторам и пользователям решать проблемы. Зачастую информация, которая содержится в этом журнале, оказывается весьма полезной при решении проблем, возникающих в работе программы.

• **Сканирование компьютера**: в этом окне отображаются результаты всех выполненных операций сканирования. Каждая строка соответствует одной проверке компьютера. Дважды щелкните любую запись, чтобы просмотреть сведения о выбранном сканировании.

• **Отправленные файлы**: здесь содержатся записи об образцах, отправленных в ESET LiveGuard.

• **HIPS**: здесь содержатся записи конкретных правил системы предотвращения вторжений на узел, которые помечены для регистрации. В протоколе отображается приложение, которое запустило операцию, ее результат (разрешение или запрещение правила) и имя правила.

• **Защита браузера**: содержит записи непроверенных/недоверенных файлов, загруженных в браузере.

• **Защита сети**: в журнале защиты сети отображаются все попытки удаленных атак, которые обнаружили файервол, средство защиты от сетевых атак (IDS) и защиты от ботнетов. В нем находится информация обо всех атаках, которые были направлены на компьютер пользователя. В столбце Событие отображаются обнаруженные атаки. В столбце Источник указываются дополнительные сведения о злоумышленнике. В столбце Протокол перечисляются протоколы обмена данными, которые использовались для атаки. Анализ журнала защиты сети может помочь своевременно обнаружить попытки заражения компьютера, чтобы предотвратить несанкционированный доступ. Дополнительные сведения о сетевых атаках см. в разделе IDS и расширенные параметры.

• **Отфильтрованные веб-сайты**: Этот список полезен, если вы хотите просмотреть список веб-сайтов, заблокированных защитой доступа в Интернет или родительским контролем. В каждом журнале указываются время, URL-адрес, пользователь и приложение, с помощью которого установлено подключение к конкретному веб-сайту.

• **Защита почтового клиента от спама**: содержит записи, связанные с сообщениями электронной почты, которые были помечены как спам.

• **Родительский контроль**: содержит список веб-страниц, разрешенных или заблокированных функцией родительского контроля. В столбцах Тип соответствия и Значения соответствия указывается, какие правила фильтрации были применены.

• **Контроль устройств**: содержит список подключенных к компьютеру съемных носителей и устройств. В журнале регистрируются только те устройства, которые соответствуют правилу контроля. В противном случае в журнале не создаются записи о них. Здесь же отображаются такие сведения, как тип устройства, серийный номер, имя поставщика и размер носителя (при его наличии).

• **Защита веб-камеры**: содержит сведения о приложениях, заблокированных модулем защиты веб-камеры.

Выделите содержимое любого журнала и нажмите клавиши **CTRL + C**, чтобы скопировать его в буфер обмена. Удерживайте клавишу **CTRL** или **SHIFT**, чтобы выделить несколько записей.

Щелкните элемент **Фильтрация**, чтобы открыть окно Фильтрация журнала, где можно задать критерии фильтрации.

Щелкните правой кнопкой мыши определенную запись, чтобы открыть контекстное меню. В контекстном меню доступны перечисленные ниже параметры.

• **Показать**: просмотр в новом окне подробной информации о выбранном журнале.

• **Фильтрация одинаковых записей**: после активации этого фильтра будут показаны только записи одного типа (диагностические записи, предупреждения и т. д.).

• **Фильтр**: при выборе этого параметра на экран выводится окно Фильтрация журнала, в котором можно задать критерии фильтрации для определенных записей журнала.

• **Включить фильтр**: активация настроек фильтра.

• **Отключить фильтр**: удаляются все параметры фильтра (созданные, как описано выше).

• **Копировать/копировать все**: копирование информации о выбранных записях.

• **Копировать ячейку**: копирование содержимого ячейки по ее щелчку правой кнопкой мыши.

• **Удалить/удалить все**: удаление выделенных записей или всех отображаемых записей. Для этого действия нужны права администратора.

• **Экспорт/Экспортировать все**: экспорт информации о выбранных записях или всех записях в формате XML.

• **Найти/Найти следующее/Найти ранее**: щелкнув этот параметр, можно определить критерии фильтрации, чтобы выделить определенную запись в окне «Фильтрация журнала».

• **Описание обнаружения**: открывает энциклопедию угроз ESET, которая содержит подробную информацию об опасностях и симптомах зарегистрированного заражения.

• **Создать исключение**: создание нового Исключения из обнаружения с помощью мастера (Недоступно для обнаружения вредоносных программ).

• **Добавить в список разрешенных объектов для защиты браузера**: открывает окно Список разрешенных объектов для защиты браузера и добавляет элемент в список.

Фильтрация журнала

Чтобы указать критерии фильтрации, выберите **Сервис** > **Файлы журнала** и щелкните **Фильтрация**.

С помощью функции фильтрации журналов можно найти нужную информацию среди множества записей. Эта функция позволяет сузить круг, если вы ищете записи журнала по типу события, состоянию или периоду времени. Можно отфильтровать записи журнала по определенным параметрам поиска. В окне «Файлы журналов» отобразятся только записи, которые соответствуют этим параметрам.

В поле **Найти текст** введите ключевое слово для поиска. Используйте раскрывающееся меню **Искать в столбцах**, чтобы уточнить условия поиска. Выберите одну или несколько записей в раскрывающемся меню **Типы записей журнала**. Задайте **период времени**, результаты за который нужно вывести на экран. Можете также использовать другие параметры поиска, например **Только слова целиком** или **С учетом регистра**.

Найти текст

Введите строку (слово целиком или частично). Появятся только записи, в которых содержится эта строка. Остальные записи будут опущены.

Искать в столбцах

Выберите, какие столбцы будут учитываться при поиске. Для использования в поиске можно отметить один столбец или сразу несколько.

Типы записей

Выберите один или несколько типов записей журнала в раскрывающемся меню.

• **Диагностика**: в журнал вносится информация, необходимая для тщательной настройки программы, и все перечисленные выше записи.

• **Информация**: в журнал вносятся информационные сообщения, в том числе сообщения об успешном выполнении обновления, а также все перечисленные выше записи.

• **Предупреждения**: в журнал вносится информация обо всех критических ошибках и предупреждениях.

• **Ошибки**: в журнал вносится информация об ошибках загрузки файлов и критических ошибках.

• **Критическое**: регистрируются только критические ошибки (ошибки запуска защиты от вирусов,

Период времени, с

Период времени: задайте период времени, результаты за который нужно вывести на экран:

• **Не указано** (по умолчанию). Поиск по периоду времени не выполняется, а ведется в журнале целиком.

• **Прошлый день**

• **Прошлая неделя**

• **Прошлый месяц**

• **Период времени**. Можно указать определенный период времени (начало и конец периода), чтобы отфильтровать записи по нему.

Только слова целиком

Установите этот флажок, если для получения более точных результатов нужно искать определенные слова целиком.

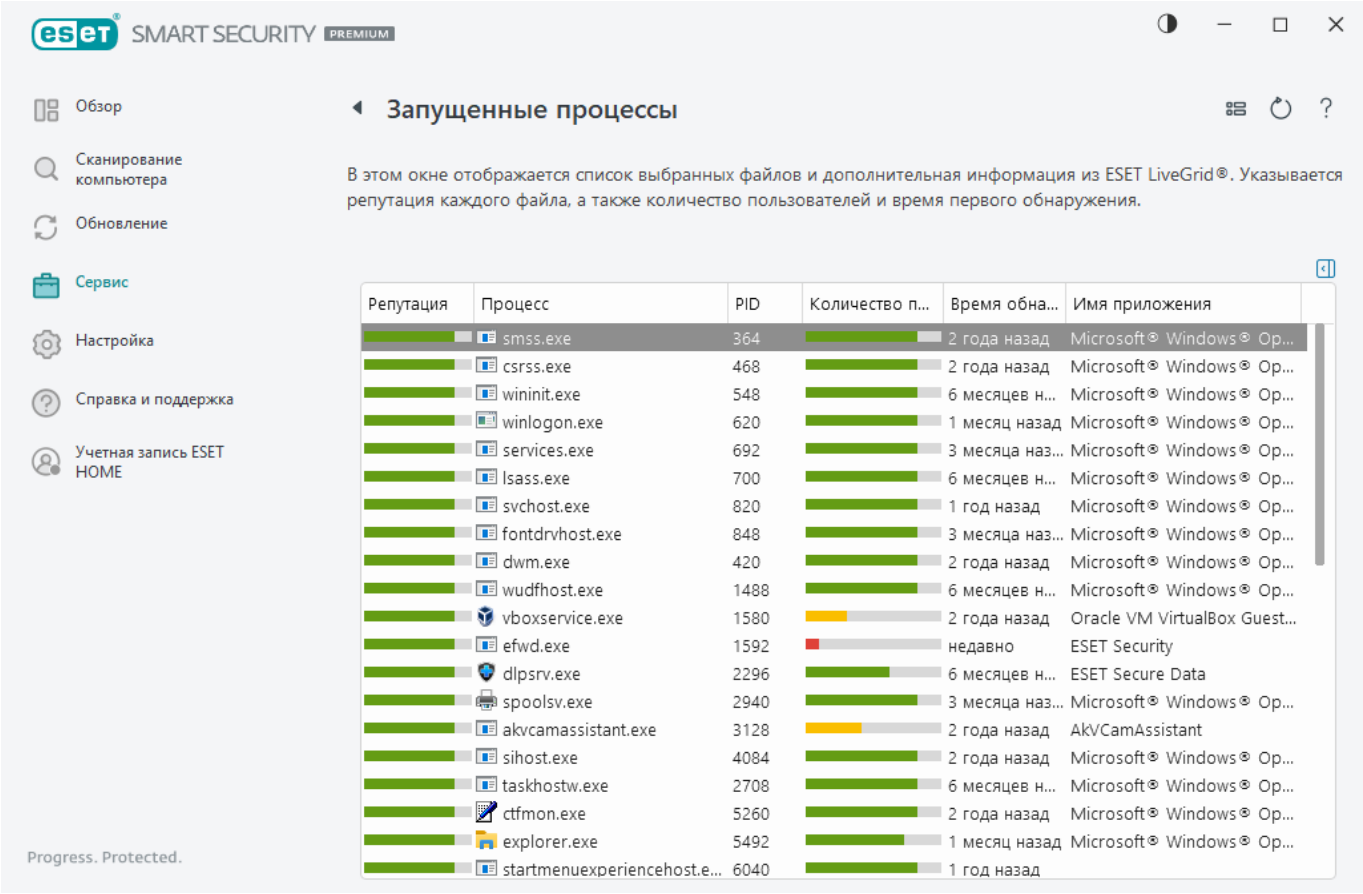
С учетом регистра

Включите этот параметр, если при фильтрации должен учитываться регистр букв. После настройки параметров поиска или фильтрации нажмите кнопку **OK**, чтобы отобразились отфильтрованные записи журнала, или нажмите кнопку **Найти**, чтобы начать поиск. Поиск в файлах журнала ведется сверху вниз, начиная с текущей позиции (выделенной записи).

Поиск прекращается, когда находится первая соответствующая его критериям запись. Чтобы найти следующую запись, нажмите клавишу **F3**. Чтобы уточнить критерии поиска, щелкните правой кнопкой мыши и выберите пункт **Найти**.

Запущенные процессы

В разделе «Запущенные процессы» отображаются выполняемые на компьютере программы или процессы. Кроме того, он позволяет оперативно и непрерывно уведомлять компанию ESET о новых заражениях. ESET Security Ultimate предоставляет подробные сведения о запущенных процессах для защиты пользователей с помощью технологии ESET LiveGrid®.



Репутация: в большинстве случаев ESET Security Ultimate и технология ESET LiveGrid® присваивают объектам (файлам, процессам, разделам реестра и т. п.) уровни риска на основе наборов эвристических правил, которые изучают характеристики каждого объекта и затем оценивают вероятность их вредоносной деятельности. На основе такого эвристического анализа объектам присваивается уровень риска: от 1 — безопасно (зеленый) до 9 — опасно (красный).

Процесс: имя образа программы или процесса, запущенных в настоящий момент на компьютере. Для просмотра всех запущенных на компьютере процессов также можно использовать диспетчер задач Windows. Чтобы открыть диспетчер задач, щелкните правой кнопкой мыши в пустой области на панели задач, после чего выберите пункт **Диспетчер задач**. Или воспользуйтесь сочетанием клавиш **CTRL** + **SHIFT** + **ESC**.

Известные приложения, имеющие пометку Безопасно (зеленый), определенно являются чистыми (находятся в белом списке) и исключаются из сканирования. Этим достигается повышение производительности.

Идентификатор процесса: идентификационный номер процесса может использоваться в качестве параметра в вызовах различных функций, таких как изменение приоритета процесса.

Количество пользователей: количество пользователей данного приложения. Эта информация собирается технологией ESET LiveGrid®.

Время обнаружения: время, прошедшее с момента обнаружения приложения технологией ESET LiveGrid®.

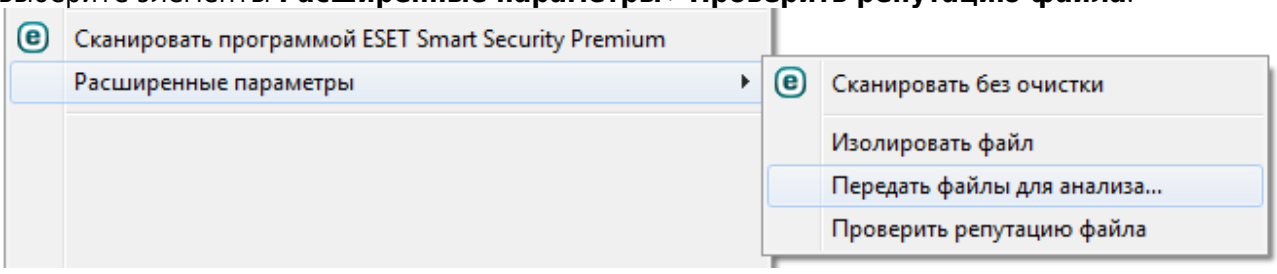
Если приложение имеет пометку Неизвестно (оранжевый), оно не обязательно является вредоносным. Обычно это просто новое приложение. Если вы не уверены в безопасности файла, его можно отправить на анализ в исследовательскую лабораторию ESET. Если файл окажется вредоносным приложением, то в следующем обновлении он будет распознаваться.

Имя приложения: конкретное имя программы или процесса.

Щелкните приложение, чтобы отобразить указанные ниже сведения о нем.

- **Путь**: расположение приложения на компьютере.
- **Размер**: размер файла в КБ (килобайтах) или МБ (мегабайтах).
- **Описание**: характеристики файла на основе его описания в операционной системе.
- **Компания**: название поставщика или процесса приложения.
- **Версия**: информация от издателя приложения.
- **Продукт**: имя приложения и/или наименование компании.
- **Дата создания или изменения**: дата и время создания (изменения).

Кроме того, вы можете проверить репутацию файлов, не действующих как выполняемые программы либо процессы. Для этого щелкните их правой кнопкой мыши в проводнике и выберите элементы **Расширенные параметры** > **Проверить репутацию файла**.



Отчет по безопасности

Эта функция позволяет получить обзор статистики для следующих категорий:

- **Заблокированные веб-страницы**: отображает количество заблокированных веб-страниц (URL-адрес внесен в «черный» список потенциально нежелательных приложений, фишинговый сайт, взломанный маршрутизатор, IP-адрес или сертификат).

• **Обнаружены зараженные объекты электронной почты**: отображается количество обнаруженных зараженных объектов электронной почты.

• **Веб-страницы в родительском контроле заблокированы**: отображается количество заблокированных веб-страниц в родительском контроле.

• **Обнаружено потенциально нежелательное приложение**: отображается количество потенциально нежелательных приложений.

• **Обнаружен спам в электронной почте**: отображается количество обнаруженного спама в электронной почте.

• **Заблокирован доступ к веб-камере**: отображается количество заблокированных попыток доступа к веб-камере.

• **Просканировано документов**: отображается количество просканированных объектов документов.

• **Просканировано приложений**. Отображается количество просканированных исполняемых объектов.

• **Просканировано других объектов**. Отображается количество других просканированных объектов.

• **Просканировано объектов на веб-страницах**. Отображается количество просканированных объектов на веб-страницах.

• **Просканировано объектов электронной почты**: отображается количество просканированных объектов электронной почты.

• **Файлы, проанализированные ESET LiveGuard**: отображается количество образцов, проанализированных системой ESET LiveGuard.

Порядок расположения этих категорий определяется их числовыми значениями — от большего к меньшему. Категории с нулевыми значениями не отображаются. Щелкните "**Больше**", чтобы развернуть и отобразить скрытые категории.

В заключительной части отчета по безопасности вам будет предложено активировать следующие функции:

• ESET LiveGuard

• Secure Data

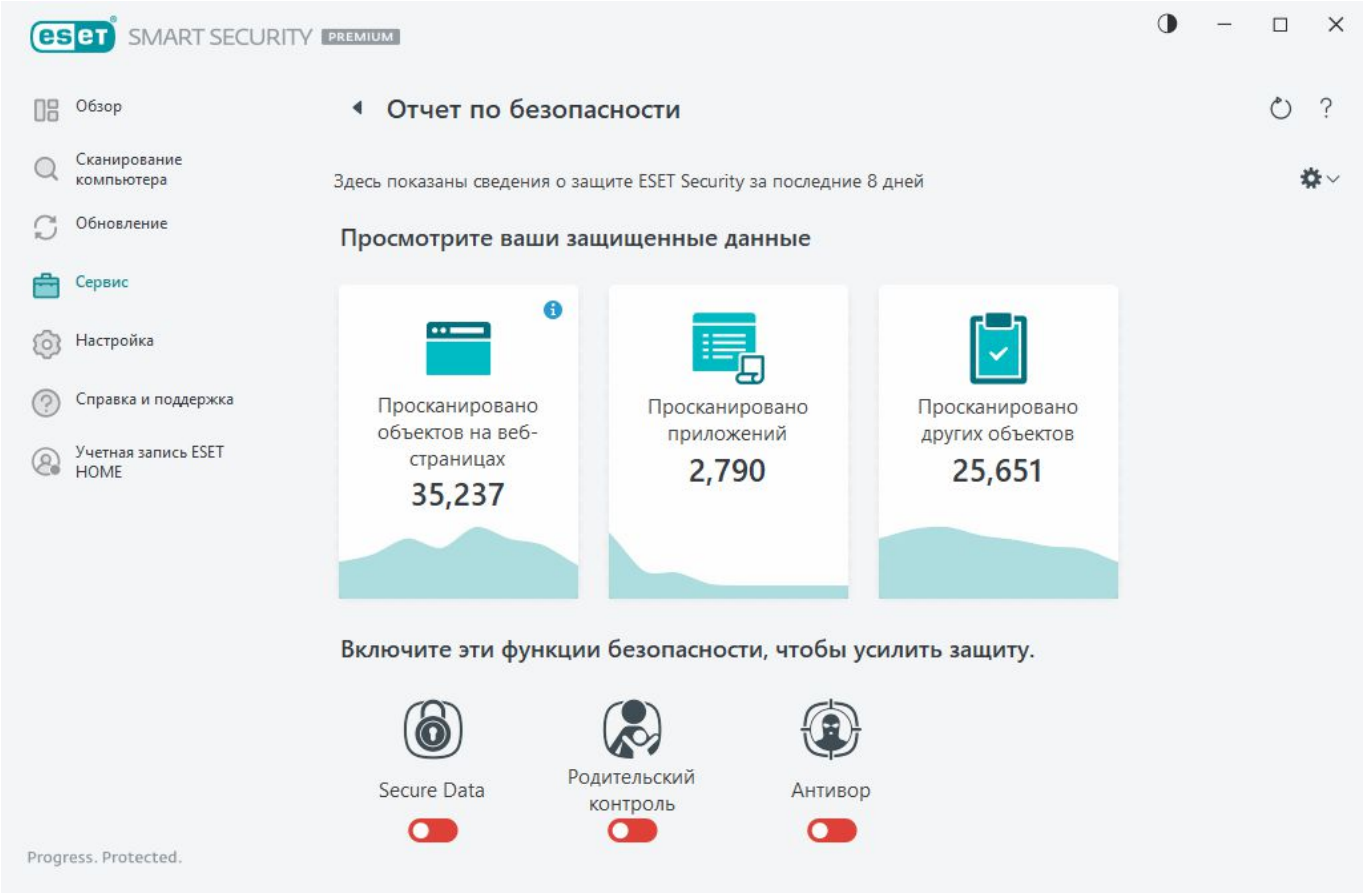
• Родительский контроль

• Антивор

После активации эта функция больше не будет отображаться в отчете по безопасности как неработающая.

В правом верхнем углу щелкните значок шестеренки ⚙, чтобы **включить или выключить уведомления отчета по безопасности** или выбрать, за какой период нужно отобразить данные: за последние 30 дней или с момента активации продукта. Если установка ESET Security

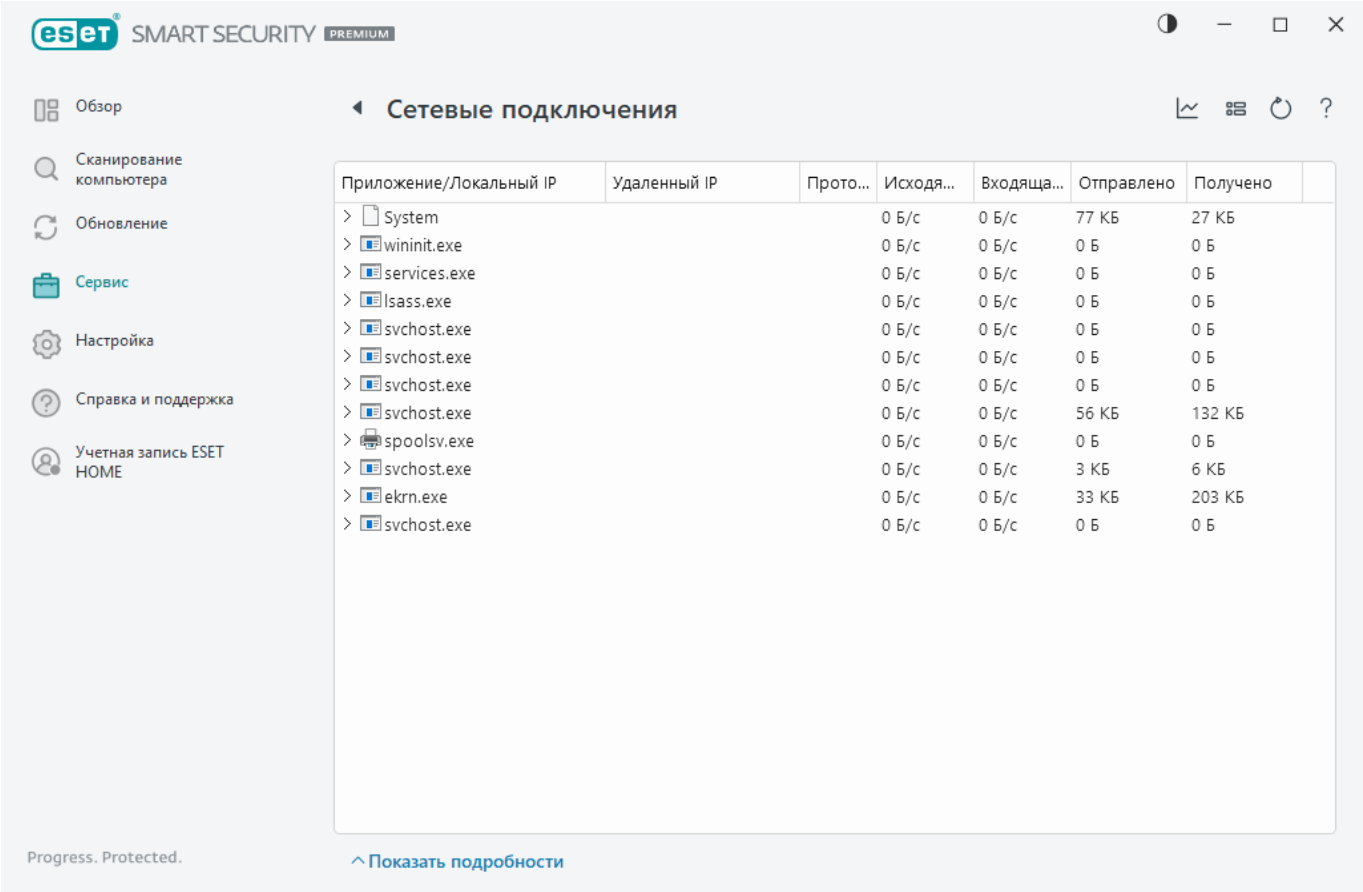
Ultimate выполнялась меньше 30 дней назад, вы сможете выбрать только количество дней с момента установки. По умолчанию выбран период 30 дней.



Элемент **Сбросить данные** позволяет очистить статистику и удалить существующие данные отчета по безопасности. Это действие нужно подтвердить, если только флажок **Запрашивать подтверждение перед сбросом статистики** не снят в меню Расширенные параметры > **Уведомления** > **Интерактивный режим** > **Подтверждения** > **Изменить**.

Сетевые подключения

В разделе «Сетевые подключения» отображается список активных и отложенных соединений. Это позволяет управлять всеми приложениями, которые устанавливают исходящие соединения.



Щелкните значок графика , чтобы открыть раздел Сетевая активность.

Первая строка содержит имя приложения и его скорость передачи данных. Для просмотра списка соединений отдельного приложения (и более подробной информации) щелкните **>**.

Столбцы

Приложение/Локальный IP-адрес: имя приложения, локальные IP-адреса и порты обмена данными.

Удаленный IP-адрес: IP-адрес и номер порта соответствующего удаленного компьютера.

Протокол: используемый протокол передачи данных.

Исходящая скорость/Входящая скорость: текущая скорость обмена данными в соответствующих направлениях.

Отправлено/Получено: объем переданных данных с начала соединения.

Показать подробности: выберите эту функцию для отображения подробной информации о выбранном подключении.

Щелкните подключение правой кнопкой мыши, чтобы просмотреть дополнительные параметры, среди которых есть следующие.

Определять имена хостов: все сетевые адреса, если это возможно, отображаются в формате DNS, а не в числовом формате IP-адресов.

Показывать только соединения по TCP: в списке отображаются только подключения по протоколу TCP.

Показывать ожидание соединения: установите этот флажок для отображения только тех подключений, по которым в настоящий момент не происходит обмена данными, но для которых система уже открыла порт и ожидает подключения.

Показывать внутренние соединения: установите этот флажок, чтобы отобразить только те соединения, в которых удаленной стороной является локальный компьютер (так называемые localhost).

Обновить скорость: выберите периодичность обновления активных подключений.

Обновить сейчас: перезагрузка окна **«Сетевые подключения»**.

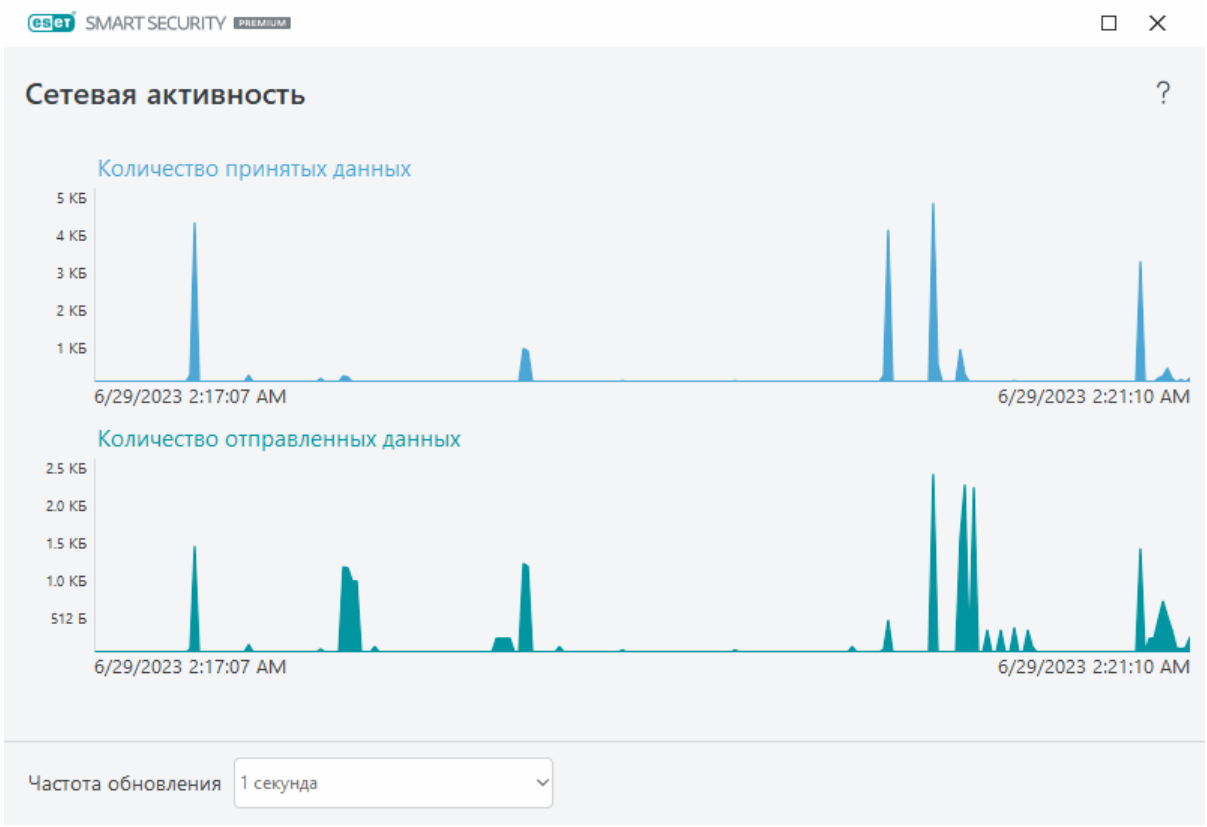
Представленные ниже возможности доступны, только если щелкнуть приложение или процесс, а не активное подключение.

Временно запретить обмен данными для процесса: запретить текущие соединения для данного приложения. При создании нового соединения файервол использует предопределенное правило. Описание настроек см. в разделе Правила файервола.

Временно разрешить обмен данными для процесса: разрешить текущие соединения для данного приложения. При создании нового соединения файервол использует предопределенное правило. Описание настроек см. в разделе Правила файервола.

Сетевая активность

Чтобы просмотреть текущую **сетевую активность** в графическом виде, выберите **Сервис** > **Сетевые подключения** и щелкните значок графика . В нижней части графика находится временная шкала, на которой отображается сетевая активность в режиме реального времени за выбранный временной интервал. Чтобы изменить временной интервал, выберите необходимое значение в раскрывающемся меню **Частота обновления**.



Доступны следующие варианты:

- **1 секунда**: диаграмма обновляется каждую секунду, временная шкала охватывает последние 4 минут.
- **1 минута (последние 24 часа)**: диаграмма обновляется каждую минуту, временная шкала охватывает последние 24 часа.
- **1 час (последний месяц)**: диаграмма обновляется каждый час, временная шкала охватывает последний месяц.

На вертикальной оси графика отображается объем полученных или отправленных данных. Наведите указатель мыши на график, чтобы увидеть точный объем полученных или отправленных данных в конкретный момент.

ESET SysInspector

ESET SysInspector — это приложение, которое тщательно проверяет компьютер и собирает подробные сведения о таких компонентах системы, как драйверы и приложения, сетевые подключения и важные записи реестра, а также оценивает уровень риска для каждого компонента. Эта информация способна помочь определить причину подозрительного поведения системы, которое может быть связано с несовместимостью программного или аппаратного обеспечения или заражением вредоносными программами. Чтобы узнать, как использовать ESET SysInspector, см. интерактивную справку ESET SysInspector.

В окне ESET SysInspector отображаются следующие сведения о журналах:

- **Время**: время создания журнала.

• **Комментарий**: краткий комментарий.

• **Пользователь**: имя пользователя, создавшего журнал.

• **Состояние**: состояние создания журнала.

Доступны перечисленные далее действия.

• **Показать** — открывает выбранный журнал в ESET SysInspector. Вы также можете щелкнуть файл журнала правой кнопкой мыши и выбрать в контекстном меню пункт **Показать**.

• **Создать**: создание журнала. Прежде чем пытаться открыть журнал, подождите, пока не сгенерируется ESET SysInspector (состояние **Создано**). Журнал сохраняется в папке C:\ProgramData\ESET\ESET Security\SysInspector.

• **Удалить**: удаление выделенных журналов из списка.

Если выбраны файлы журнала, в контекстном меню доступны следующие элементы:

• **Показать**: открытие выбранного журнала в ESET SysInspector (аналогично двойному щелчку).

• **Создать**: создание журнала. Прежде чем пытаться открыть журнал, подождите, пока не сгенерируется ESET SysInspector (состояние **Создано**).

• **Удалить**: удаление выделенных журналов из списка.

• **Удалить все**: удаление всех журналов.

• **Экспорт**: экспорт журнала в файл или архив в формате XML.

Планировщик

Планировщик управляет запланированными задачами и запускает их с предварительно заданными параметрами и свойствами.

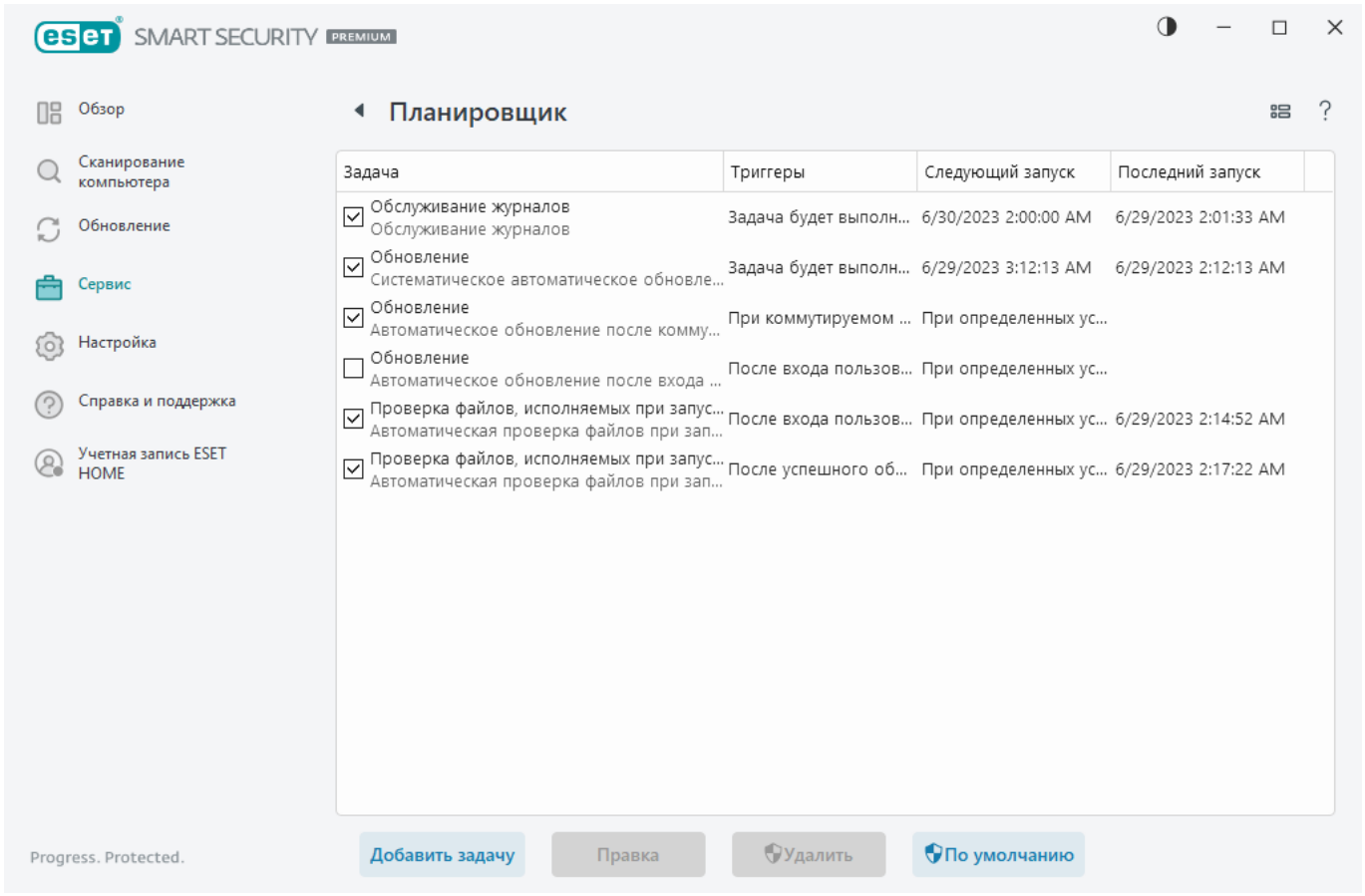
Планировщик можно открыть из главного окна программы ESET Security Ultimate, щелкнув элемент **Сервис** > **Планировщик**. Здесь приведен полный список запланированных задач и параметры их запуска (дата, время и используемый профиль сканирования).

Планировщик предназначен для планирования выполнения следующих задач: обновление модулей, сканирование, проверка файлов, исполняемых при запуске системы, и обслуживание журнала. Добавлять и удалять задачи можно непосредственно в главном окне планировщика (нажмите кнопку **Добавить задачу** или **Удалить** в нижней части окна). Вы можете восстановить список запланированных задач по умолчанию и удалить все изменения, щелкнув параметр **По умолчанию**. С помощью контекстного меню окна планировщика можно выполнить следующие действия: отображение подробной информации, выполнение задачи немедленно, добавление новой задачи и удаление существующей задачи. Используйте флажки в начале каждой записи, чтобы активировать или отключить соответствующие задачи.

По умолчанию в **планировщике** отображаются следующие запланированные задачи.

- **Обслуживание журнала**
- **Регулярное автоматическое обновление**
- **Автоматическое обновление после входа пользователя в систему**
- **Автоматическая проверка файлов при запуске системы** (после входа пользователя в систему)
- **Автоматическая проверка файлов при запуске системы** (после успешного обновления модуля обнаружения)

Чтобы изменить конфигурацию имеющейся запланированной задачи (как задачи по умолчанию, так и пользовательской), щелкните правой кнопкой мыши нужную задачу и выберите в контекстном меню команду **Изменить** или выделите задачу, которую необходимо изменить, а затем нажмите кнопку **Изменить**.



Добавление новой задачи

1. Щелкните **Добавить задачу** в нижней части окна.
2. Введите имя задачи.
3. Выберите нужную задачу в раскрывающемся меню.
   - **Запуск внешнего приложения**: планирование выполнения внешнего приложения.
   - **Обслуживание журнала** - в файлах журнала также содержатся остатки удаленных

записей. Эта задача регулярно оптимизирует записи в файлах журнала для эффективной работы.

• **Проверка файлов при загрузке системы**: проверка файлов, исполнение которых разрешено при запуске или входе пользователя в систему.

• **Создать снимок состояния компьютера**: создание снимка состояния компьютера в ESET SysInspector, для которого собираются подробные сведения о компонентах системы (например, драйверах, приложениях) и оценивается уровень риска для каждого их них.

• **Сканирование компьютера по требованию**: сканирование файлов и папок на компьютере.

• **Обновление**: планирование задачи обновления путем обновления модулей.

4. Щелкните ползунок рядом с элементом **Включено**, чтобы активировать задачу (это можно сделать позже, установив/сняв флажок в списке запланированных задач), нажмите **Далее** и выберите один из режимов времени выполнения.

• **Однократно**: задача будет выполнена однократно в указанные дату и время.

• **Многократно**: задача будет выполняться регулярно через указанный промежуток времени.

• **Ежедневно**: задача будет многократно выполняться каждые сутки в указанное время.

• **Еженедельно**: задача будет выполняться в выбранный день недели в указанное время.

• **При определенных условиях**: задача будет выполнена при возникновении указанного события.

5. Установите флажок **Пропускать задачу, если устройство работает от аккумулятора**, чтобы свести к минимуму потребление системных ресурсов, когда ноутбук работает от аккумулятора. Задача будет выполняться в день и время, указанные в полях области **Выполнение задачи**. Если задача не могла быть выполнена в отведенное ей время, можно указать, когда будет предпринята следующая попытка запуска задачи.

• **В следующее запланированное время**

• **Как можно скорее**

• **Немедленно, если время с момента последнего запуска превышает (часы)** — представляет время, прошедшее с момента первого пропущенного запуска задания. Если это время превышено, задание будет запущено незамедлительно. Установите время с помощью счетчика ниже.

Чтобы просмотреть запланированную задачу, щелкните ее правой кнопкой мыши и выберите **Показать информацию о задаче**.

Параметры сканирования по расписанию

В этом окне можно задать расширенные параметры для запланированных задач сканирования компьютера.

Чтобы выполнить сканирование без очистки, щелкните **Дополнительные параметры** и выберите **Сканировать без очистки**. История сканирования сохраняется в журнале сканирования.

Если выбран параметр **Пропустить исключения**, файлы с расширениями, которые ранее были исключены из сканирования, будут просканированы.

В раскрывающемся меню **Действие после сканирования** можно настроить действие, которое будет выполняться автоматически после завершения сканирования:

- **Ничего не предпринимать**: после сканирования действия предприниматься не будут.
- **Выключить**: после сканирования компьютер отключается.
- **Перезапуск при необходимости**: компьютер перезапускается, только если нужно завершить очистку обнаруженных угроз.
- **Перезагрузить**: после сканирования открытые программы закрываются, а компьютер перезагружается.
- **Принудительный перезапуск при необходимости**: компьютер принудительно перезапускается, только если нужно завершить очистку обнаруженных угроз.
- **Принудительная перезагрузка**: все открытые программы принудительно закрываются, не дожидаясь вмешательства пользователя, и компьютер перезапускается после завершения сканирования.
- **Спящий режим**: сеанс сохраняется, и компьютер переходит в режим пониженного энергопотребления (т. е. пользователь может быстро возобновить работу).
- **Режим гибернации**: все компоненты, использующие ОЗУ, переносятся в специальный файл на жестком диске. Компьютер выключается, и при следующем включении вернется в предыдущее состояние.

> Доступность действий **Сон** и **Гибернация** зависит от параметров питания и спящего режима операционной системы и возможностей вашего ноутбука или компьютера. Не забывайте, что компьютер в спящем режиме все же работает. Компьютер выполняет основные функции и потребляет электричество, когда работает от аккумулятора. Чтобы сохранить время работы батареи (например, если вы находитесь в пути), рекомендуется перевести компьютер в режим гибернации.

Выбранное действие будет запущено после того, как все запущенные процессы сканирования будут завершены. При выборе **Завершение работы** или **Перезагрузка** в диалоговом окне подтверждения будет отображаться 30-секундный обратный отсчет (щелкните **Отмена**, чтобы деактивировать запрошенное действие).

Выберите элемент **Сканирование не может быть отменено**, чтобы пользователи, не

обладающие нужными правами, не могли отменить действия, которые выполняются после сканирования.

Включите параметр **Сканирование может быть приостановлено пользователем на (мин.)**, чтобы пользователи, обладающие ограниченными правами, могли приостанавливать сканирование компьютера на определенный период времени.

См. также Ход сканирования.

Обзор запланированных задач

В данном диалоговом окне отображается подробная информация о выбранной запланированной задаче, если дважды щелкнуть настраиваемую задачу или щелкнуть правой кнопкой мыши настраиваемую задачу планировщика и выбрать команду **Показать информацию о задаче**.

Сведения о задаче

Введите **имя задачи**, выберите **тип задачи** и щелкните **Далее**.

- **Запуск внешнего приложения**: планирование выполнения внешнего приложения.
- **Обслуживание журнала** - в файлах журнала также содержатся остатки удаленных записей. Эта задача регулярно оптимизирует записи в файлах журнала для эффективной работы.
- **Проверка файлов при загрузке системы**: проверка файлов, исполнение которых разрешено при запуске или входе пользователя в систему.
- **Создать снимок состояния компьютера**: создание снимка состояния компьютера в ESET SysInspector, для которого собираются подробные сведения о компонентах системы (например, драйверах, приложениях) и оценивается уровень риска для каждого их них.
- **Сканирование компьютера по требованию**: сканирование файлов и папок на компьютере.
- **Обновление**: планирование задачи обновления путем обновления модулей.

Время задачи

Задача будет выполняться регулярно через указанный промежуток времени. Выберите один из следующих параметров.

- **Однократно**: задача будет выполнена однократно в установленные дату и время.
- **Многократно**: задача будет выполняться регулярно через указанный промежуток времени (в часах).
- **Ежедневно**: задача будет выполняться раз в сутки в указанное время.

• **Еженедельно**: задача будет выполняться один или несколько раз в неделю в указанные дни и время.

• **При определенных условиях**: задача будет выполнена при возникновении указанного события.

Пропускать задачу, если устройство работает от аккумулятора: задача не запустится, если на момент планируемого запуска задачи компьютер работает от аккумулятора. Это также относится к компьютерам, работающим от источника бесперебойного питания.

Время выполнения задачи: однократно

Выполнение задачи: указанная задача будет выполнена однократно в указанные дату и время.

Время выполнения задачи: ежедневно

Задача будет выполняться раз в сутки в указанное время.

Время выполнения задачи: еженедельно

Задача будет выполняться каждую неделю в указанные день и время.

Время выполнения задачи: при определенных условиях

Задача запускается в случае возникновения одного из перечисленных далее событий.

- **Каждый раз при запуске компьютера**
- **Каждые сутки при первом запуске компьютера**
- **При коммутируемом подключении к Интернету/VPN**
- **После успешного обновления модуля**
- **После успешного обновления программы**
- **Вход пользователя**
- **Обнаружение угроз**

При планировании задачи по событию пользователь может указать минимальный интервал между двумя окончаниями выполнения задачи. Например, если пользователь входит в систему несколько раз в день, выберите 24 часа, чтобы задача выполнялась только при первом входе в систему за сутки, а затем только на следующий день.

Пропущенная задача

Задача может быть пропущена, если компьютер выключен или работает от аккумулятора. Выберите среди этих вариантов, когда должна быть запущена пропущенная задача, и нажмите кнопку **Далее**.

• **В следующее запланированное время** — задание будет запущено, если компьютер будет включен в следующее запланированное время.

• **Как можно скорее** — задание будет запускаться при включении компьютера.

• **Немедленно, если время с момента последнего запланированного запуска превышает (часы)** — представляет время, прошедшее с момента первого пропущенного запуска задания. Если это время превышено, задание будет запущено незамедлительно.

Немедленно, если время с момента последнего запланированного запуска превысит (ч) – примеры

Для примера задания настроен повторный запуск каждый час. Выбрана опция **Немедленно, если время, прошедшее с момента последнего запланированного запуска, превышает (часы)**, а для превышенного времени установлено два часа. Задание запускается в 13:00, и по его завершении компьютер переходит в спящий режим:

• Компьютер выходит из спящего режима в 15:30. Первый пропущенный запуск задания был в 14:00. С 14:00 прошло всего 1,5 часа, поэтому задание будет запущено в 16:00.

• Компьютер выходит из спящего режима в 16:30. Первый пропущенный запуск задачи был в 14:00. С 14:00 прошло два с половиной часа, поэтому задание будет запущено немедленно.

Сведения о задаче: обновление

Если нужно иметь возможность обновлять программу с двух серверов обновлений, нужно создать два разных профиля обновления. Если не удастся загрузить файлы обновлений с одного сервера, программа автоматически переключится на другой. Этот вариант подходит, например, для ноутбуков, которые обычно обновляются с сервера обновлений в локальной сети, но при этом их владельцы часто подключаются к Интернету в других сетях. Таким образом, если с первым профилем возникнет ошибка, файлы обновлений с серверов обновлений ESET автоматически будут загружены через второй профиль.

Сведения о задаче: запуск приложения

С помощью этой задачи можно запланировать выполнение внешнего приложения.

Исполняемый файл: выберите исполняемый файл в дереве каталогов или нажмите кнопку **...**, чтобы вручную ввести путь.

Рабочая папка: задайте рабочий каталог внешнего приложения. Все временные файлы выбранного в поле **Исполняемый файл** файла будут создаваться в этом каталоге.

Параметры: параметры командной строки для приложения (необязательно).

Нажмите кнопку **Готово** для применения задачи.

Средство очистки системы

После удаления угрозы средство очистки системы помогает восстановить компьютер до состояния, пригодного к эксплуатации. Вредоносные программы могут привести к отключению таких системных программ, как редактор реестра или обновления Windows. Средство очистки системы одним щелчком восстанавливает для данной системы значения и параметры по умолчанию.

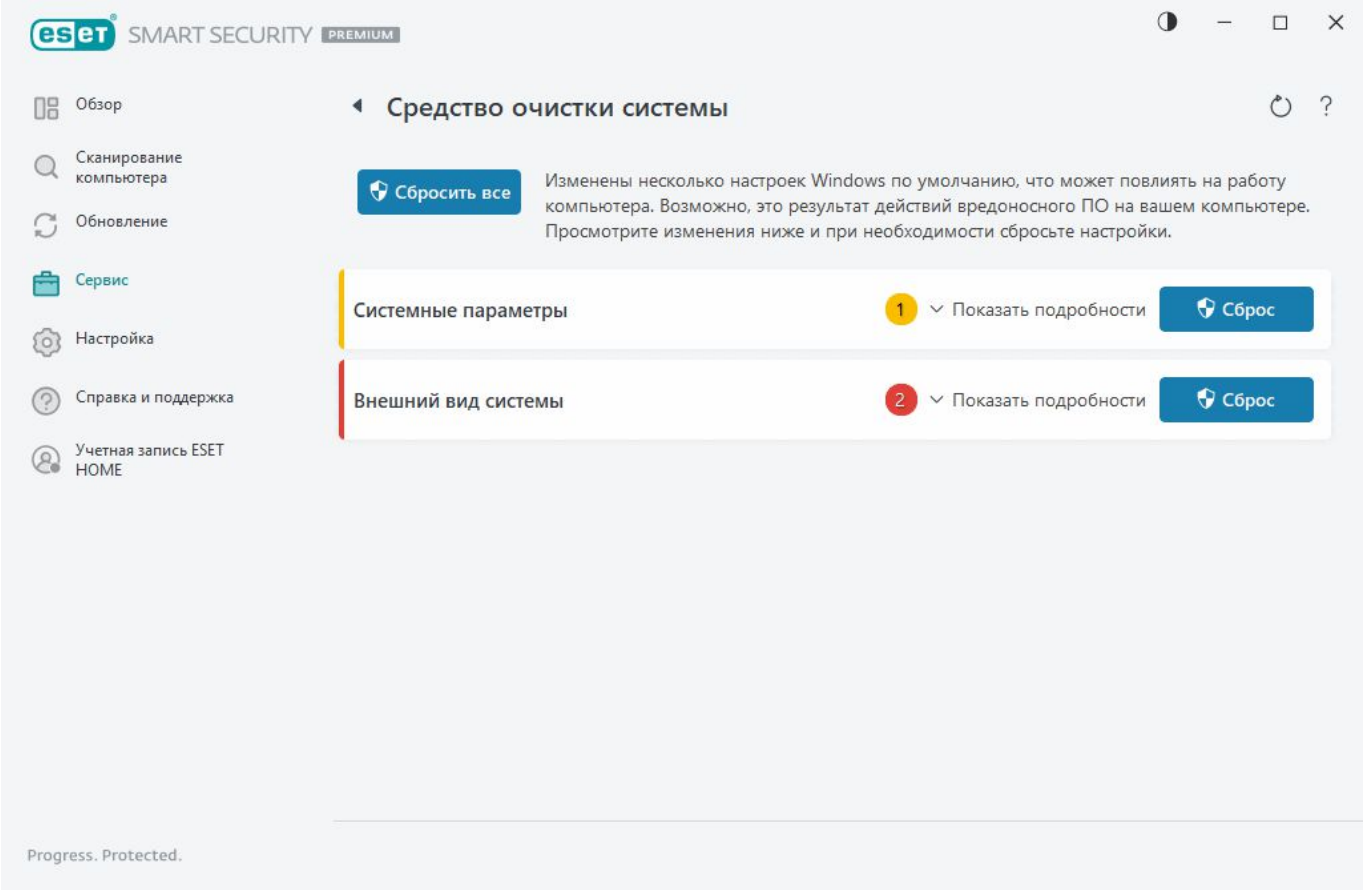
Средство очистки системы сообщает о проблемных параметрах в пяти категориях:

- **Настройки безопасности**: изменения в параметрах, которые могут привести к повышению уязвимости вашего компьютера, например изменения в Центре обновления Windows.
- **Системные параметры**: изменение системных параметров, которое может изменить поведение компьютера, например изменение сопоставления файлов.
- **Внешний вид системы**: параметры, влияющие на внешний вид системы, например фоновый рисунок рабочего стола.
- **Отключенные компоненты**: важные компоненты и приложения, которые могут быть отключены.
- **Восстановление системы Windows**: параметры функции восстановления системы Windows, которая дает возможность восстановить предыдущее состояние системы.

Очистку системы можно запросить в следующих случаях:

- при обнаружении угрозы;
- при нажатии кнопки **Сброс**.

При необходимости можно просматривать изменения и сбрасывать настройки.



Действия в средстве очистки системы может выполнять только пользователь с правами администратора.

Инспектор сети

Инспектор сети может помочь выявить уязвимости в вашей доверенной (домашней или офисной) сети (например, открытые порты или ненадежный пароль маршрутизатора). Кроме того, вы получаете список подключенных устройств, в котором устройства упорядочены по типам (например, принтер, маршрутизатор, мобильное устройство и т. п.) и который позволяет узнать, какие устройства подключены к вашей сети (например, игровая консоль, устройство IoT или другие устройства «умного» дома).

Инспектор сети позволяет обнаружить уязвимости маршрутизатора и повышает уровень защиты при подключении к сети.

Инспектор сети не выполняет повторную настройку маршрутизатора вместо вас. Вы сами вносите изменения при помощи специализированного интерфейса маршрутизатора. Домашние маршрутизаторы могут быть весьма уязвимыми для вредоносных программ, используемых для запуска распределенных атак типа «отказ в обслуживании» (DDoS). Если пароль маршрутизатора, заданный по умолчанию, не был изменен пользователем, для злоумышленников не составит труда подобрать пароль, авторизоваться в вашем маршрутизаторе и перенастроить его либо взломать вашу сеть.

Настоятельно рекомендуется создать надежный и длинный пароль с использованием цифр, специальных символов или заглавных букв. Чтобы повысить надежность пароля, используйте сочетания разных символов.

Если сеть, к которой вы подключены, конфигурирована как доверенная, сеть можно пометить как «Моя сеть». Щелкните **Пометить как «Моя сеть»**, чтобы добавить к сети тег «Моя сеть». Этот тег будет отображаться рядом с сетью во всем ESET Security Ultimate для лучшей идентификации и обзора безопасности. Щелкните **Снять пометку «Моя сеть»**, чтобы удалить тег.

Каждое устройство, подключенное к вашей сети, отображается с основной информацией в виде списка. Щелкните устройство, чтобы изменить его или просмотреть подробные сведения о нем.

С помощью раскрывающегося меню **Сети** можно фильтровать устройства, основываясь на таких критериях:

- Устройства, подключенные к определенной сети
- Устройства, подключенные ко **всем сетям**
- устройства без категории;

Щелкните значок устройства, чтобы изменить устройство или просмотреть подробные сведения о нем. Недавно подключенные устройства показаны ближе к маршрутизатору, чтобы вам было проще их обнаружить.

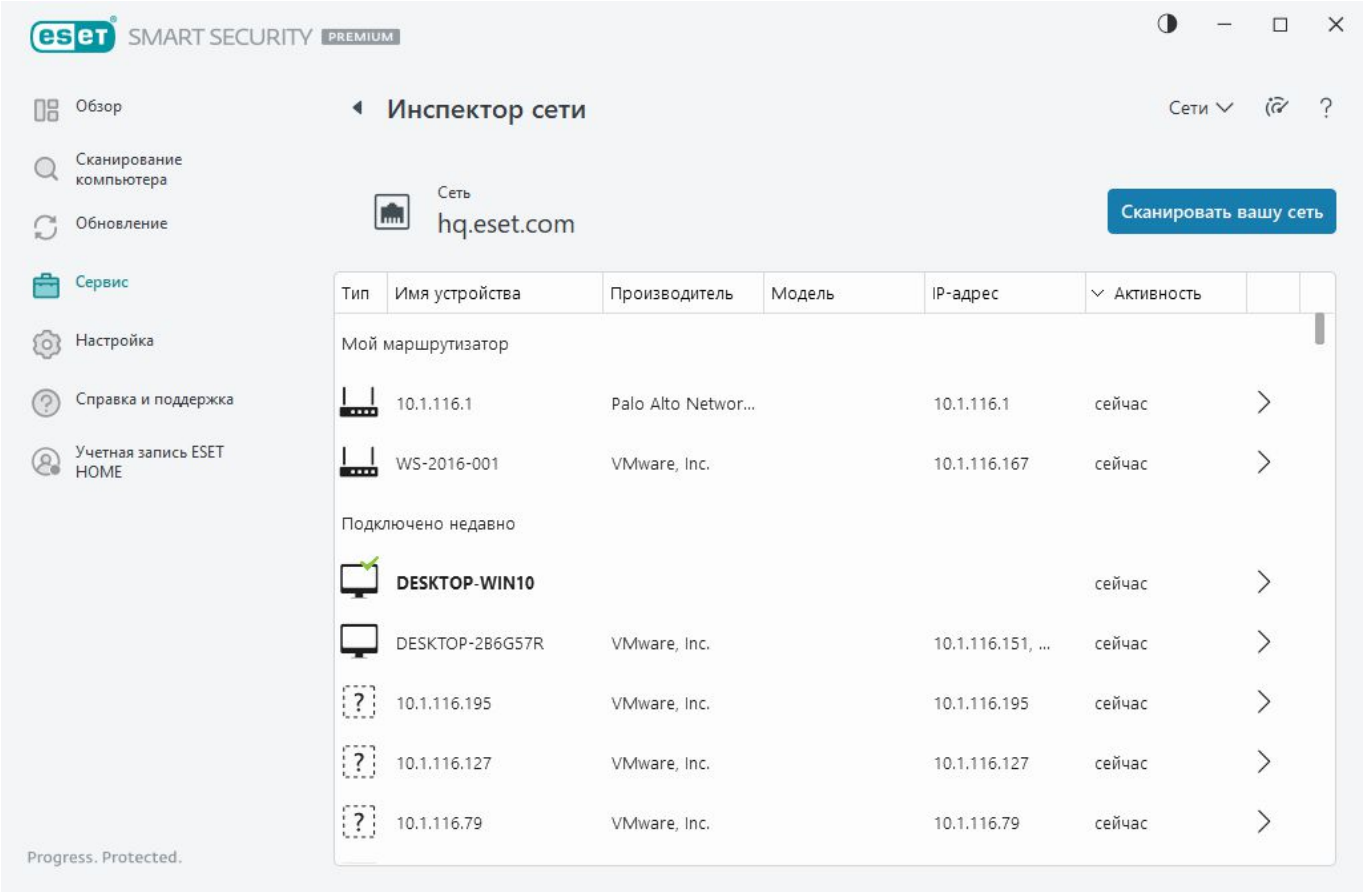
Щелкните шестеренку ⚙ в правом верхнем углу, чтобы выбрать, необходимо ли уведомлять об обнаружении нового устройства в сети.

Щелкните **Сканировать сеть**, чтобы вручную просканировать сеть, к которой вы подключены. **Сканирование сети** доступно только для доверенной сети. Сведения о просмотре или изменении настроек сети см. в разделе Профили сетевых подключений.

Доступны следующие параметры сканирования.

- Сканировать все
- Сканировать только маршрутизатор
- Сканировать только устройства

⚠ Выполняйте сканирование сети только в доверенной сети! Делать это в недоверенной сети опасно.



По завершении сканирования отобразится уведомление, содержащее ссылку на основные сведения об устройстве. Также можно просмотреть эти сведения, дважды щелкнув подозрительное устройство в списке или представлении локатора. Щелкните **Устранить неполадки**, чтобы просмотреть недавно заблокированные соединения. Подробные сведения об устранении неполадок файервола.

Модуль Инспектор сети отображает уведомления двух типов:

- **К сети подключено новое устройство**: отображается, если к сети подключается не использовавшееся ранее устройство, когда пользователь подключен.

- **Найдены новые сетевые устройства**: отображается, если вы заново подключаетесь к своей доверенной сети и в ней обнаруживается ранее не использовавшееся устройство.

Оба типа уведомлений сообщают вам, что к сети пытается подключиться неавторизованное устройство. Щелкните **Просмотр устройства**, чтобы увидеть сведения об устройстве.

Что означают значки на устройствах в Инспекторе сети?

	Значок в виде желтой звезды обозначает устройства, которые являются новыми для сети или которые в первый раз были обнаружены компанией ESET.
	Желтый значок предупреждения означает, что ваш маршрутизатор может содержать уязвимости. Чтобы просмотреть более подробные сведения о проблеме, щелкните значок продукта.

	Красный значок предупреждения обозначает устройства, на которых маршрутизатор содержит уязвимости и может быть заражен. Чтобы просмотреть более подробные сведения о проблеме, щелкните значок продукта.
	Синий значок может появиться, когда у продукта ESET есть дополнительные сведения для вашего маршрутизатора, но немедленное вмешательство не требуется, так как угрозы безопасности отсутствуют. Чтобы просмотреть более подробные сведения, щелкните значок продукта.

Сетевое устройство в Инспекторе сети

Этот раздел содержит подробные сведения об устройстве, в том числе:

- имя устройства;
- Тип устройства
- последний контакт;
- имя сети;
- IP-адрес;
- MAC-адрес.
- Операционная система

Значок карандаша означает, что имя и тип устройства можно изменить.

Удалить из истории: удаление устройства из списка устройств. Эта опция доступна только для устройств, которые не подключены в данный момент к вашей сети.

Для каждого типа устройства доступны перечисленные далее действия:

Маршрутизатор

Параметры маршрутизатора — доступ к параметрам маршрутизатора возможен через веб-интерфейс, мобильное приложение или с помощью кнопки **Открыть интерфейс маршрутизатора**. Если маршрутизатор предоставлен вам поставщиком услуг Интернета, возможно, вам нужно будет связаться с его службой поддержки или с производителем маршрутизатора для устранения выявленных проблем безопасности. Обязательно соблюдайте надлежащие меры предосторожности, которые приведены в документации маршрутизатора.
Защита – Чтобы защитить маршрутизатор и сеть от кибератак, соблюдайте следующие общие рекомендации.

Сетевое устройство

Идентификационные данные устройства — если вы не знаете, какое устройство подключено к вашей сети, найдите название поставщика или производителя под именем устройства. С помощью этой информации вам будет проще определить, что это за устройство. Имя устройства можно изменить, чтобы в дальнейшем его было легко узнать.
Отключение устройства — если вы не уверены, что подключенное устройство безопасно для вашей сети или других устройств, измените права доступа к сети для этого устройства в параметрах маршрутизатора или измените пароль сети.
Защита — чтобы защитить устройство от атак и вредоносных программ, установите систему обеспечения кибербезопасности на свое устройство и своевременно обновляйте операционную систему и установленное ПО. Чтобы сохранить защиту, не подключайте устройство к незащищенным сетям Wi-Fi.

Это устройство

Это устройство — ваш компьютер в сети.
Сетевые адаптеры — сведения о ваших сетевых адаптерах.

Уведомления | Инспектор сети

Ниже показано несколько вариантов уведомлений, которые могут отображаться, когда ESET Security Ultimate обнаруживает проблемы с уязвимостью в вашем маршрутизаторе. Каждое уведомление содержит короткое описание и решение либо шаги, которые помогут минимизировать риск от уязвимости вашего маршрутизатора. Если у вас нет опыта в изменении настроек маршрутизатора, рекомендуем обратиться к производителю маршрутизатора или к своему поставщику услуг Интернета.

Найдена потенциальная уязвимость
Маршрутизатор может содержать известные уязвимости, которые можно легко атаковать и использовать. Обновите встроенное ПО маршрутизатора.

Найдена уязвимость
Маршрутизатор содержит известные уязвимости, которые можно легко атаковать и использовать. Обновите встроенное ПО маршрутизатора.

Угроза найдена
Маршрутизатор заражен вредоносным ПО. Перезапустите маршрутизатор и повторите сканирование.

Ненадежный пароль маршрутизатора
Пароль вашего маршрутизатора ненадежен. Его легко может угадать другой человек. Измените пароль в маршрутизаторе.

Вредоносное перенаправление в сети
Кажется, ваш интернет-трафик перенаправляется на вредоносные веб-сайты. Возможно, ваш маршрутизатор скомпрометирован. Измените настройки DNS-сервера в маршрутизаторе.

Открытые сетевые службы
Ваш маршрутизатор запускает сетевые службы, которые могут использовать другие люди. Это может быть связано с неправильной настройкой или скомпрометированным маршрутизатором. Проверьте конфигурацию маршрутизатора.

Конфиденциальные открытые сетевые службы
Ваш маршрутизатор запускает конфиденциальные сетевые службы, которые могут использоваться другими людьми. Это может быть связано с неправильной настройкой или скомпрометированным маршрутизатором. Проверьте конфигурацию маршрутизатора.

Встроенное ПО устарело
Встроенное ПО вашего маршрутизатора устарело и может содержать уязвимости. Обновите встроенное ПО маршрутизатора.

Вредоносная настройка маршрутизатора
Этот DNS-сервер, используемый вашим маршрутизатором, является вредоносным. Он может перенаправлять вас на опасные веб-сайты. Возможно, ваш маршрутизатор скомпрометирован. Измените настройки DNS-сервера в маршрутизаторе.

Сетевые службы
Ваш маршрутизатор запускает общие сетевые службы. Они нужны для работы в сети и, вероятно, безопасны. Проверьте конфигурацию маршрутизатора.

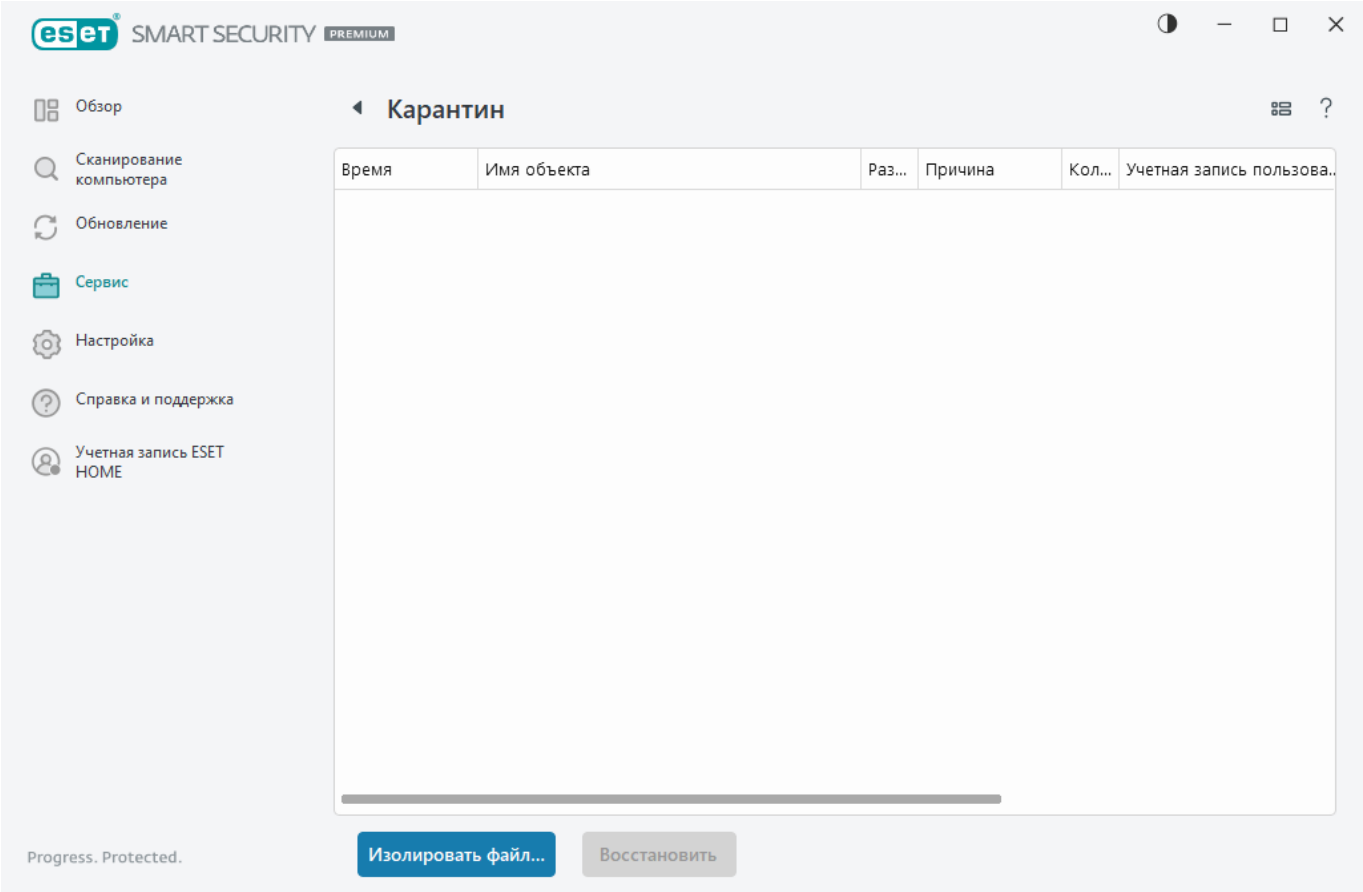
Карантин

Главная функция карантина — безопасное хранение обнаруженных объектов (например, вредоносных программ, зараженных файлов или потенциально нежелательных приложений).

Карантин можно открыть из главного окна программы ESET Security Ultimate, щелкнув элемент **Сервис** > **Карантин**.

Информацию о файлах, помещенных на карантин, можно просмотреть в виде таблицы, содержащей такие сведения:

- дату и время помещения файла на карантин;
- путь к исходному расположению файла;
- его размер в байтах;
- причину помещения файла на карантин (например, объект добавлен пользователем);
- количество обнаружений (например, повторяющиеся обнаружения одного и того же файла или архив, содержащий несколько заражений).



Помещение файлов на карантин

Программа ESET Security Ultimate автоматически помещает удаленные файлы на карантин (если пользователь не отключил эту функцию в окне предупреждения).

Дополнительные файлы следует помещать на карантин, если:

a.их нельзя вылечить;

b.их нельзя безопасно удалить;

c.они отнесены программой ESET Security Ultimate к зараженным по ошибке;

d.файл с подозрительной активностью, но не определяется Защитамы.

Чтобы поместить файл на карантин, можно использовать несколько приведенных ниже вариантов.

a.Используйте функцию перетаскивания, чтобы вручную отправить файл на карантин. Для этого щелкните файл, переместите указатель мыши в отмеченную область, удерживая нажатой кнопку мыши, после чего отпустите кнопку мыши. После этого приложение будет переведено в фоновый режим.

b.Щелкните файл правой кнопкой мыши и выберите **Расширенные параметры** > **Поместить файл в карантин**.

c.Щелкните **Изолировать файл...** в окне **Карантин**.

d.Для этого также можно воспользоваться контекстным меню, нажав правой кнопкой мыши в окне **Карантин** и выбрав пункт **Карантин**

Восстановление из карантина

Файлы, помещенные на карантин, можно также восстановить в исходное расположение.

• Для этого щелните правой кнопкой мыши файл, помещенный на карантин, и в контекстном меню нажмите кнопку **Восстановить**.

• Если файл помечен как потенциально нежелательное приложение, параметр **Восстановить и исключить из сканирования** включен. См. также Исключения.

• Контекстное меню содержит также функцию **Восстановить в**, которая позволяет восстановить файл в расположение, отличное от исходного.

• Функция восстановления недоступна в некоторых случаях, например, для файлов, расположенных в сетевой папке, доступной только для чтения.

Удаление из карантина

Щелкните элемент правой кнопкой мыши и выберите команду **Удалить из карантина** или выберите элемент, который нужно удалить, и нажмите клавишу **DELETE** на клавиатуре. Если вы хотите выбрать и удалить все элементы в карантине, можно нажать клавиши **Ctrl + A**, а затем клавишу **Delete** на клавиатуре. Удаленные элементы безвозвратно удаляются с вашего устройства и из карантина.

Отправка файла из карантина

Если на карантин помещен файл, который не распознан программой, или файл неверно квалифицирован как зараженный (например, в результате ошибки эвристического метода кода) и изолирован, передайте образец в исследовательскую лабораторию ESET для проведения анализа. Чтобы отправить файл, щелкните его правой кнопкой мыши и в контекстном меню выберите пункт **Передать на анализ**.

Описание обнаружения

Щелкните элемент правой кнопкой мыши и выберите пункт **Описание обнаружения**, чтобы открыть энциклопедию угроз ESET, которая содержит подробную информацию об опасностях и симптомах зарегистрированного заражения.

Иллюстрированные инструкции

Следующие статьи из базы знаний ESET могут быть доступны только на английском языке:

- Восстановление файла из карантина в ESET Security Ultimate
- Удаление помещенного в карантин файла в ESET Security Ultimate
- Продукт ESET уведомил меня об обнаружении. Что мне делать?

Не удалось отправить на карантин

Ниже указаны причины, по которым определенные файлы не могут быть перемещены в

карантин.

- **У вас нет разрешений на чтение**: это означает, что вы не можете просматривать содержимое файла.

- **У вас нет разрешений на запись**: это означает, что вы не можете изменять содержимое файла, т. е. добавлять новое содержимое или удалять существующее.

- **Файл, который вы пытаетесь отправить на карантин, слишком велик**: необходимо уменьшить размер файла.

Если вы получили сообщение об ошибке «Не удалось отправить на карантин», щелкните **Подробнее**. Откроется окно со списком ошибок карантина, где вы увидите имя файла и причину, по которой не удается поместить файл на карантин.

Выбор образца для анализа

При обнаружении подозрительного файла на компьютере или подозрительного сайта в Интернете его можно отправить на анализ в исследовательскую лабораторию ESET (может быть недоступно в зависимости от конфигурации ESET LiveGrid®).

Перед отправкой образцов в ESET

Вы можете отправлять только образцы, которые соответствуют по крайней мере одному из следующих критериев:
• Программа ESET не обнаруживает образец.
• Образец ошибочно обнаруживается как угроза.
• Мы не принимаем личные файлы (которые вы хотите просканировать на наличие вредоносных программ с помощью ESET) в качестве образцов (вирусная лаборатория ESET не проводит сканирование по запросу пользователей).
• Тема письма должна описывать проблему, а текст должен содержать как можно более полную информацию о файле (например, снимок экрана или адрес веб-сайта, с которого он был загружен).

Отправить образец (файл или веб-сайт) на анализ в ESET можно одним из следующих способов.

1. Воспользуйтесь формой отправки образца в своем продукте. Чтобы открыть ее, нажмите **Сервис** > **Отправка образца на анализ**. Максимальный размер отправляемого образца — 256 МБ.

2. Файл также можно отправить по электронной почте. Если этот способ для вас удобнее, заархивируйте файлы с помощью программы WinRAR/WinZIP, защитите архив паролем «infected» и отправьте его по адресу samples@eset.com.

3. Чтобы сообщить о спаме, ложном обнаружении спама или веб-сайтах, которые модуль родительского контроля отнес не к той категории, ознакомьтесь с этой статьей в базе знаний ESET.

В форме **Выбор образца для анализа** выберите раскрывающееся меню **Причина отправки файла** и укажите наиболее подходящее описание своего сообщения:

- Подозрительный файл

- Подозрительный сайт (веб-сайт, зараженный вредоносной программой)
- Ложно обнаруженный сайт
- Ложно обнаруженный файл (файл обнаружен как зараженный, хотя не является таковым)
- Другое

Файл/сайт: путь к отправляемому на анализ файлу или веб-сайту.

Адрес электронной почты: адрес отправляется в ESET вместе с подозрительными файлами и может использоваться для запроса дополнительной информации, необходимой для анализа. Указывать адрес электронной почты необязательно. Чтобы не заполнять это поле, выберите вариант **Отправить анонимно**

> **Вы можете не получить ответа от ESET**
> Поскольку каждый день на серверы ESET поступают десятки тысяч файлов, невозможно отправить ответ на каждый запрос. Вам ответят только в том случае, если для анализа потребуется дополнительная информация.
> Если образец окажется вредоносным приложением или веб-сайтом, его обнаружение будет добавлено при следующем обновлении программы ESET.

Выбор образца для анализа — подозрительный файл

Обнаруженные признаки и симптомы заражения вредоносной программой: введите описание поведения подозрительного файла на вашем компьютере.

Источник файла (URL-адрес или поставщик): укажите источник файла и опишите, как он попал на ваш компьютер.

Примечания и дополнительная информация: здесь можно ввести дополнительную информацию или описание, которые помогут в обработке подозрительного файла.

> Первый параметр (**Обнаруженные признаки и симптомы заражения вредоносной программой**) является обязательным, но предоставление дополнительной информации также очень поможет идентифицировать и обработать образцы в лаборатории.

Выбор образца для анализа — подозрительный сайт

В раскрывающемся меню **Проблема с сайтом** выберите одно из следующих значений.

- **Зараженный**: веб-сайт содержит вирусы или другие вредоносные программы, которые распространяются различными способами.
- **Фишинг** часто используется для получения доступа к конфиденциальным сведениям,

таким как номера банковских счетов, PIN-коды и т. п. Дополнительную информацию об этом типе атаки см. в глоссарии.

• **Мошеннический**: фальшивый или мошеннический веб-сайт, созданный для быстрого получения прибыли.

• Выберите **Другое**, если вышеуказанные варианты не соответствуют сайту, о котором вы сообщаете.

Примечания и дополнительная информация: можно ввести дополнительные сведения или описание, которые помогут проанализировать подозрительный веб-сайт.

Выбор образца для анализа — ложно обнаруженный файл

Мы просим отправлять файлы, которые обнаруживаются как зараженные, но при этом не являются таковыми, чтобы мы могли улучшить наш модуль защиты от вирусов и шпионских программ и обеспечить защиту другим пользователям. Ложное обнаружение возможно, когда шаблон файла совпадает с таким же шаблоном, присутствующим в модуле обнаружения.

Имя и версия приложения: имя программы и ее версия (например, номер, псевдоним или кодовое название).

Источник файла (URL-адрес или поставщик): укажите источник файла и опишите, как он попал на ваш компьютер.

Цель приложения: это общее описание приложения, его типа (например, браузер, проигрыватель мультимедиа и т. п.) и функциональности.

Примечания и дополнительная информация: здесь можно ввести дополнительную информацию или описание, которые помогут в обработке подозрительного файла.

> Первые три параметра нужно указать, чтобы идентифицировать нормальные приложения и отличить их от вредоносного кода. Предоставление дополнительной информации в значительной степени помогает лаборатории в процессе идентификации и обработки образцов.

Выбор образца для анализа — ложно обнаруженный сайт

Мы просим отправлять нам сведения о сайтах, которые определены как зараженные, мошеннические или фишинговые, но таковыми не являются. Ложное обнаружение возможно, когда шаблон файла совпадает с таким же шаблоном, присутствующим в модуле обнаружения. Отправьте нам сведения об этом веб-сайте, чтобы мы могли улучшить наш модуль защиты от вирусов и фишинга и обеспечить защиту других пользователей.

Примечания и дополнительная информация: здесь можно ввести дополнительную информацию или описание, которые помогут в обработке подозрительного веб-сайта.

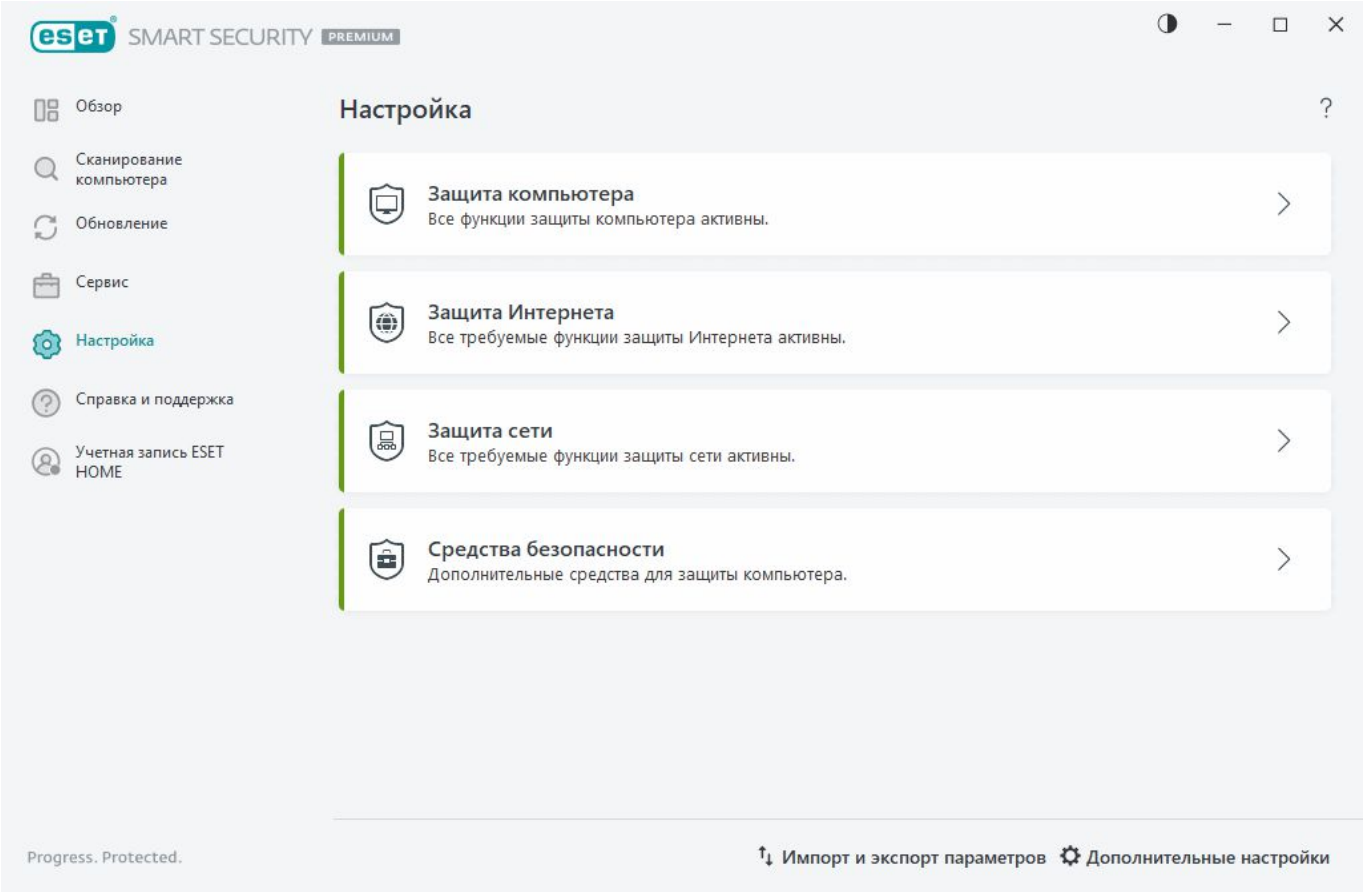
Выбор образца для анализа — другое

Этот вариант следует использовать, если файл невозможно отнести к категории **Подозрительный файл** или **Ложное срабатывание**.

Причина отправки файла: введите подробное описание и причину отправки файла.

Настройка

Группы доступных функций защиты можно найти в главном окне программы в разделе **Настройка**.



Меню **Настройка** содержит следующие разделы:

Защита компьютера

Защита в Интернете

Защита сети

Средства безопасности

В нижней части окна настройки есть дополнительные параметры. Чтобы выполнить более подробную настройку параметров для каждого модуля, щелкните Расширенные параметры.

Чтобы загрузить параметры настройки из файла конфигурации в формате .xml или сохранить текущие параметры настройки в файл конфигурации, воспользуйтесь функцией Импорт и экспорт параметров.

Защита компьютера

Щелкните элемент **Защита компьютера** в главном окне программы в разделе **Настройка**, чтобы просмотреть общие сведения обо всех модулях защиты.

• Защита файловой системы в режиме реального времени: при открытии, создании или исполнении файлов они сканируются на наличие вредоносного кода.

• ESET LiveGuard — добавляет уровень облачной защиты, специально разработанный для устранения невиданных ранее угроз.

• Проактивная защита: блокировка исполнения новых файлов до получения результата анализа ESET LiveGuard. Если вы хотите разблокировать анализируемый файл, щелкните его правой кнопкой мыши и выберите **Разблокировать файл, проанализированный службой ESET LiveGuard**.

• Контроль устройств: этот модуль используется для сканирования, блокирования и изменения расширенных фильтров и разрешений. С его помощью пользователь может выбирать способ получения доступа к конкретному устройству (компакт- или DVD-диску, USB-накопителю и т. д.) и работы с ним.

• Система HIPS: система предотвращения вторжений на узел отслеживает события в операционной системе и реагирует на них в соответствии с существующим набором правил.

• Игровой режим: включение или отключение игрового режима. После включения игрового режима на экран будет выведено предупреждение (о потенциальной угрозе безопасности), а для оформления главного окна будет применен оранжевый цвет.

• Защита веб-камеры: контролирует процессы и приложения, осуществляющие доступ к подключенной камере.

Чтобы приостановить или отключить отдельные модули защиты, щелкните значок переключателя .

⚠ Отключение модулей может привести к снижению уровня защиты вашего компьютера.

Щелкните значок шестеренки рядом с модулем защиты, чтобы получить доступ к его расширенным настройкам.

Для **защиты файловой системы в реальном времени** щелкните значок шестеренки и выберите один из следующих вариантов.

• **Настроить**: будут открыты расширенные параметры защиты файловой системы в реальном времени.

• **Изменить исключения**: будет открыто окно настройки исключений, в котором можно

исключить файлы и папки из сканирования.

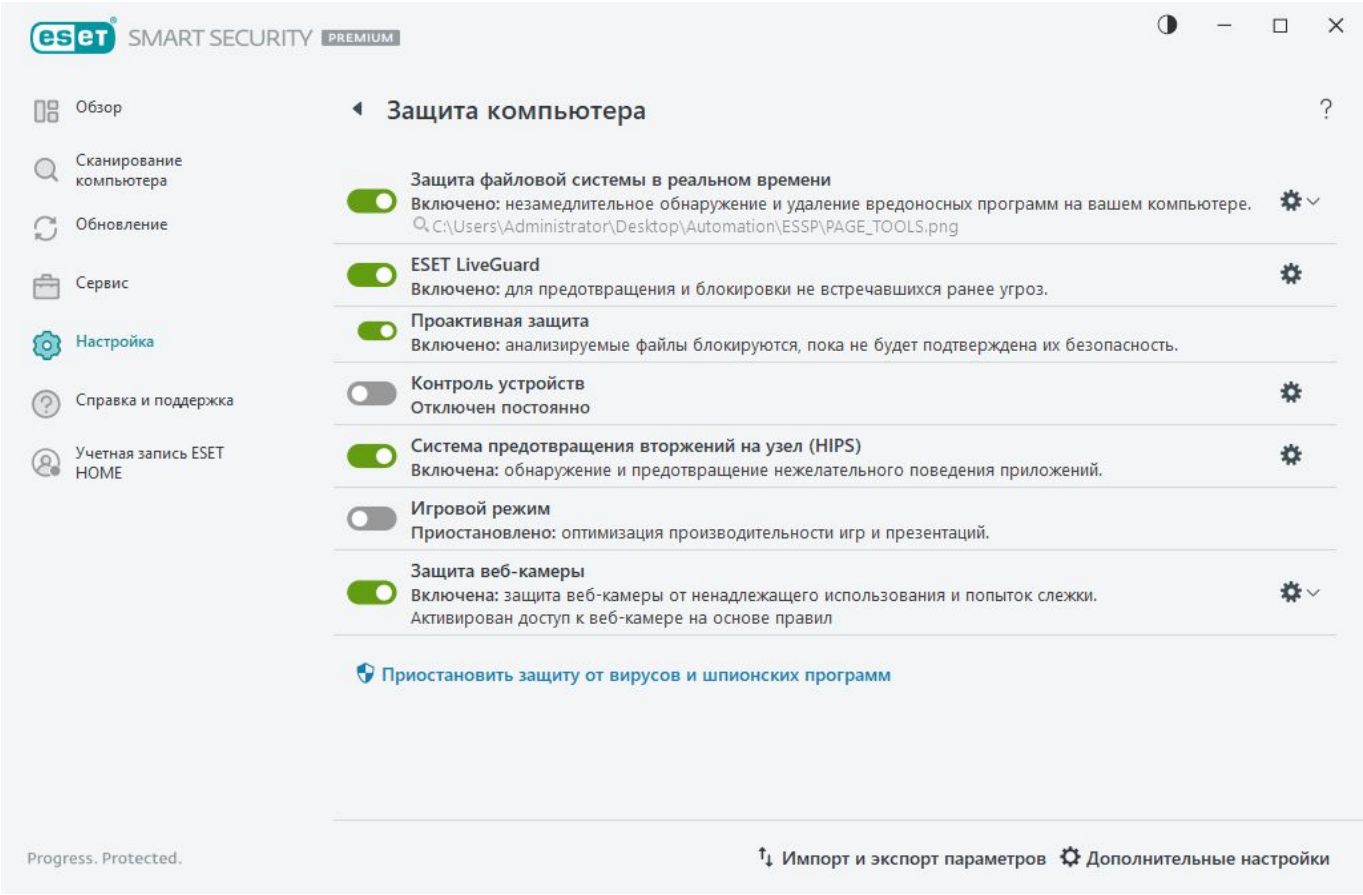
Для **защиты веб-камеры** щелкните значок шестеренки и выберите один из следующих вариантов.

• **Настроить**: будут открыты расширенные параметры защиты веб-камеры.

• **Заблокировать все попытки доступа до перезапуска**: блокировка всех попыток доступа к веб-камере до перезапуска компьютера.

• **Заблокировать все попытки доступа постоянно**: блокировка всех попыток доступа к веб-камере до отключения этого параметра.

• **Остановить блокировку всех попыток доступа**: отключение возможности блокировать доступ к веб-камере. Этот параметр доступен, только если доступ к веб-камере заблокирован.



Приостановить защиту от вирусов и шпионских программ: отключение всех модулей защиты от вирусов и шпионских программ. При отключении защиты отображается окно, где можно задать время, на которое она будет отключена, выбрав значение в раскрывающемся меню **Интервал времени**. Используйте эту возможность, только если вы опытный пользователь или получили соответствующую инструкцию от службы технической поддержки ESET.

Действия при обнаружении заражения

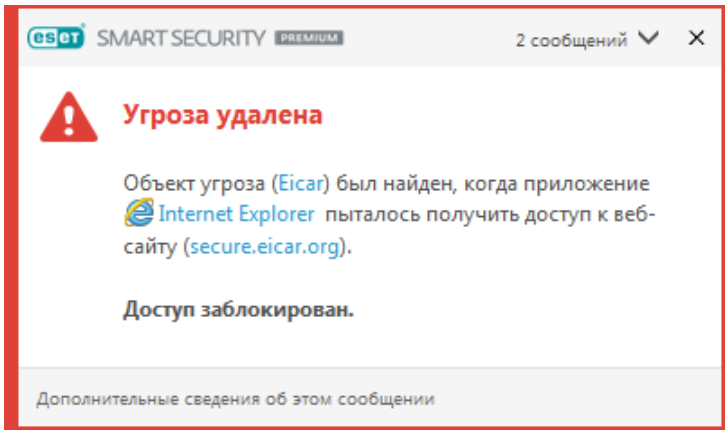
Заражения могут попасть на компьютер из различных источников, таких как веб-сайты, общие папки, электронная почта или съемные носители (накопители USB, внешние диски, компакт- или DVD-диски и т. д.).

Стандартное поведение

Обычно ESET Security Ultimate обнаруживает заражения с помощью перечисленных ниже модулей.

- Защита файловой системы в режиме реального времени
- Защита доступа в Интернет
- Защита почтового клиента
- сканирование компьютера по требованию;

Каждый модуль использует стандартный уровень очистки и пытается очистить файл, поместить его в карантин или прервать подключение. В правом нижнем углу экрана отображается окно уведомлений. Подробные сведения об обнаруженных и очищенных объектах можно найти в файлах журнала. Дополнительные сведения об уровнях очистки и поведении см. в разделе Уровень очистки.



Сканирование компьютера на наличие зараженных файлов

Если на компьютере возникли признаки заражения вредоносной программой (например, он стал медленнее работать, часто зависает и т. п.), рекомендуется выполнить следующие действия.

1.Откройте ESET Security Ultimate и выберите команду «**Сканирование компьютера**».

2.Выберите вариант **Сканировать компьютер** (дополнительную информацию см. в разделе Сканирование компьютера).

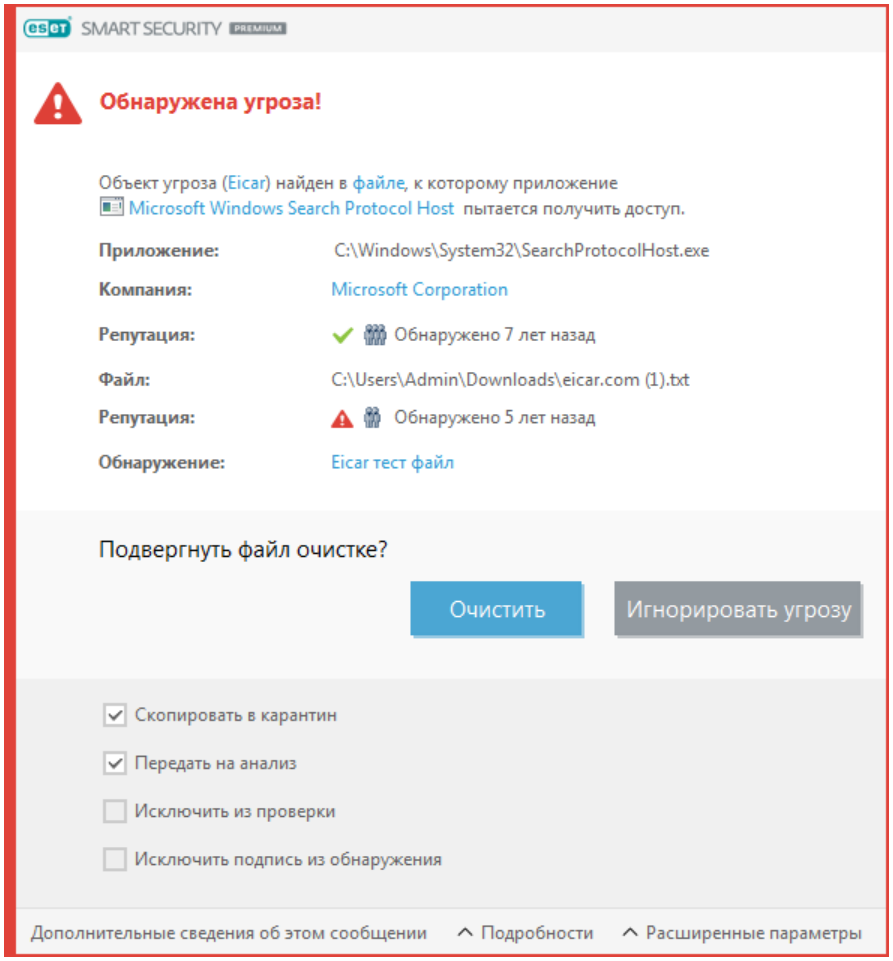
3.По завершении сканирования просмотрите в журнале количество проверенных,

зараженных и очищенных файлов.

Если следует сканировать только определенную часть диска, выберите вариант **Выборочное сканирование** и укажите объекты, которые нужно сканировать на предмет наличия вирусов.

Очистка и удаление

Если действие по умолчанию для модуля защиты файловой системы в режиме реального времени не определено, пользователю предлагается выбрать его в окне предупреждения. Обычно доступны варианты **Очистить**, **Удалить** или **Ничего не предпринимать**. Не рекомендуется выбирать действие **Ничего не предпринимать**, поскольку при этом зараженные файлы не будут очищены. Исключение допустимо только в том случае, если вы уверены, что файл безвреден и был обнаружен по ошибке.



Очистку следует применять, если файл был атакован вирусом, который добавил к нему вредоносный код. В этом случае сначала программа пытается очистить зараженный файл, чтобы восстановить его первоначальное состояние. Если файл содержит только вредоносный код, его следует удалить.

Если зараженный файл заблокирован или используется каким-либо системным процессом, обычно он удаляется только после освобождения. Как правило, это происходит после перезапуска системы.

Восстановление из карантина

Карантин можно открыть из главного окна программы ESET Security Ultimate, щелкнув элемент **Сервис** > **Карантин**.

Файлы, помещенные на карантин, можно также восстановить в исходное расположение.

• Для этого щелните правой кнопкой мыши файл, помещенный на карантин, и в контекстном меню нажмите кнопку **Восстановить**.

• Если файл помечен как потенциально нежелательное приложение, параметр **Восстановить и исключить из сканирования** включен. См. также Исключения.

• Контекстное меню содержит также функцию **Восстановить в**, которая позволяет восстановить файл в расположение, отличное от исходного.

• Функция восстановления недоступна в некоторых случаях, например, для файлов, расположенных в сетевой папке, доступной только для чтения.

Множественные угрозы

Если при сканировании компьютера какие-либо зараженные файлы не были очищены (или для параметраУровень очистки было установлено значение **Без очистки**), на экране отобразится окно предупреждения, в котором вам будет предложено выбрать действие для таких файлов. Следует выбрать действия для файлов (действия выбираются отдельно для каждого файла в списке), а затем нажать кнопку **Готово**.

Удаление файлов из архивов.

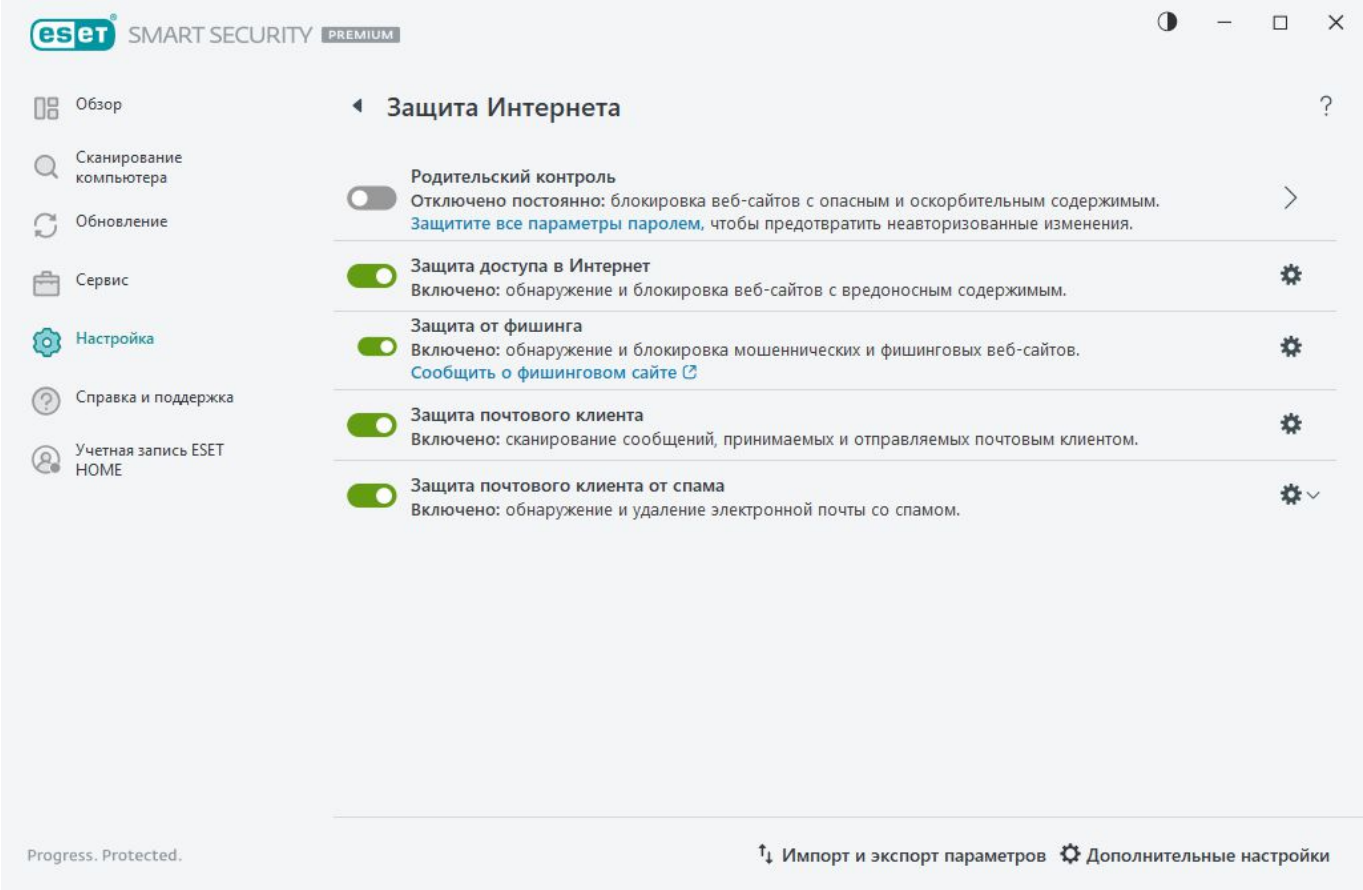
В режиме очистки по умолчанию архив удаляется целиком только в том случае, если он содержит только зараженные файлы. Иначе говоря, архивы, в которых есть незараженные файлы, не удаляются. Однако следует проявлять осторожность при сканировании в режиме тщательной очистки, так как при этом архив удаляется, если содержит хотя бы один зараженный файл, независимо от состояния других файлов в архиве.

Защита в Интернете

Подключение к Интернету стало стандартной функцией персонального компьютера. К сожалению, Интернет также стал и основной средой распространения вредоносного кода. Откройте главное окно программы > **Настройка** > **Защита Интернета**, чтобы настроить функции ESET Security Ultimate, повышающие вашу защиту в Интернете.

Чтобы приостановить или отключить отдельные модули защиты, щелкните значок переключателя  .

⚠ Отключение модулей может привести к снижению уровня защиты вашего компьютера.



Щелкните значок шестеренки ⚙ рядом с модулем защиты, чтобы получить доступ к его расширенным настройкам.

Модуль родительского контроля обеспечивает защиту для детей, блокируя нежелательное или опасное содержимое в Интернете.

Защита доступа в Интернет сканирует обмен данными по протоколу HTTP/HTTPS на наличие вредоносных программ и фишинга. Отключать защиту доступа в Интернет следует только для устранения неполадок.

Защита от фишинга дает возможность блокировать веб-страницы, на которых есть фишинговое содержимое. Настоятельно рекомендуется оставить все опции защиты от фишинга включенными.

Сообщить о фишинговом сайте: отправьте сведения о фишинговом или вредоносном веб-сайте в ESET для анализа.

> Прежде чем отправлять адрес веб-сайта в компанию ESET, убедитесь в том, что он соответствует одному или нескольким из следующих критериев:
> • Веб-сайт совсем не обнаруживается.
> • Веб-сайт неправильно обнаруживается как угроза. В таком случае можно сообщить о ложной метке фишингового сайта.

Защита почтового клиента обеспечивает контроль обмена данными по протоколам POP3(S) и IMAP(S). С помощью подключаемого модуля для почтового клиента программа ESET Security Ultimate позволяет контролировать весь обмен данными, осуществляемый почтовым клиентом.

Защита почтового клиента от спама отфильтровывает нежелательные сообщения электронной

почты.

Для **защиты почтового клиента от спама** щелкните значок шестеренки и выберите одну из следующих опций.

• **Настроить**: переход к расширенным настройкам защиты почтового клиента от спама.

• **Список адресов пользователя** (если включен) — открывает диалоговое окно, в котором можно добавлять, редактировать или удалять адреса для определения правил защиты от спама. Правила в этом списке будут применяться к текущему пользователю.

• **Глобальный список адресов** (если включено) — открывает диалоговое окно, в котором можно добавлять, редактировать или удалять адреса для определения правил защиты от спама. Правила в этом списке будут применяться ко всем пользователям.

Защита от фишинга

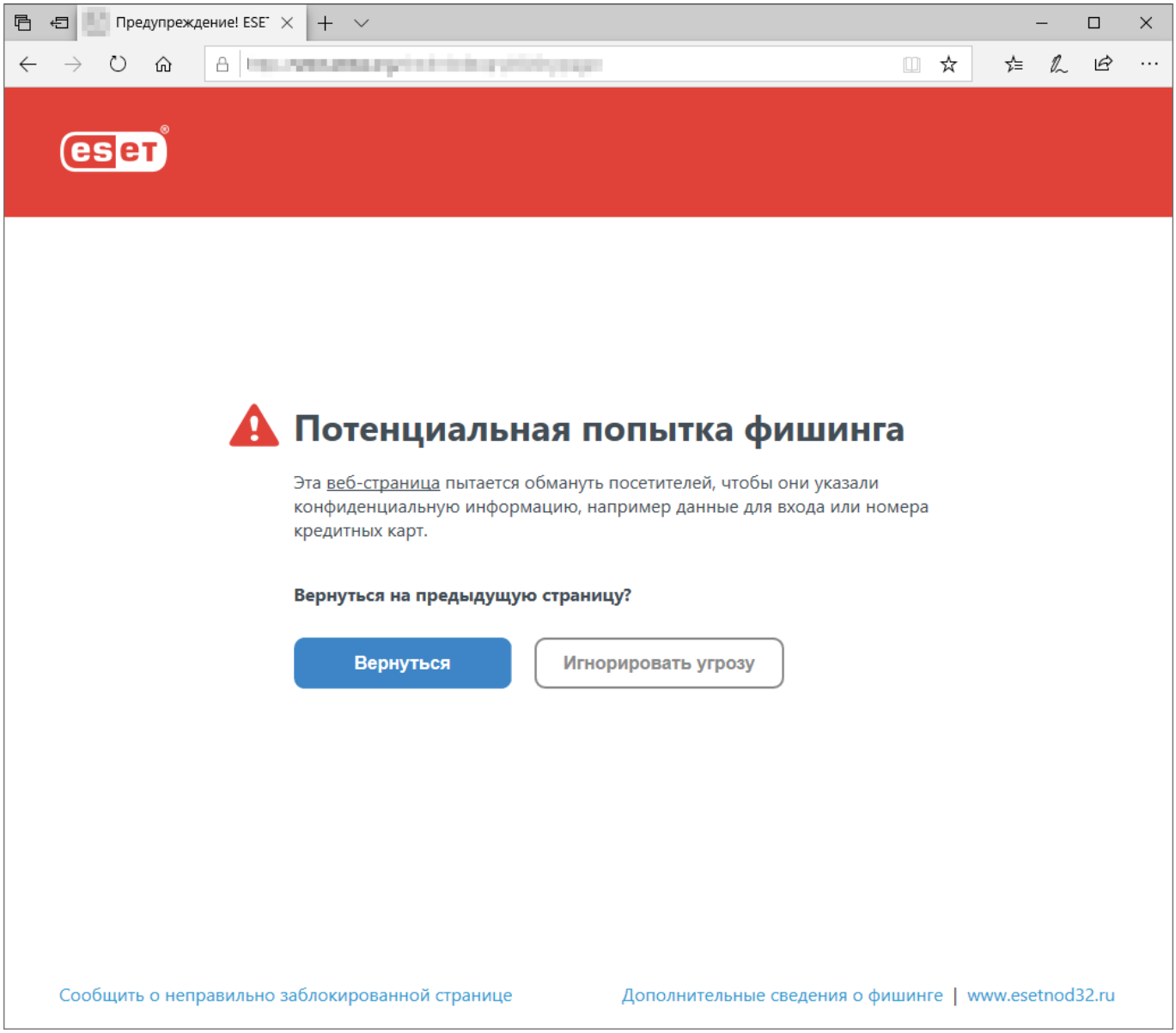
Фишинг — это преступная деятельность с использованием социальной инженерии (манипулирование пользователями для получения конфиденциальной информации). Фишинг используется для получения таких конфиденциальных данных, как номера банковских счетов, PIN-коды и т. д. Дополнительные сведения можно найти в глоссарии. Программа ESET Security Ultimate обеспечивает защиту от фишинга, блокируя веб-страницы, о которых известно, что они распространяют такой тип содержимого.

Защита от фишинга включена по умолчанию. Этот параметр можно настроить в разделе Расширенные параметры > **Защита** > **Защита доступа в Интернет**.

Дополнительные сведения о защите от фишинга в программе ESET Security Ultimate см. в статье нашей базы знаний.

Доступ к фишинговому веб-сайту

При доступе к известному фишинговому веб-сайту в вашем веб-браузере отобразится следующее диалоговое окно. Если вы все равно хотите открыть этот веб-сайт, щелкните элемент **Игнорировать угрозу** (не рекомендуется).



Время, в течение которого можно получить доступ к потенциальному фишинговому веб-сайту, занесенному в «белый» список, по умолчанию истекает через несколько часов. Чтобы разрешить доступ к веб-сайту на постоянной основе, используйте инструмент Управление URL-адресами. В разделе Дополнительные настройки > **Защиты** > **Защита доступа в Интернет** > **Управление URL-адресами** > **Список адресов** > **Изменить** и добавьте необходимый веб-сайт в список.

Сообщить о фишинговом сайте

С помощью ссылки **Сообщить о неправильно заблокированной странице** можно сообщить о веб-сайте, который неправильно определен как угроза.

Или же адрес веб-сайта можно отправить по электронной почте. Отправьте письмо на адрес samples@eset.com. Помните, что тема письма должна описывать проблему, а в тексте письма следует указать максимально полную информацию о веб-сайте (например, веб-сайт, с которого вы попали на этот сайт, как вы узнали об этом сайте и т. д.).

Родительский контроль

Модуль родительского контроля позволяет настраивать соответствующие параметры, которые дают родителям возможность использовать автоматизированные средства для защиты своих детей и задавать ограничения для устройств и служб. Цель заключается в предотвращении доступа детей и подростков к страницам, содержимое которых является для них неприемлемым или вредоносным.

Родительский контроль позволяет блокировать веб-страницы, которые могут содержать потенциально нежелательные материалы. Кроме того, родители могут запрещать доступ к веб-сайтам предварительно заданных категорий (более 40) и подкатегорий (более 140).

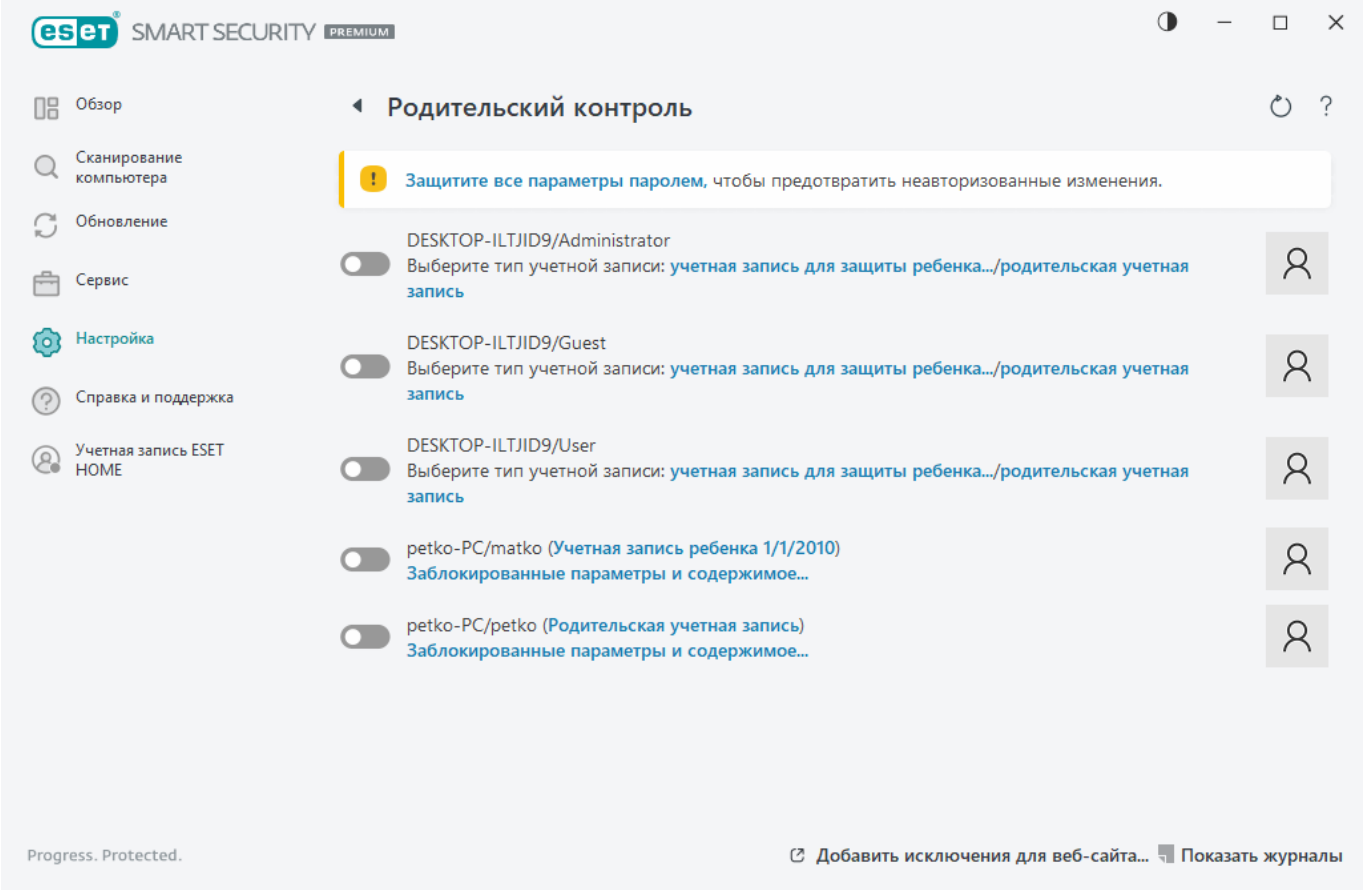
Чтобы активировать родительский контроль для определенной учетной записи пользователя, выполните следующие действия.

1. По умолчанию родительский контроль в программе ESET Security Ultimate отключен. Существует два способа активации родительского контроля.

   • В главном окне программы щелкните элемент  и последовательно выберите элементы **Настройка** > **Защита интернета** > **Родительский контроль**, после чего включите функцию родительского контроля.

   • Откройте раздел Расширенные параметры > **Защита** > **Защита доступа в Интернет** > **Родительский контроль**, а затем включите переключатель рядом с элементом **Включить родительский контроль**.

2. В главном окне программы выберите элементы **Настройка** > **Защита интернета** > **Родительский контроль**. Хотя для параметра **Родительский контроль** и отображается значение **Включено**, необходимо настроить родительский контроль для нужной учетной записи. Для этого щелкните значок стрелки, а в следующем окне выберите элемент **Защитить детскую учетную запись** или **Родительская учетная запись**. В следующем окне укажите дату рождения, чтобы определить уровень доступа и подходящие для этого возраста веб-страницы. Теперь родительский контроль включен для указанной учетной записи. Рядом с именем учетной записи щелкните элемент **Заблокированные параметры и содержимое**, чтобы задать категории, которые требуется разрешить или заблокировать, на вкладке Категории. Чтобы разрешить или заблокировать определенные веб-страницы, которые не соответствуют категории, откройте вкладку Исключения.



Если в главном окне программы ESET Security Ultimate щелкнуть **Настройка** > **Защита интернета** > **Родительский контроль**, вы увидите описанное далее содержимое главного окна.

Учетные записи пользователей Windows

Если вы создали роль для существующей учетной записи, она отобразится здесь. Щелкните ползунок, чтобы рядом с параметром родительского контроля для учетной записи отобразился зеленый флажок. В активной учетной записи щелкните Заблокированные параметры и содержимое, чтобы просмотреть список разрешенных для этой учетной записи категорий веб-страниц, а также заблокированных и разрешенных веб-страниц.

Содержимое нижней части окна

Добавить исключение для веб-сайта : в соответствии с вашими настройками конкретный веб-сайт может быть разрешен или заблокирован отдельно для каждой родительской учетной записи.

Показать журналы: этот параметр позволяет просмотреть подробный журнал действий функции родительского контроля (заблокированные страницы, учетная запись, для которой страница была заблокирована, категория и т. п.). Также этот журнал можно отфильтровать на основе выбранных критериев, нажав кнопку **Фильтрация**.

Родительский контроль

После отключения функции родительского контроля отобразится окно а **Отключить родительский контроль**. С его помощью можно настроить время, на которое отключается

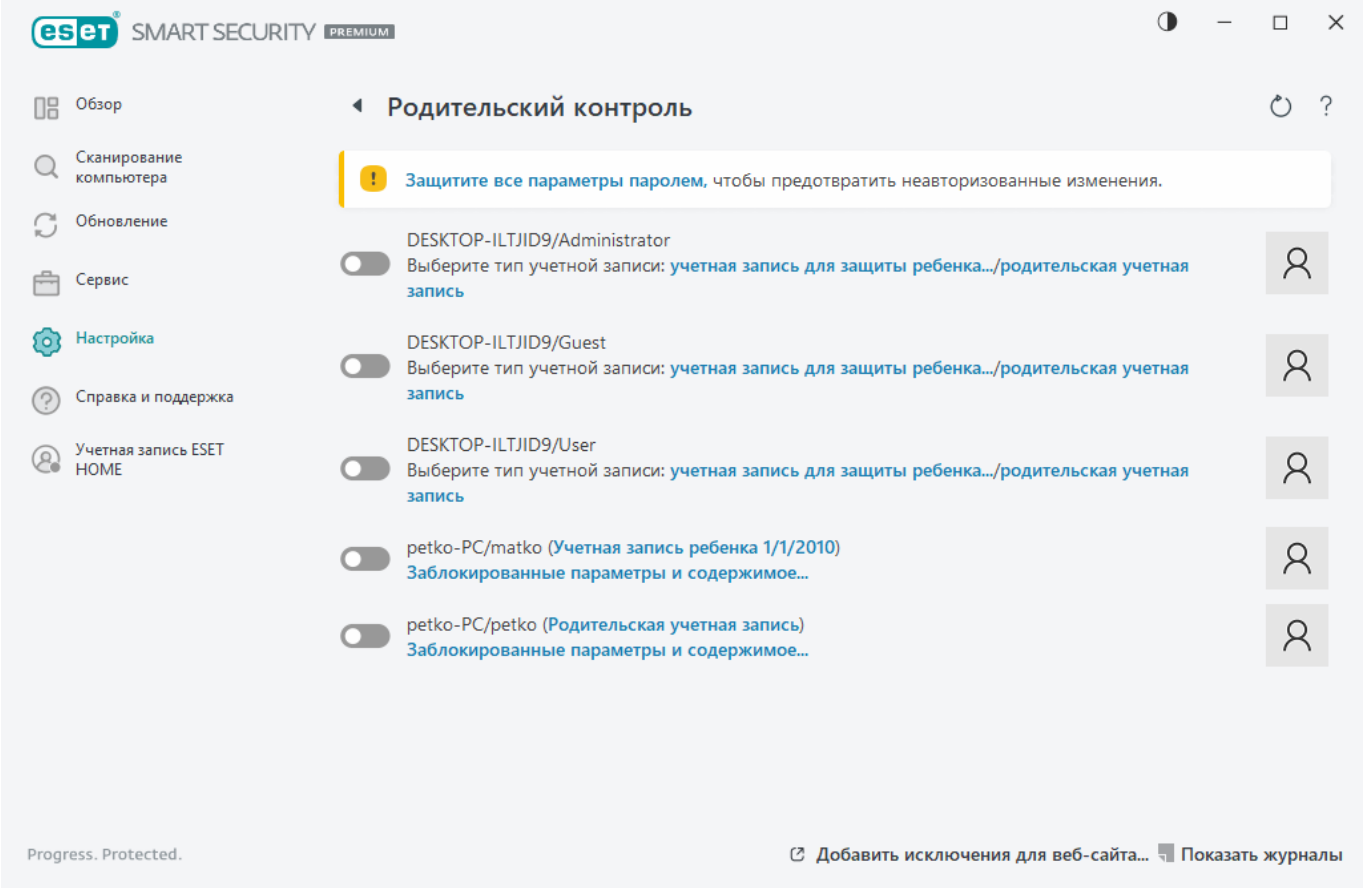
такая защита. После этого значение параметра изменится на **Приостановлено** или **Полностью отключено**.

Важно защищать параметры ESET Security Ultimate паролем. Такой пароль задается в разделе Настройка доступа. Если пароль не задан, отобразится следующее предупреждение: **Защитить все параметры паролем**, чтобы предотвратить несанкционированные изменения. Ограничения, установленные в разделе «Родительский контроль», распространяются только на стандартные учетные записи пользователей. Поскольку администратор может обойти любые ограничения, то они не будут действовать.

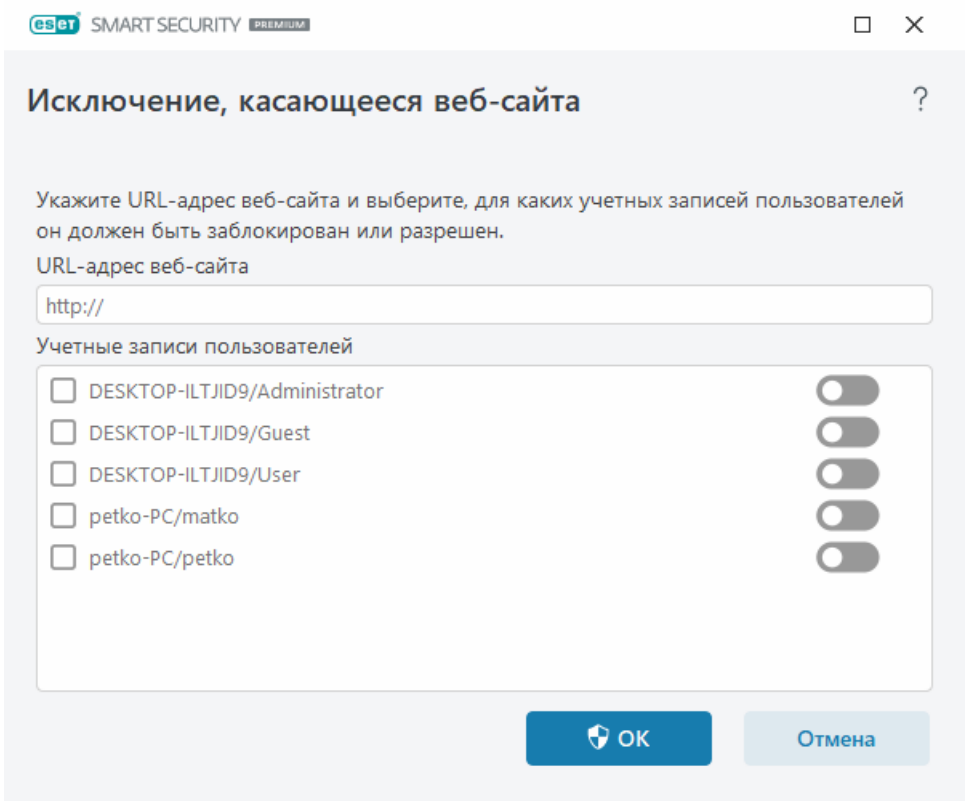
Для правильной работы родительского контроля должны быть включены сканер сетевого трафика, сканирование трафика HTTP(S) и файервол. По умолчанию они включены.

Исключения, касающиеся веб-сайтов

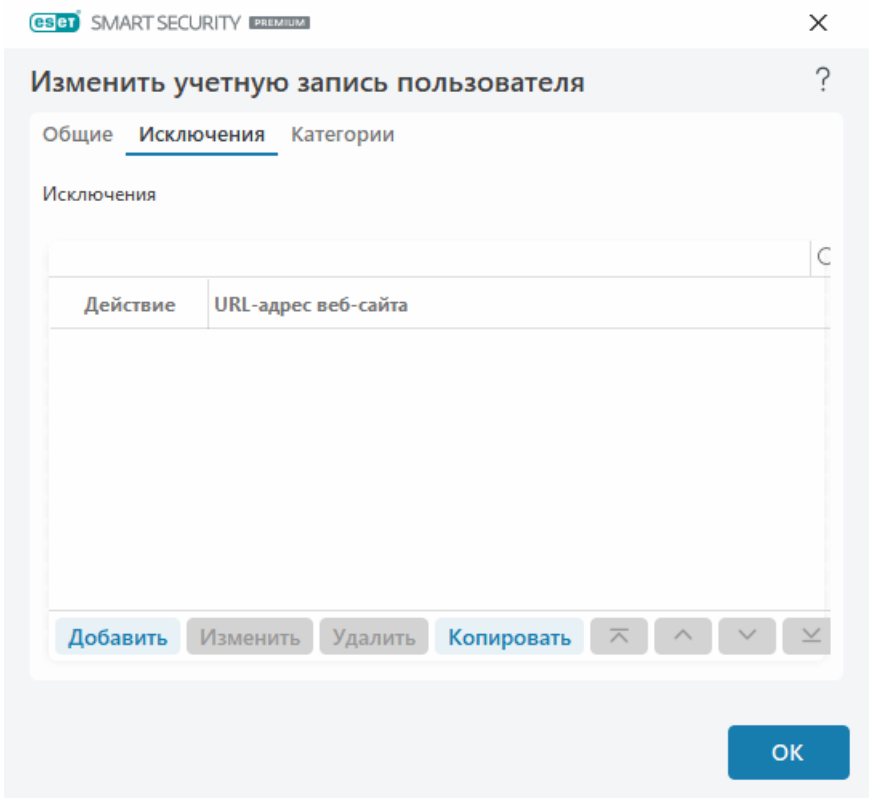
Чтобы добавить исключение для веб-сайта, последовательно выберите элементы **Настройка** > **Защита интернета** > **Родительский контроль**, а затем щелкните элемент **Добавить исключение для веб-сайта**.



Введите URL-адрес в поле **URL-адрес веб-сайта**, выберите ✔ (разрешено) или ⊘ (заблокировано) для каждой учетной записи пользователя, после чего нажмите кнопку **OK**, чтобы добавить исключение в список.



Чтобы удалить URL-адрес из списка, последовательно щелкните элементы **Настройка** > **Защита интернета** > **Родительский контроль**, затем щелкните элемент **Заблокированные параметры и содержимое** для нужной учетной записи, перейдите на вкладку **Исключение**, выберите исключение и нажмите кнопку **Удалить**.



Во всех списках URL-адресов нельзя использовать специальные символы «*» (звездочка) и «?» (вопросительный знак). Например, вручную нужно вводить адреса веб-страниц с несколькими доменами верхнего уровня (examplepage.com*examplepage.com, examplepage.sk*examplepage.sk и т. д.).

При добавлении домена в список все содержимое, расположенное в нем и во всех поддоменах (например, sub.examplepage.com*sub.examplepage.com*), будет разрешено или заблокировано в зависимости от выбранного вами действия на основе URL-адреса.

Блокирование или разрешение конкретной веб-страницы может быть более точным, чем блокирование или разрешение категории веб-страниц. Следует быть особенно внимательным при изменении этих параметров и добавлении категории или веб-страницы в список.

Копирование исключения из пользователя

Выберите пользователя в раскрывающемся списке, откуда требуется скопировать созданное исключение.

Копирование категорий из учетной записи

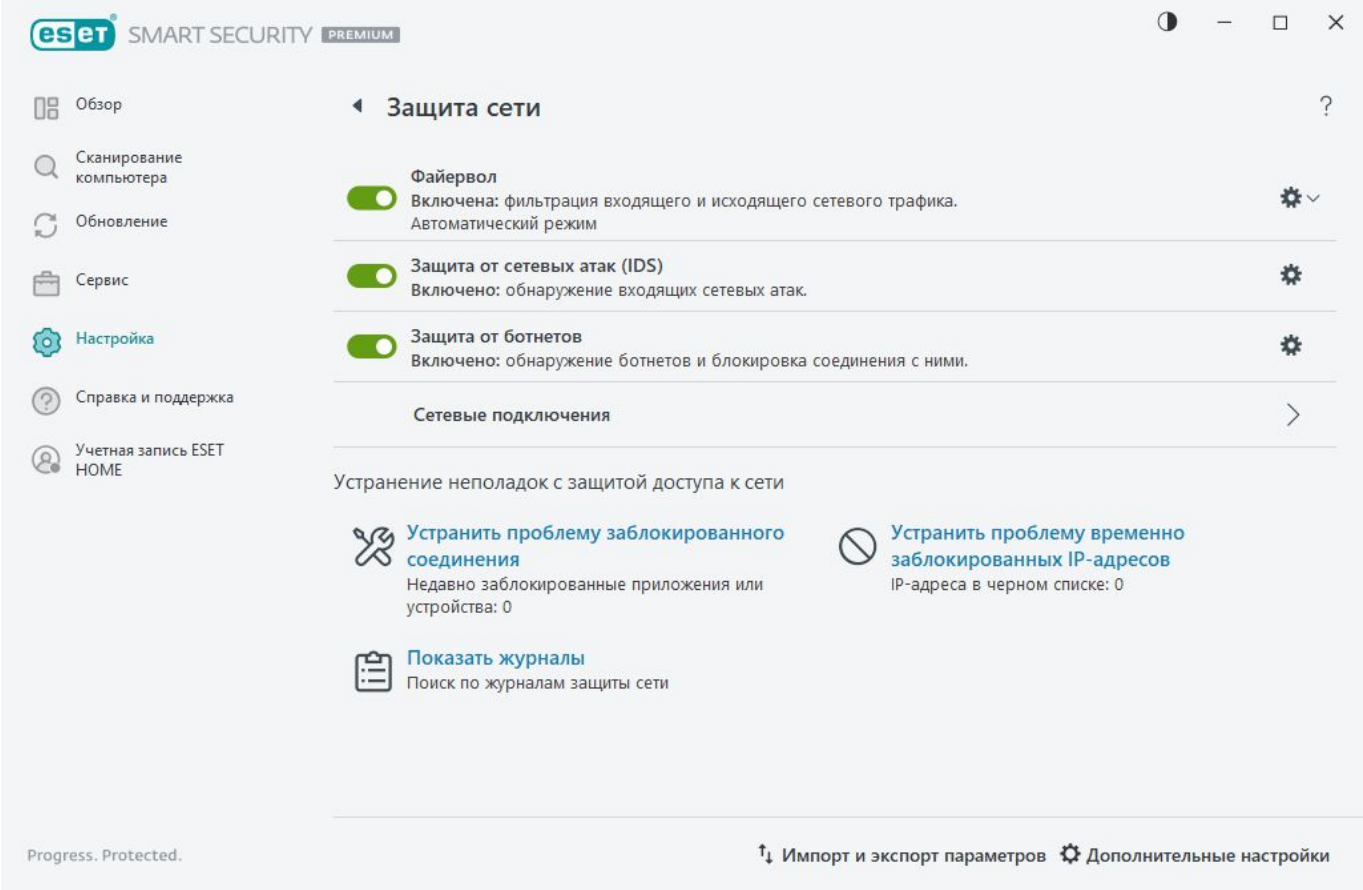
Позволяет скопировать список заблокированных или разрешенных категорий из существующей измененной учетной записи.

Защита сети

Откройте главное окно программы > **Настройка** > **Защита сети**, чтобы настроить основные параметры защиты сети или устранить неполадки сетевого подключения.

Чтобы приостановить или отключить отдельные модули защиты, щелкните значок переключателя  .

Отключение модулей может привести к снижению уровня защиты вашего компьютера.



Щелкните значок шестеренки ⚙ рядом с модулем защиты, чтобы получить доступ к его расширенным настройкам.

Файервол: фильтрует весь сетевой обмен данными согласно конфигурации ESET Security Ultimate.

Настроить: открывается окно «Файервол» меню дополнительных настроек, в котором можно определить, каким образом файервол будет обрабатывать сетевой обмен данными.

Приостановить работу файервола (разрешить весь трафик): В этом режиме файервол отключает все функции фильтрации и разрешает все входящие и исходящие соединения. Щелкните **Включить файервол**, чтобы повторно включить файервол, когда для фильтрации сетевого трафика включен этот режим.

Блокировать весь трафик: все входящие и исходящие соединения будут блокироваться файерволом. Используйте этот параметр только в особых случаях, когда возникает опасная критическая ситуация, требующая немедленного отключения от сети. Если для фильтрации сетевого трафика выбрано состояние **Блокировать весь трафик**, щелкните **Остановить блокировку всего трафика**, чтобы восстановить нормальную работу файервола.

Автоматический режим (если включен другой режим фильтрации): воспользуйтесь этой командой, чтобы перевести фильтрацию в автоматический режим (с учетом правил, определяемых пользователем).

Интерактивный режим (если включен другой режим фильтрации): воспользуйтесь этой командой, чтобы перевести фильтрацию в интерактивный режим.

Защита от сетевых атак (IDS): анализ содержимого сетевого трафика и защита от сетевых атак. Любой трафик, который определяется как «вредоносный», будет заблокирован. ESET Security Ultimate будет информировать при подключении к незащищенной беспроводной сети или сети

со слабой защитой.

Защита от ботнетов: быстрое и точное выявление вредоносных программ на компьютере.

Сетевые подключения: отображение сетей, к которым подключены сетевые адаптеры, с подробными сведениями.

Устранить проблему заблокированного соединения: помогает устранять проблемы с подключением, вызванные файерволом ESET. Для получения дополнительных сведений см. раздел Мастер устранения неполадок.

Устранить проблему временно заблокированных IP-адресов — Просмотр списка IP-адресов, которые обнаружены как источники атак и добавлены в черный список, чтобы блокировать соединение в течение определенного периода времени.

Показать журналы: открывает файл журнала защиты сети.

Сетевые подключения

Отображение сетей, к которым подключены сетевые адаптеры. Чтобы просмотреть сетевые подключения, откройте главное окно программы > **Настройка** > **Защита сети** > **Сетевые подключения**.

Дважды щелкните подключение в списке, чтобы отобразить сведения о нем и о сетевом адаптере.

Наведите курсор на конкретное сетевое подключение и щелкните значок меню ⋮ в столбце **Доверенное**, чтобы выбрать одну из следующих опций:

- **Изменить** — открывает окно Настройка защиты сети, в котором можно назначить профиль защиты определенной сети.
- **Забыть** — сбрасывает конфигурацию сетевого подключения до значений по умолчанию.
- **Сканировать сеть с помощью Инспектора сети** — открывает Инспектор сети для запуска сканирования сети.
- **Пометить как «Моя сеть»** — добавляет к сети тег «Моя сеть». Этот тег будет отображаться рядом с сетью в программе ESET Security Ultimate для улучшения идентификации и общих сведений о безопасности.
- **Снять пометку «Моя сеть»** — удаляет тег «Моя сеть». Этот параметр доступен только в том случае, если сеть уже помечена тегом.

Сведения о сетевом подключении

Дважды щелкните подключение в списке Сетевые подключения, чтобы отобразить сведения о нем и о сетевом адаптере. С помощью сведений о сетевом подключении и адаптере можно определить сеть, которую вы пытаетесь настроить в разделе Защита доступа к сети.

Сведения о сетевом подключении:

- Состояние сетевого подключения
- Дата и время первого обнаружения сети
- Время последней активности сети
- Общее время подключения к этой сети
- Профиль сетевого подключения
- Профиль сетевого подключения, определенный в Windows
- Конфигурация защиты сети (является ли сеть доверенной)

Сведения о сетевом адаптере:

- Тип подключения (проводное, виртуальное и т. д.)
- Имя сетевого адаптера
- Описание адаптера
- IP-адрес и MAC-адрес
- IPv4- и IPv6-адрес сети с подсетью
- DNS-суффикс
- IP-адрес DNS-сервера
- IP-адрес DHCP-сервера
- IP- и MAC-адрес шлюза по умолчанию
- MAC-адрес адаптера

Устранение неполадок с доступом к сети

Мастер устранения неполадок помогает устранить проблемы с подключениями, вызванные файерволом. Параметр **Устранение неполадок с доступом к сети** можно найти в главном окне программы в разделе **Настройка** > **Защита сети** > **Устранить проблему заблокированного соединения**.

Выберите, что необходимо отобразить — соединение, заблокированное для **локальных приложений**, или заблокированный обмен данными с **удаленных устройств**.

Выберите в раскрывающемся меню период времени, в течение которого связь была заблокирована. Список недавно заблокированных подключений отображает общие данные о типе приложения или устройства, репутации и общем числе приложений и устройств, заблокированных в течение такого периода времени. Нажмите кнопку **Подробности**, чтобы просмотреть подробные сведения о заблокированном подключении. Затем разблокируйте

приложение или устройство, с которым возникли проблемы подключения.

После нажатия кнопки **Разблокировать** ранее заблокированное подключение будет разрешено. Если проблемы с приложением продолжаются или ваше устройство не работает надлежащим образом, щелкните **Создание еще одного правила**, и все подключения, ранее заблокированные для этого устройства, будут разрешены. Если это не поможет, перезагрузите компьютер.

Щелкните **Открыть правила файервола**, чтобы просмотреть правила, созданные мастером. Кроме того, просмотреть правила, созданные мастером, можно в разделе Расширенные параметры > **Защита** > **Защита доступа к сети** > **Файервол** > **Правила** > **Изменить**.

Если правило не может быть создано, отобразится сообщение об ошибке. Щелкните **Повторить попытку** и повторите этот процесс, чтобы разблокировать обмен данными, или создайте еще одно правило из списка заблокированных подключений.

Временный черный список IP-адресов

Чтобы просмотреть список IP-адресов, которые были обнаружены как источники атак и добавлены в черный список для блокировки соединений в течение определенного периода времени, откройте главное окно программы > **Настройка** > **Защита сети** > **Устранить проблему временно заблокированных IP-адресов**. Временно блокируемые IP-адреса блокируются на 1 час.

Столбцы

IP-адрес. Отображение IP-адреса, который был заблокирован.

Причина блокирования: отображение типа атаки, которая была предотвращена с адреса (например, атака сканирования портов TCP).

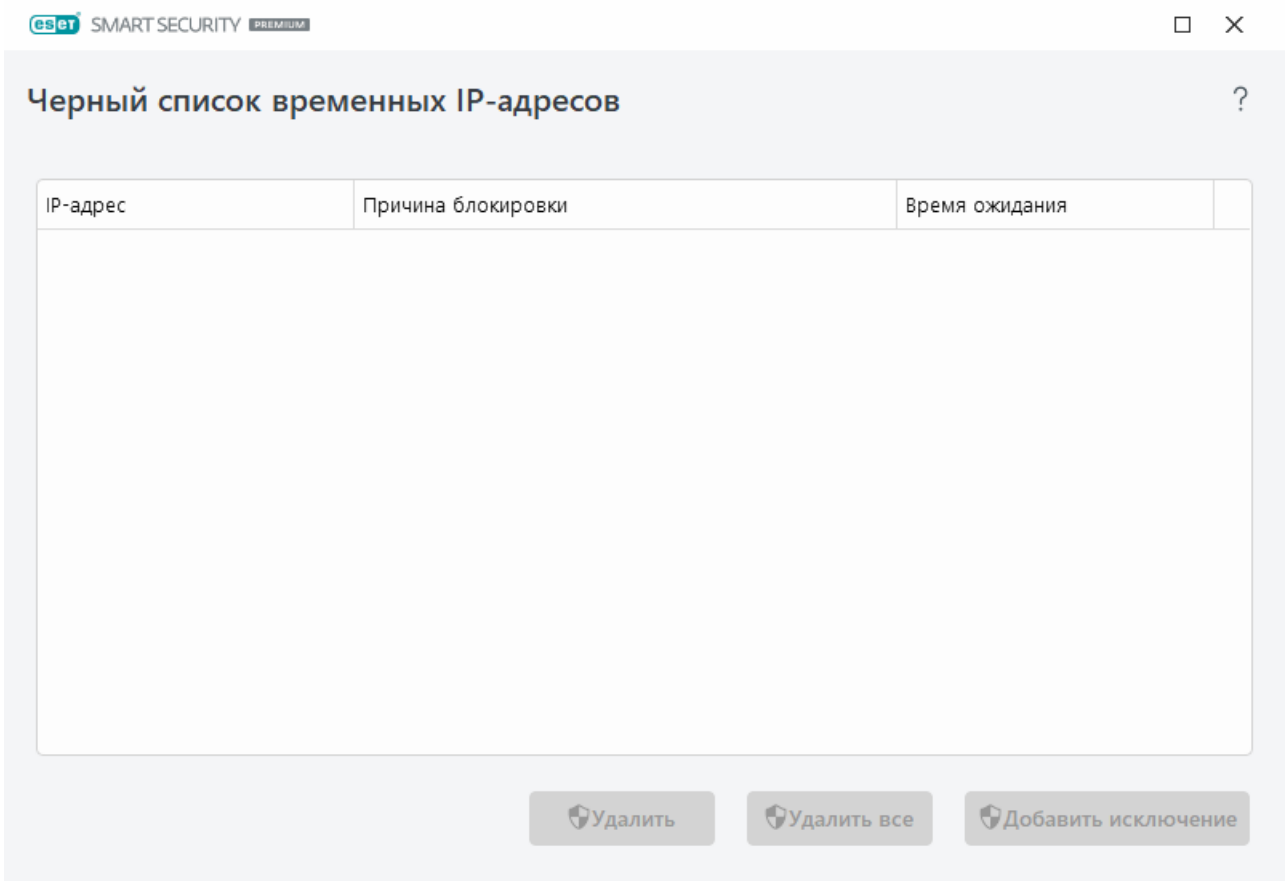
Время ожидания: отображение времени и даты, когда адрес будет удален из «черного» списка.

Элементы управления

Удалить. Щелкните, чтобы удалить IP-адрес из черного списка до того, как истечет срок действия списка.

Удалить все. Щелкните, чтобы немедленно удалить все адреса из черного списка.

Добавить исключение. Щелкните, чтобы добавить исключение файервола в фильтрацию IDS.



Журналы защиты сети

Функция защиты сети программы ESET Security Ultimate сохраняет сведения обо всех важных событиях в файл журнала. Для просмотра файла журнала откройте главное окно программы > **Настройка** > **Защита сети** > **Показать журналы**.

Файлы журнала могут использоваться для обнаружения ошибок и вторжений на компьютер. Журналы защиты сети содержат следующие сведения:

- Дата и время события.
- имя события;
- источник;
- сетевой адрес целевого объекта;
- сетевой протокол связи;
- Примененное правило или имя червя (если определено).
- Путь и имя приложения.
- Хэш
- Пользователь.
- Лицо, подписавшее приложение (издатель).

- Имя пакета
- Имя службы.

Тщательный анализ информации значительно облегчает процесс оптимизации безопасности компьютера. Многие факторы являются признаками потенциальных угроз и позволяют пользователю свести их влияние к минимуму: частые соединения от неизвестных компьютеров, множественные попытки установить соединение, сетевая активность неизвестных приложений или с использованием неизвестных номеров портов.

> **Использование уязвимости в системе безопасности**
> Сообщение об использовании уязвимости в системе безопасности записывается даже в том случае, если конкретная уязвимость уже исправлена, так как попытка использования обнаруживается и блокируется на сетевом уровне до возникновения фактического использования.

Решение проблем с файерволом

Если ESET Security Ultimate не удается подключиться к сети, есть несколько способов узнать, обусловлены ли они работой файервола. Кроме того, с помощью файервола можно создать новые правила или исключения для решения проблем с подключением.

Для решения проблем с файерволом см. следующие темы:

- Устранение неполадок с доступом к сети
- Ведение журнала и создание правил и исключений на основе журнала
- Создание исключений на основе уведомлений файервола
- Расширенное ведение журналов для защиты сети
- Решение проблем со сканером сетевого трафика

Ведение журнала и создание правил и исключений на основе журнала

По умолчанию файервол ESET не вносит в журнал все блокируемые соединения. Если вы хотите видеть, что заблокировала функция защиты сети, откройте раздел Расширенные параметры > **Сервис** > **Диагностика** > **Расширенное ведение журналов** и включите параметр **Включить расширенное ведение журналов для защиты сети**. Если в журнале есть элемент, который файерволу не следует блокировать, можно создать правило или правило IDS, щелкнув этот элемент правой кнопкой мыши и выбрав **Не блокировать подобные события в будущем**. Обратите внимание, что журнал всех заблокированных соединений может содержать тысячи элементов, поэтому найти конкретный элемент может быть трудно. После решения проблемы ведение журнала можно выключить.

Для получения дополнительных сведений о журнале см. раздел Файлы журнала.

Используйте журнал, чтобы узнать, в каком порядке Защита сети блокировала те или иные соединения. Кроме того, правила, созданные на основе журнала, будут выполнять нужные вам действия.

Создание правил на основе журнала

В новой версии ESET Security Ultimate можно создавать правила на основе журнала. В главном меню последовательно выберите **Инструменты** > **Файлы журнала**. В раскрывающемся меню выберите пункт **Защита сети**, щелкните нужную запись журнала правой кнопкой мыши и в контекстном меню выберите пункт **Не блокировать подобные события в будущем**. Новое правило отобразится в окне уведомлений.

Чтобы можно было создавать правила на основе журнала, ESET Security Ultimate следует настроить следующим образом:

1. Установите минимальную степень детализации журнала **Диагностика**, последовательно выбрав Дополнительные настройки > **Служебные программы** > **Файлы журнала**.

2. Включите параметр **Уведомлять о входящих атаках, которые используют бреши в системе безопасности** в разделе Расширенные параметры > **Защита** > **Защита доступа к сети** > **Защита от сетевых атак** > **Расширенные параметры** > **Обнаружение вторжений**.

Создание исключений на основе уведомлений файервола

Когда файервол ESET обнаруживает вредоносную сетевую деятельность, отображается окно уведомления с описанием этого события. Уведомление содержит ссылку, перейдя по которой можно получить дополнительные сведения о событии и настроить правило для этого события (если нужно).

Если сетевое приложение или устройство не соблюдает сетевые стандарты надлежащим образом, возможно, начнут регулярно появляться уведомления IDS файервола. Благодаря этому файервол ESET не будет обнаруживать это приложение или устройство.

Расширенное ведение журналов для защиты сети

Эта функция предназначена для предоставления более комплексных файлов журнала для службы технической поддержки ESET. Используйте эту функцию только по запросу службы технической поддержки ESET, так как она может создать очень большой файл журнала и замедлить работу компьютера.

1. Откройте раздел Расширенные параметры > **Сервис** > **Диагностика** > **Расширенное ведение журналов** и включите параметр **Включить расширенное ведение журналов для защиты сети**.

2. Попробуйте воспроизвести текущую проблему.

3. Отключите функцию «Расширенное ведение журналов для защиты сети».

4. Файл журнала PCAP, созданный с помощью функции «Расширенное ведение журналов для защиты сети», можно найти в папке, где создаются дампы памяти для диагностики: *C:\ProgramData\ESET\ESET Security\Diagnostics*

Решение проблем со сканером сетевого трафика

Если возникают проблемы с браузером или почтовым клиентом, сначала следует определить, не является ли причиной этому сканер сетевого трафика. Для этого временно отключите сканер сетевого трафика в разделе Расширенные параметры > **Модуль обнаружения** > **Сканер сетевого трафика** (обязательно снова включите его после решения проблемы, иначе браузер и почтовый клиент останутся без защиты). Если после отключения неполадка исчезает, см. ниже список типичных проблем и способов их решения.

Проблемы с обновлением или безопасностью подключения

У приложения проблемы с обновлением или защищенностью канала связи.

- Если включен параметр SSL/TLS, попробуйте временно его отключить. Если помогло, значит, можно продолжать использовать SSL/TLS и выполнять обновления.
  Отключить SSL/TLS Запустите обновление еще раз. Должно появиться диалоговое окно с уведомлением о зашифрованном сетевом трафике. Приложение должно быть аналогичным тому, с которым возникли проблемы, а сертификат должен исходить из сервера, с которого выполняются обновления. Затем запомните действия для сертификата и нажмите кнопку «Пропустить». Если не отобразятся соответствующие диалоговые окна, переключитесь обратно в автоматический режим фильтрации. Проблема должна быть решена.

- Если приложение не является браузером или почтовым клиентом, его можно полностью исключить из защиты доступа в интернет (исключение браузера или почтового клиента оставило бы вас незащищенным). Любое приложение, в отношении которого выполнялась в прошлом фильтрация соединений, должно быть в списке, предоставляемом при добавлении исключений. Поэтому не должно возникнуть необходимости добавлять исключения вручную.

Проблема с доступом к устройству в сети

Если не удается использовать какие-либо функции устройства в сети (например, не удается открыть веб-страницу своей веб-камеры или воспроизвести видео на домашнем мультимедийном проигрывателе), добавьте IPv4- и IPv6-адреса такого устройства в список исключенных адресов.

Проблемы с определенным веб-сайтом

Исключить определенные веб-сайты из защиты доступа в Интернет можно с помощью

управления URL-адресами. Например, если не удается получить доступ к странице https://www.gmail.com/intl/en/mail/help/about.html, попробуйте добавить *gmail.com* в список исключенных адресов.

Ошибка «Все еще работают некоторые приложения, которые могут импортировать корневой сертификат»

При включении SSL/TLS программа ESET Security Ultimate выполняет фильтрацию протокола SSL так, что установленные программы доверяют ее действиям (происходит импорт сертификата в их хранилище сертификатов). Для импорта сертификата некоторым приложениям может потребоваться перезапуск. Например, для браузеров Firefox и Opera. Закройте эти приложения (для этого рекомендуется открыть диспетчер задач и удалить записи firefox.exe и opera.exe на вкладке «Процессы»), а затем нажмите кнопку «Повторить».

Ошибка: недоверенный издатель или недопустимая подпись

Скорее всего, это значит, что при вышеописанном импорте произошла ошибка. Сначала закройте все упомянутые приложения. Затем отключите параметр SSL/TLS и снова включите его. Будет выполнена повторная попытка импорта.

> См. статью базы знаний об управлении сканером сетевого трафика в Windows-продукте ESET для домашнего использования.

Сетевая угроза заблокирована

Такая ситуация может произойти, когда, например, приложение на компьютере пытается направить вредоносный трафик на другие устройство или сеть, используя брешь в системе безопасности, или при обнаружении попытки сканирования портов системы.

Тип угрозы и IP-адрес соответствующего устройства отображаются в уведомлении. Щелкните **Изменить способ обработки этой угрозы**, чтобы отобразились следующие опции.

Продолжить блокировать: обнаруженные угрозы блокируются. Чтобы больше не получать уведомления об угрозах этого типа с определенного удаленного адреса, выберите переключатель **Не уведомлять**, а затем щелкните **Продолжить блокировать**. При этом будет создано правило службы обнаружения вторжений (Intrusion Detection Service, IDS) со следующей конфигурацией: **Блокировать** — по умолчанию, **Уведомить** — нет, **Записать в журнал** — нет.

Разрешить: создается правило службы обнаружения вторжений (Intrusion Detection Service, IDS), разрешающее обнаруженную угрозу. Выберите одну из следующих опций, чтобы указать настройки правила, и щелкните **Разрешить**.

- **Уведомлять только тогда, когда эта угроза блокируется** — конфигурация правила: **Блокировать** — нет, **Уведомить** — нет, **Записать в журнал** — нет.

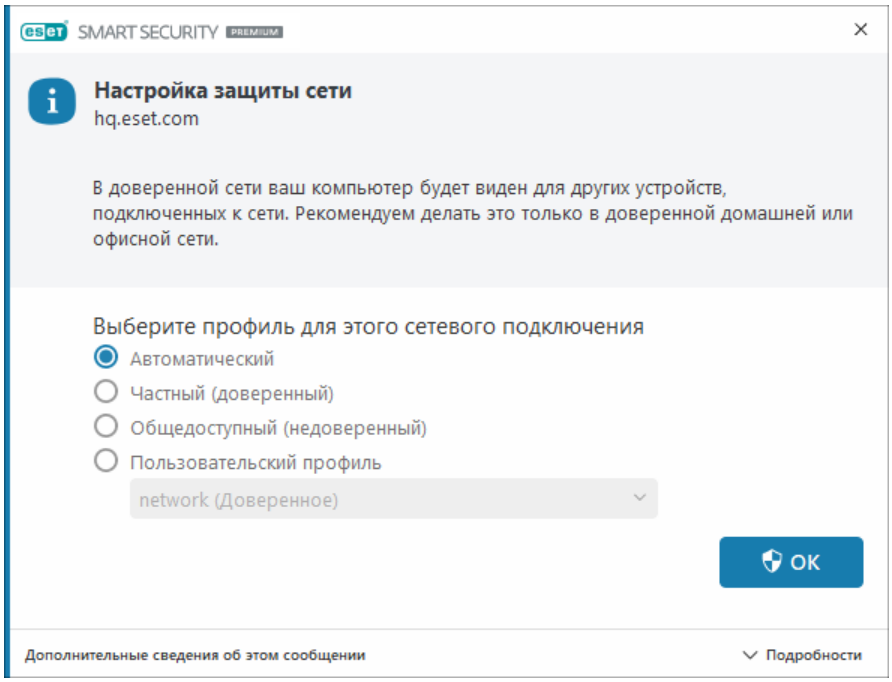
- **Уведомлять всегда, когда эта угроза появляется** — конфигурация правила: **Блокировать** — нет, **Уведомить** — по умолчанию, **Записать в журнал** — по умолчанию.

• **Не уведомлять** — конфигурация правила: **Блокировать** — нет, **Уведомить** — нет, **Записать в журнал** — нет.

Отображаемая в этом окне информация зависит от типа обнаруженной угрозы. Для получения дополнительных сведений об угрозах и других связанных терминах см. раздел о типах удаленных атак или типах обнаруженных угроз.
Сведения о том, как разрешить событие **Дублирующиеся IP-адреса в сети**, можно найти в статье базы знаний ESET.

Обнаружена новая сеть

По умолчанию ESET Security Ultimate использует параметры Windows при обнаружении новой сети. Чтобы при обнаружении новой сети отображалось диалоговое окно, установите для параметра Назначение профиля защиты сети значение **Запросить**. Конфигурация защиты сети отображается при каждом подключении вашего компьютера к новой сети.



Вы можете выбрать один из следующих профилей сетевых подключений.

Автоматический: ESET Security Ultimate автоматически выберет профиль согласно активаторам, настроенным для каждого профиля.

Конфиденциально — для доверенной сети (домашней или офисной сети). Ваш компьютер и общие файлы, хранящиеся на нем, видны для других пользователей сети, а также другим пользователям сети доступны системные ресурсы (доступ к общим файлам и принтерам включен, входящее подключение RPC включено, общий доступ к удаленному рабочему столу предоставлен). Этот параметр рекомендуется использовать при доступе к безопасной локальной сети. Этот профиль автоматически назначается сетевому подключению, если оно настроено как доменная или частная сеть в Windows.

Общедоступная — для недоверенных (общедоступных) сетей. Файлы и папки в вашей системе не являются общими для других пользователей в сети, и другие пользователи сети их не видят, а общий доступ к системным ресурсам отключен. Этот параметр рекомендуется

использовать при доступе к беспроводным сетям. Этот профиль автоматически назначается любому сетевому подключению, которое не настроено как доменная или частная сеть в Windows.

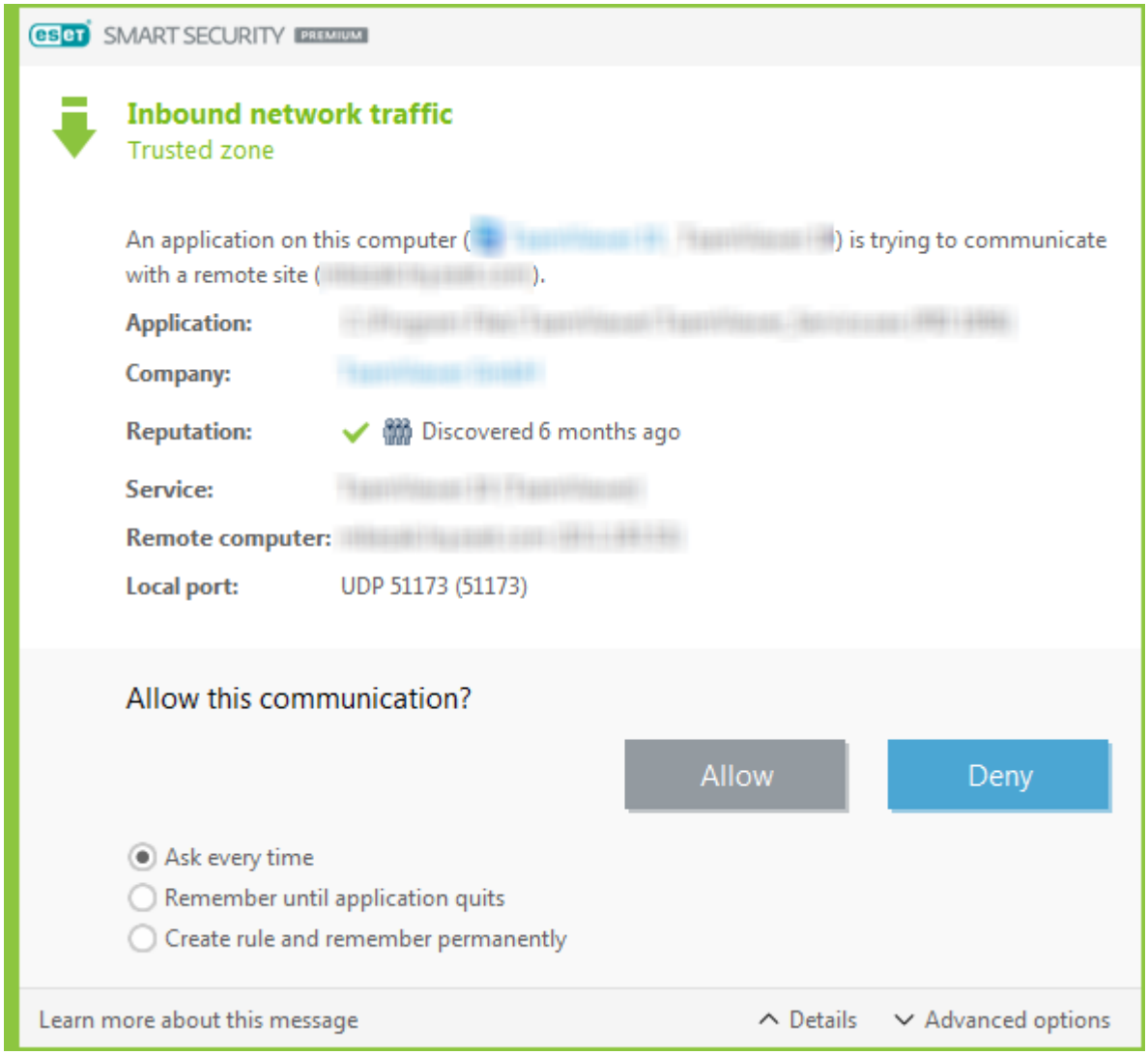
Пользовательский профиль: в раскрывающемся меню можно выбрать один из созданных вами профилей. Эта опция доступна только в том случае, если вы создали хотя бы один пользовательский профиль.

> Неправильная конфигурация сети может представлять угрозу безопасности вашего компьютера.

Установка соединения: обнаружение

Файервол обнаруживает каждое из вновь созданных сетевых соединений. Активный режим персонального файервола определяет, какие действия должны выполняться для нового правила. Если активирован **автоматический режим** или **режим на основе политики**, файервол выполнит предварительно заданные действия без вмешательства пользователя.

В **интерактивном режиме** выводится информационное окно с уведомлением об обнаружении нового сетевого соединения. В окне приводится дополнительная информация о соединении. Вы можете **Разрешить** или **Запретить** (заблокировать) соединение. Если соединения одного типа возникают регулярно, и их приходится разрешать вручную, рекомендуется создать для них правило. Выберите функцию **Создать правило и запомнить навсегда** и сохраните новое правило для файервола. Если персональный файервол обнаружит такое соединение в будущем, он применит это правило.



При создании новых правил разрешайте только защищенные соединения. Если разрешить все соединения, файервол не сможет обеспечивать защиту. Ниже перечислены наиболее важные параметры соединений.

Приложение — расположение исполняемого файла и идентификатора процесса. Не разрешайте соединения для неизвестных приложений и процессов.

Сведения о подписавшем: имя издателя приложения. Щелкните текст, чтобы показать сертификат безопасности для компании.

Репутация — уровень риска соединения. Соединениям назначен уровень риска: Хорошо (зеленый), Неизвестно (оранжевый) или Опасно (красный), с использованием ряда эвристических правил, которые исследуют характеристики каждого соединения, количество пользователей и время обнаружения. Эта информация собирается технологией ESET LiveGrid®.

Служба — имя службы, если приложение является службой Windows.

Удаленный компьютер — адрес удаленного устройства. Разрешать соединения только с доверенными и известными адресами.

Удаленный порт — порт связи. Связь через обычные порты (например, веб-трафик — номер порта 80 443) может быть разрешена в обычных условиях.

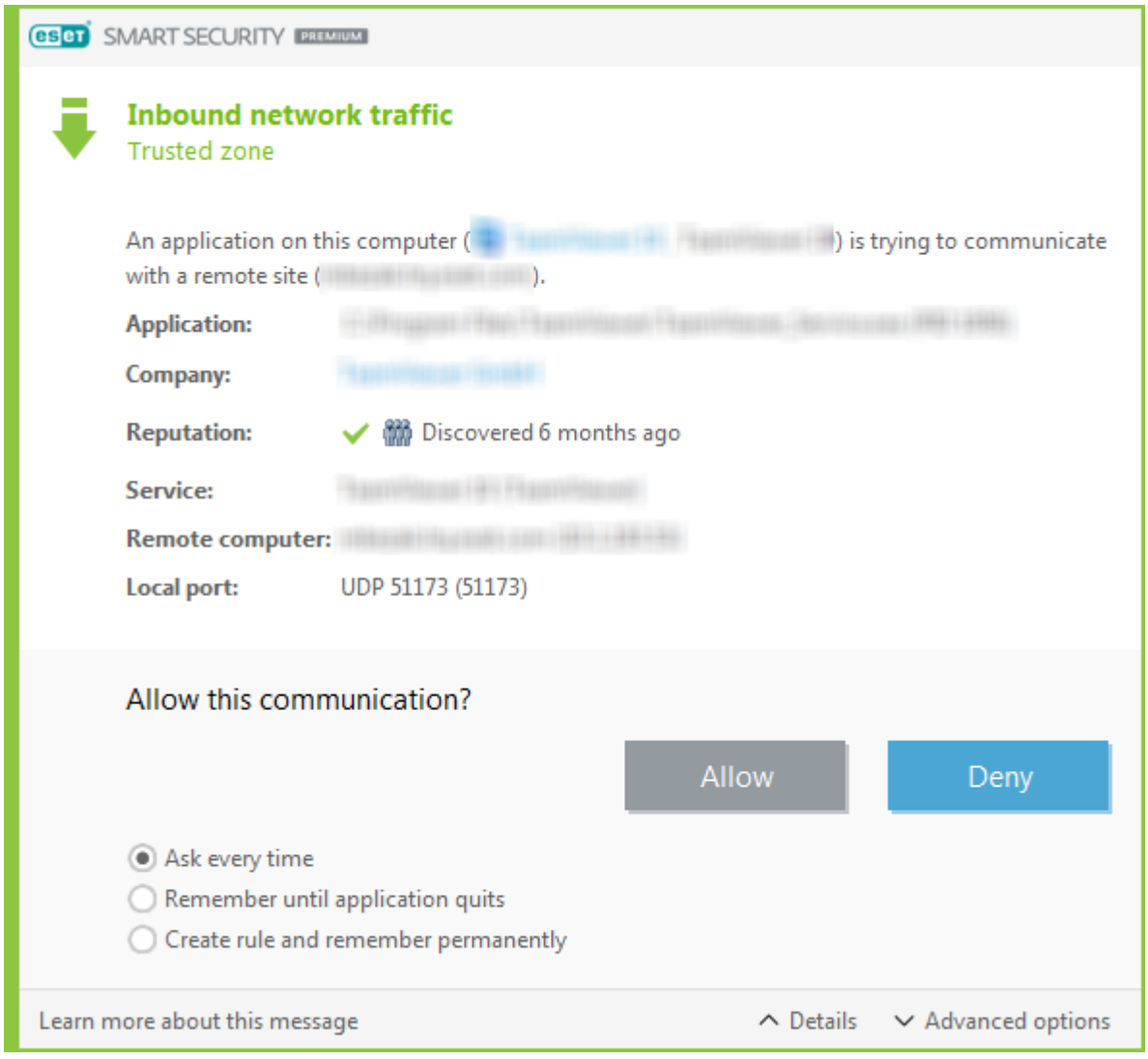
Компьютерные вирусы часто используют соединения с Интернетом или скрытые соединения, через которые происходит заражение других компьютеров. Если правила настроены правильно, файервол является эффективным средством противодействия разнообразным атакам с применением вредоносного кода.

Изменение приложения

Файервол обнаружил на компьютере пользователя изменение приложения, которое используется для исходящих соединений. Возможно, приложение просто обновилось до новой версии. С другой стороны, изменение может быть вызвано вредоносным приложением. Если пользователю неизвестна причина изменения приложения, рекомендуется прервать соединение и просканировать компьютер с помощью обновленной базы данных сигнатур вирусов.

Входящее доверенное соединение

Пример входящего соединения в пределах доверенной зоны:
Удаленный компьютер, находящийся в пределах доверенной зоны, пытается установить соединение с приложением, запущенном на локальном компьютере.



Приложение: приложение, с которым связывается удаленно устройство.

Путь приложения: расположение приложения.

Приложение Microsoft Store: имя приложения в магазине Microsoft Store.

Сведения о подписавшем: имя издателя приложения. Щелкните текст, чтобы показать сертификат безопасности для компании.

Репутация: репутация приложения, полученная с помощью технологии ESET LiveGrid®.

Служба: имя службы, запущенной в настоящий момент на компьютере.

Удаленный компьютер: удаленный компьютер, который пытается установить соединение с приложением на локальном компьютере.

Удаленный порт: порт, используемый для обмена данными.

Спрашивать каждый раз: если для правила по умолчанию установлено действие **Запрашивать**, при каждом запуске правила будет отображаться диалоговое окно.

Запомнить до закрытия приложения: ESET Security Ultimate запомнит выбранное действие до следующей перезагрузки.

Создать правило и запомнить навсегда: если выбрать этот вариант, прежде чем разрешить или запретить обмен данными, ESET Security Ultimate запомнит действие и будет использовать его, когда удаленный компьютер еще раз попытается установить соединение с этим приложением.

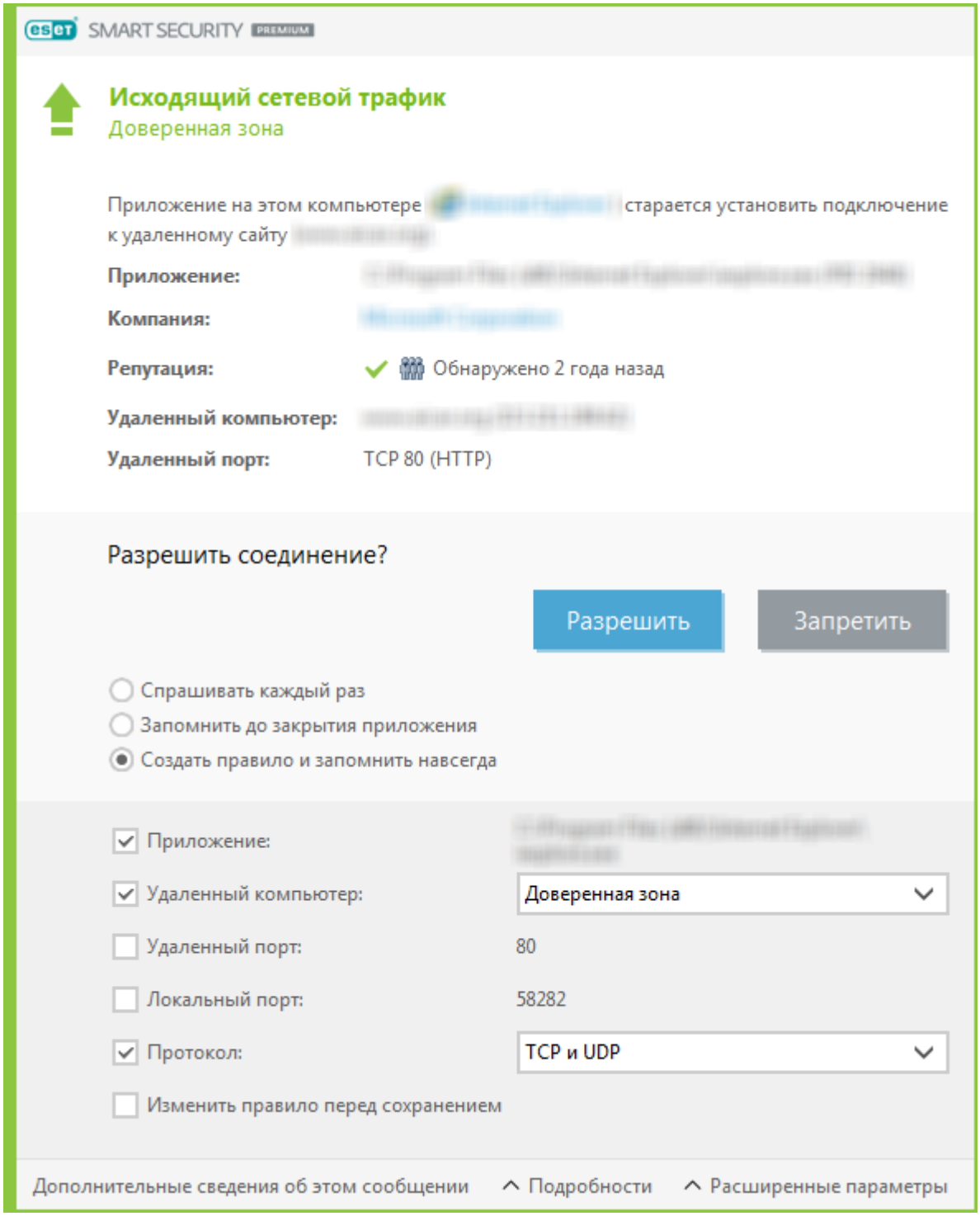
Разрешить: разрешить входящие соединения.

Запретить: запретить входящие соединения.

Изменить правило: позволяет настраивать свойства правила с помощью редактора правил файервола.

Исходящее доверенное соединение

Пример исходящего соединения в пределах доверенной зоны:
Приложение на локальном компьютере пытается установить соединение с другим компьютером в пределах локальной сети или сети в доверенной зоне.



Приложение: приложение, с которым связывается удаленно устройство.

Путь приложения: расположение приложения.

Приложение Microsoft Store: имя приложения в магазине Microsoft Store.

Сведения о подписавшем: имя издателя приложения. Щелкните текст, чтобы показать сертификат безопасности для компании.

Репутация: репутация приложения, полученная с помощью технологии ESET LiveGrid®.

Служба: имя службы, запущенной в настоящий момент на компьютере.

Удаленный компьютер: удаленный компьютер, который пытается установить соединение с приложением на локальном компьютере.

Удаленный порт: порт, используемый для обмена данными.

Спрашивать каждый раз: если для правила по умолчанию установлено действие **Запрашивать**, при каждом запуске правила будет отображаться диалоговое окно.

Запомнить до закрытия приложения: ESET Security Ultimate запомнит выбранное действие до следующей перезагрузки.

Создать правило и запомнить навсегда: если выбрать этот вариант, прежде чем разрешить или запретить обмен данными, ESET Security Ultimate запомнит действие и будет использовать его, когда удаленный компьютер еще раз попытается установить соединение с этим приложением.

Разрешить: разрешить входящие соединения.

Запретить: запретить входящие соединения.

Изменить правило: позволяет настраивать свойства правила с помощью редактора правил файервола.

Входящее соединение

Пример входящего интернет-соединения:
Удаленный компьютер пытается установить соединение с приложением, запущенным на локальном компьютере.

Приложение: приложение, с которым связывается удаленно устройство.

Путь приложения: расположение приложения.

Приложение Microsoft Store: имя приложения в магазине Microsoft Store.

Сведения о подписавшем: имя издателя приложения. Щелкните текст, чтобы показать сертификат безопасности для компании.

Репутация: репутация приложения, полученная с помощью технологии ESET LiveGrid®.

Служба: имя службы, запущенной в настоящий момент на компьютере.

Удаленный компьютер: удаленный компьютер, который пытается установить соединение с приложением на локальном компьютере.

Удаленный порт: порт, используемый для обмена данными.

Спрашивать каждый раз: если для правила по умолчанию установлено действие **Запрашивать**, при каждом запуске правила будет отображаться диалоговое окно.

Запомнить до закрытия приложения: ESET Security Ultimate запомнит выбранное действие до следующей перезагрузки.

Создать правило и запомнить навсегда: если выбрать этот вариант, прежде чем разрешить или запретить обмен данными, ESET Security Ultimate запомнит действие и будет использовать его, когда удаленный компьютер еще раз попытается установить соединение с этим приложением.

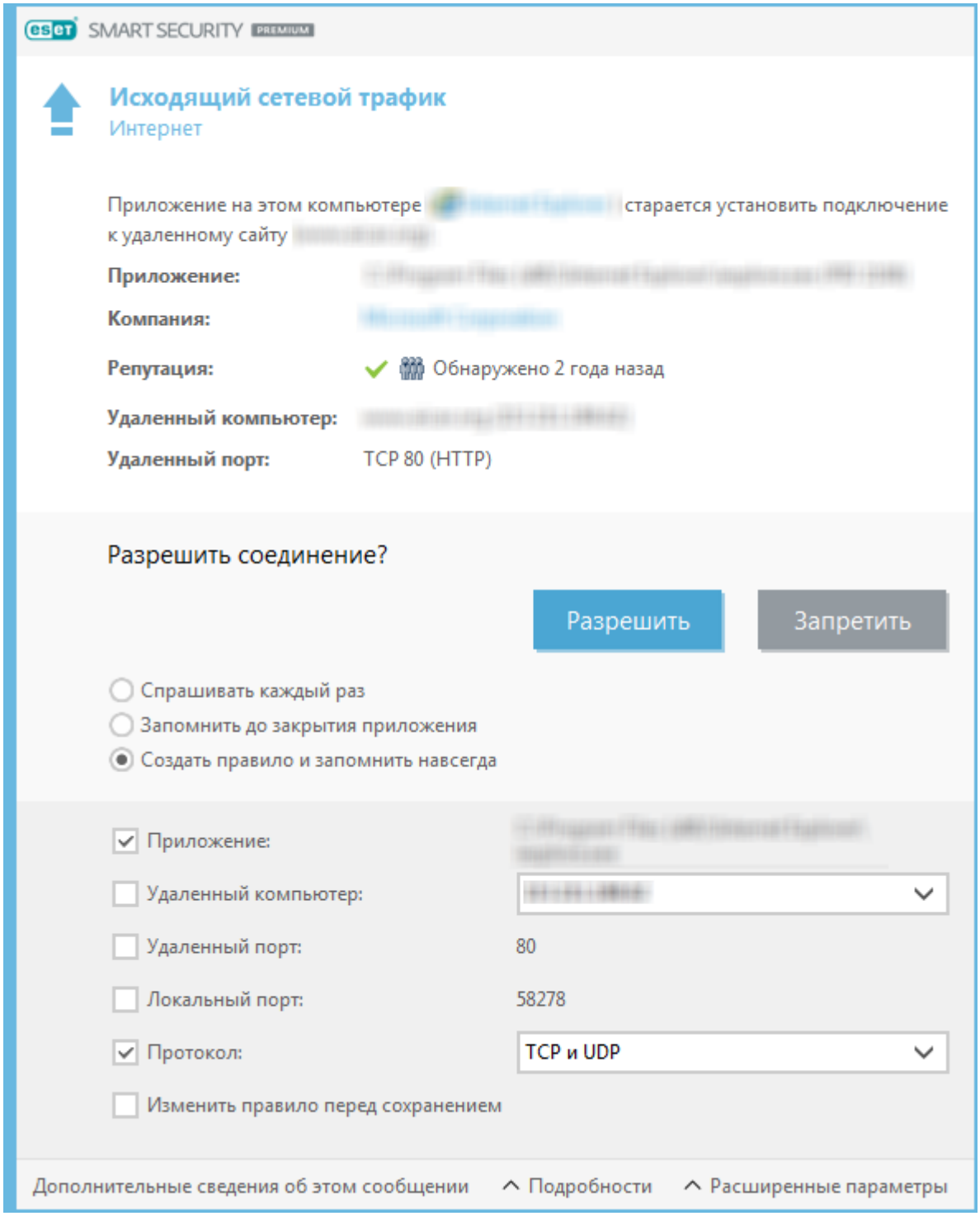
Разрешить: разрешить входящие соединения.

Запретить: запретить входящие соединения.

Изменить правило: позволяет настраивать свойства правила с помощью редактора правил файервола.

Исходящее соединение

Пример исходящего интернет-соединения:
Приложение на локальном компьютере пытается установить интернет-соединение.



Приложение: приложение, с которым связывается удаленно устройство.

Путь приложения: расположение приложения.

Приложение Microsoft Store: имя приложения в магазине Microsoft Store.

Сведения о подписавшем: имя издателя приложения. Щелкните текст, чтобы показать сертификат безопасности для компании.

Репутация: репутация приложения, полученная с помощью технологии ESET LiveGrid®.

Служба: имя службы, запущенной в настоящий момент на компьютере.

Удаленный компьютер: удаленный компьютер, который пытается установить соединение с приложением на локальном компьютере.

Удаленный порт: порт, используемый для обмена данными.

Спрашивать каждый раз: если для правила по умолчанию установлено действие **Запрашивать**, при каждом запуске правила будет отображаться диалоговое окно.

Запомнить до закрытия приложения: ESET Security Ultimate запомнит выбранное действие до следующей перезагрузки.

Создать правило и запомнить навсегда: если выбрать этот вариант, прежде чем разрешить или запретить обмен данными, ESET Security Ultimate запомнит действие и будет использовать его, когда удаленный компьютер еще раз попытается установить соединение с этим приложением.

Разрешить: разрешить входящие соединения.

Запретить: запретить входящие соединения.

Изменить правило: позволяет настраивать свойства правила с помощью редактора правил файервола.

Настройка отображения подключений

Щелкните подключение правой кнопкой мыши, чтобы просмотреть дополнительные параметры, среди которых есть следующие.

Определять имена хостов: все сетевые адреса, если это возможно, отображаются в формате DNS, а не в числовом формате IP-адресов.

Показывать только соединения по TCP: в списке отображаются только подключения по протоколу TCP.

Показывать ожидание соединения: установите этот флажок для отображения только тех подключений, по которым в настоящий момент не происходит обмена данными, но для которых система уже открыла порт и ожидает подключения.

Показывать внутренние соединения: установите этот флажок, чтобы отобразить только те соединения, в которых удаленной стороной является локальный компьютер (так называемые localhost).

Обновить скорость: выберите периодичность обновления активных подключений.

Обновить сейчас: перезагрузка окна **«Сетевые подключения»**.

Средства безопасности

Откройте главное окно программы > **Настройка** > **Средства безопасности** для настройки следующих модулей.

Защита банковских операций и браузера: добавляет дополнительный уровень защиты браузера, предназначенный для защиты ваших финансовых данных при финансовых операциях в Интернете. Включите функцию **Защита всех браузеров** в расширенных параметрах защиты банковских операций и браузера, чтобы все поддерживаемые веб-браузеры запускались в безопасном режиме.

Конфиденциальность и безопасность браузера: обеспечение конфиденциальности и безопасности ваших действий в Интернете без оставления цифрового следа.

Антивор: включите модуль Антивор, чтобы защитить компьютер в случае его потери или кражи.

Secure Data: если включен модуль Secure Data, вы можете шифровать свои данные, чтобы не допустить ненадлежащего использования конфиденциальной информации.

Password Manager: Password Manager защищает и хранит ваши пароли и личные данные.

VPN – Защищайте свои данные и избегайте нежелательного отслеживания с помощью анонимного IP-адреса.

Identity Protection: защищает вашу личную, кредитную и финансовую информацию.

Защита банковских операций и браузера

Защита банковских операций и браузера — это дополнительный уровень безопасности, разработанный для защиты ваших финансовых данных при осуществлении финансовых операций в Интернете.

По умолчанию все поддерживаемые веб-браузеры будут запускаться в защищенном режиме. Это позволяет просматривать веб-сайты, использовать интернет-банкинг и совершать онлайн-покупки и транзакции автоматически в одном защищенном браузере.

Для правильной работы защиты банковских операций и браузера должна быть включена (включена по умолчанию) система репутации ESET LiveGrid®.

Сведения о настройке защищенного браузера см. в разделе Расширенные параметры защиты банковских операций и браузера. Если параметр **Защита всех браузеров** отключен, доступ к защищенному браузеру можно получить в главном окне программы > **Обзор** > **Защита банковских операций и браузера**, или щелкнув значок **Защита банковских операций и браузера** на рабочем столе. Браузер, заданный в Windows как используемый по умолчанию, запустится в безопасном режиме.

Для защиты браузера необходимо использовать шифрованный обмен данными по протоколу HTTPS. Защиту банковских операций и браузера поддерживают следующие браузеры:

- Internet Explorer 8.0.0.0+
- Microsoft Edge 83.0.0.0+
- Google Chrome 64.0.0.0+

- Firefox 24.0.0.0+

На устройствах с процессорами ARM поддерживаются только Firefox и Microsoft Edge.

Дополнительные сведения о функции «Защита банковских операций и браузера» см. в статьях базы знаний ESET, доступных на английском и некоторых других языках.

- Как использовать защиту банковских операций и браузера ESET?
- Приостановка или отключение защиты банковских операций и браузера в Windows-продуктах ESET для домашнего использования
- Защита банковских операций и браузера ESET — распространенные ошибки
- Глоссарий ESET | Защита банковских операций и браузера

Уведомление в браузере

Сведения о текущем состоянии защищенного браузера отображаются с помощью уведомлений в браузере и цвета рамки браузера.

Уведомления в браузере отображаются на вкладке с правой стороны.

Чтобы развернуть уведомление в браузере, щелкните значок ESET. Чтобы свернуть уведомление, щелкните его текст. Чтобы скрыть уведомление и зеленую рамку браузера, щелкните значок «Закрыть».

Скрыть можно только информационное уведомление и зеленую рамку браузера.

Уведомления в браузере

Тип уведомления	Состояние
Информационное уведомление и зеленая рамка браузера	Обеспечивается максимальная защита, и уведомление в браузере свернуто по умолчанию. Разверните уведомление в браузере и щелкните **Настройки**, чтобы открыть раздел Средства безопасности.
Предупреждение и оранжевая рамка браузера	Некритическая проблема защищенного браузера требует вашего внимания. Для получения дополнительных сведений о проблеме или ее решении следуйте инструкциям в уведомлении в браузере.

Тип уведомления	Состояние
Оповещение по безопасности и красная рамка браузера	Браузер не защищен функцией «Защита банковских операций и браузера ESET». Перезапустите браузер, чтобы активировать защиту. Чтобы разрешить конфликт с файлами, загружаемыми в браузере, откройте раздел Файлы журнала > **«Защита банковских операций и браузера»** и убедитесь, что во время следующего запуска браузера занесенные в журнал файлы загружаться не будут. Если проблема повторится, обратитесь в службу технической поддержки ESET, следуя инструкциям в статье нашей базы знаний.

Конфиденциальность и безопасность браузера

Функцию «Конфиденциальность и безопасность браузера» можно включить с помощью специального расширения, доступного в поддерживаемых браузерах (только Google Chrome, Mozilla Firefox и Microsoft Edge).

Чтобы установить и включить расширение, выполните следующие действия.

1. Убедитесь, что вы используете последнюю версию ESET Security Ultimate, и перезапустите компьютер после обновления.
2. Откройте браузер.
3. Расширение будет установлено в браузере.
4. Включите расширение, и в браузере отобразится страница со сведениями о расширении.

Главное меню браузерного расширения «Конфиденциальность и безопасность браузера» разделено на следующие разделы:

Обзор

Защищенный поиск

Щелкните значок переключателя рядом с элементом **Сканировать результаты поиска**, чтобы включить эту функцию и видеть, какие результаты поиска безопасны. Функция защищенного поиска оценивает отображаемые адреса ссылок, но это не означает обязательно, что веб-сайт не содержит вредоносных программ. Затем наш модуль обнаружения находит вредоносные программы на веб-сайте.

Очистка браузера

Удалите данные просмотра веб-страниц или настройте регулярную очистку. Вы можете указать веб-сайты, на которых следует принимать файлы cookie и не выполнять выход даже после очистки браузера, **добавив их в список**.

- **Одноразовая очистка**: выберите в раскрывающемся меню период времени и тип данных,

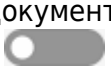
которые нужно удалить. С помощью опций можно выбрать все данные, личные данные, а также сделать произвольный выбор.

• **Регулярная очистка**: щелкните значок переключателя  рядом с элементом **Регулярная очистка**, чтобы включить эту функцию. Выберите в раскрывающемся меню период времени и тип данных, которые нужно удалять регулярно. С помощью опций можно выбрать все данные, личные данные, а также сделать произвольный выбор.

Опция **Пользовательские данные** содержит следующие категории:

- журнал браузера;
- История загрузок
- Файлы cookie и данные веб-сайтов
- Кэшированные изображения и файлы
- Пароли и данные для входа
- Данные автозаполнения форм

Очистка метаданных

Функция очистки метаданных контролирует конфиденциальные данные, которые потенциально могут быть раскрыты через метаданные EXIF, присутствующие в файлах мультимедиа, документах и других поддерживаемых форматах файлов. Щелкните значок переключателя  рядом с элементом **Очищать метаданные при каждой выгрузке изображений**, чтобы включить удаление метаданных.

> Для правильной работы функции **очистки метаданных** необходимо перезапустить браузер.

Щелкните значок переключателя  рядом с элементом **Отображение уведомлений в браузере**, чтобы включить отображение уведомлений после очистки метаданных.

Проверка настроек для веб-сайтов

Получайте доступ к разрешениям веб-сайтов и управляйте ими, чтобы контролировать, какую информацию веб-сайты могут использовать.

- **Уведомления**: проверьте, на каких веб-сайтах вы хотите **разрешать/блокировать** уведомления или хотите, чтобы расширение браузера **каждый раз спрашивало вас**.

Расширенные параметры

Очистка браузера

Дополнительные параметры файлов cookie

Список веб-сайтов, на которых следует принимать файлы cookie и не выполнять выход даже после очистки браузера. Введите URL-адрес в текстовое поле и щелкните **Добавить**. Вы

можете удалить его из списка в любой момент, щелкнув значок минуса  рядом с конкретным веб-сайтом.

Внизу страницы находится список рекомендуемых доменов, которые открыты в данный момент в браузере. Если вы не видите конкретный веб-сайт, щелкните **Обновить список** и добавьте его в список принимаемых файлов cookie, щелкнув значок плюса  .

Проверка настроек для веб-сайтов

Получайте доступ к разрешениям веб-сайтов и управляйте ими, чтобы контролировать, какую информацию веб-сайты могут использовать.

- **Уведомления**: проверьте, на каких веб-сайтах вы хотите **разрешать/блокировать** уведомления или хотите, чтобы расширение браузера **каждый раз спрашивало вас**.

Внешний вид

Настройте цветовую схему интерфейса в соответствии со своими предпочтениями. Вы можете выбрать предпочтительную цветовую схему, установив флажок **Светлая** или **Темная**.

Антивор

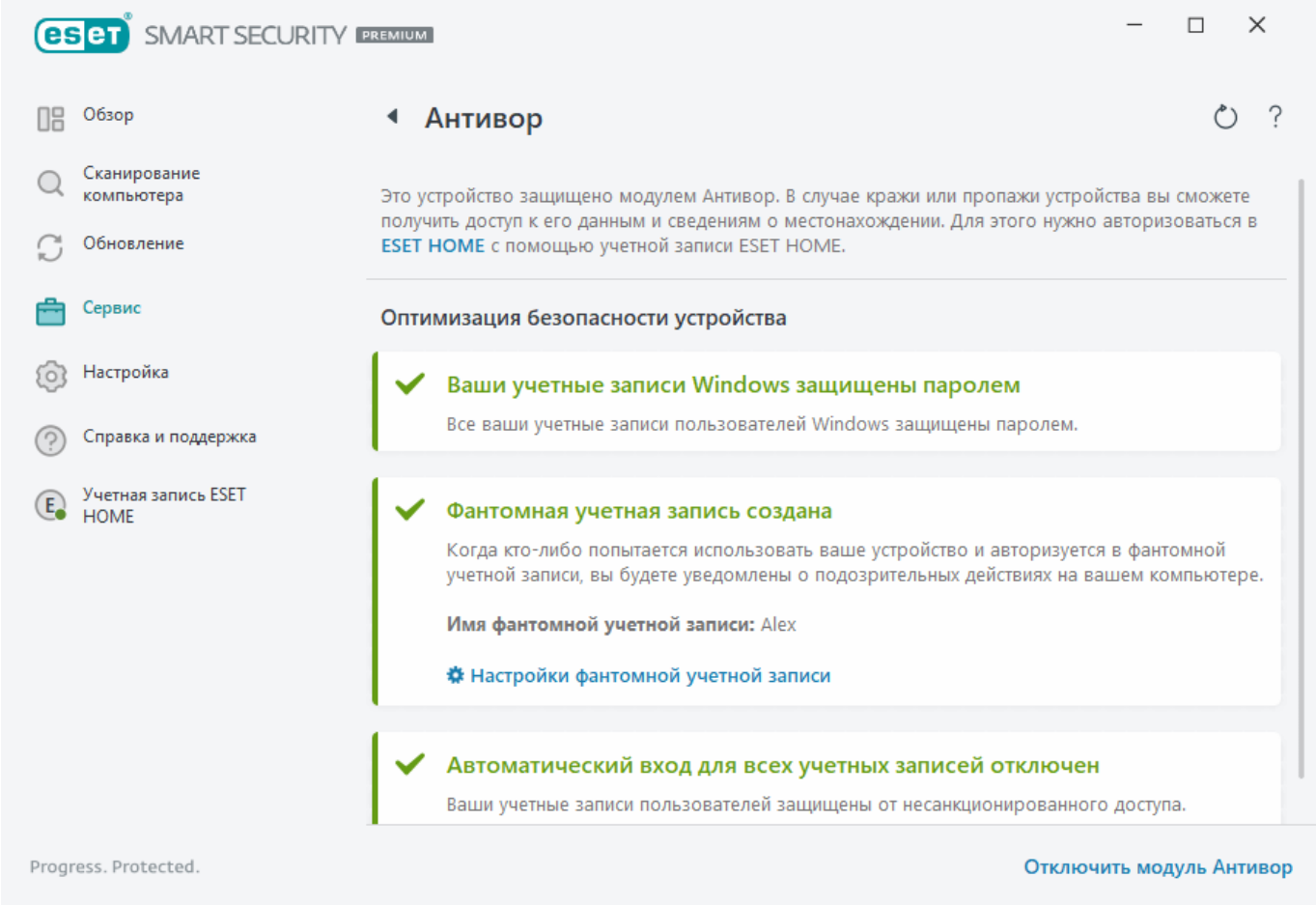
Персональные устройства постоянно подвергаются риску потери или кражи в наших повседневных поездках из дома на работу или в другие общественные места. Антивор — это функция, которая расширяет безопасность на уровне пользователя в случае потери или кражи устройства. Антивор позволяет мониторить использование устройства и отслеживать ваше потерянное устройство с помощью локализации по IP-адресу в ESET HOME, помогая восстановить устройство и защитить личные данные.

Благодаря использованию в модуле Антивор таких современных технологий, как определение географического местоположения по IP-адресу, захват изображений с помощью веб-камеры, защита учетной записи пользователя и мониторинг устройства, пользователи и правоохранительные органы имеют возможность находить потерянные или украденные компьютеры или устройства. В ESET HOME вы можете увидеть, какие действия выполняются на вашем компьютере или устройстве.

Дополнительные сведения о Антивор в ESET HOME см. в интерактивной справке ESET HOME.

Антивор может работать неправильно на компьютерах в доменах из-за ограничений в управлении учетными записями пользователей.

После включения Антивор вы сможете оптимизировать безопасность вашего устройства в главном окне программы > **Параметры** > **Средства безопасности** > **Антивор**.



Опции оптимизации

Фантомная учетная запись не создана

Создание фантомной учетной записи увеличивает вероятность обнаружения потерянного или украденного устройства. Если отметить устройство как пропавшее, Антивор заблокирует доступ к вашим активным пользовательским учетным записям, чтобы защитить ваши конфиденциальные данные. Любому, кто попытается использовать устройство, будет разрешено использовать только фантомную учетную запись. Фантомная учетная запись — это форма гостевой учетной записи с ограниченными разрешениями. Она будет использоваться в качестве системной учетной записи по умолчанию до тех пор, пока ваше устройство не будет помечено как восстановленное, что предотвратит вход в другие учетные записи пользователей или доступ к данным пользователя.

Каждый раз, когда кто-то входит в фантомную учетную запись, когда ваш компьютер находится в нормальном состоянии, вам будет отправлено уведомление по электронной почте с информацией о подозрительной активности на вашем компьютере. Получив уведомление по электронной почте, вы можете решить, желаете ли вы пометить компьютер как пропавший.

Чтобы создать фантомную учетную запись, нажмите кнопку **Создать фантомную учетную запись**, введите **имя фантомной учетной записи** в текстовом поле и нажмите кнопку **Создать**.

Если у вас есть созданная фантомная учетная запись, нажмите **Настройки фантомной учетной записи**, чтобы переименовать или удалить учетную запись.

Защита учетных записей Windows паролем

Ваша пользовательская учетная запись не защищена паролем. Вы получите это предупреждение об оптимизации, если по крайней мере одна учетная запись пользователя не защищена паролем. Создание пароля для всех пользователей (кроме **фантомной учетной записи**) на компьютере решит эту проблему.

Чтобы создать пароль для учетной записи пользователя, щелкните **Управление учетными записями Windows** и измените пароль или следуйте инструкциям ниже:

1. Нажмите сочетание клавиш CTRL+Alt+Delete на клавиатуре.
2. Щелкните **Изменить пароль**.
3. Оставьте поле **Старый пароль** пустым.
4. Введите пароль в поля **Новый пароль** и **Подтвердить пароль**, а затем нажмите кнопку **Ввод**.

Автоматический вход для учетных записей Windows

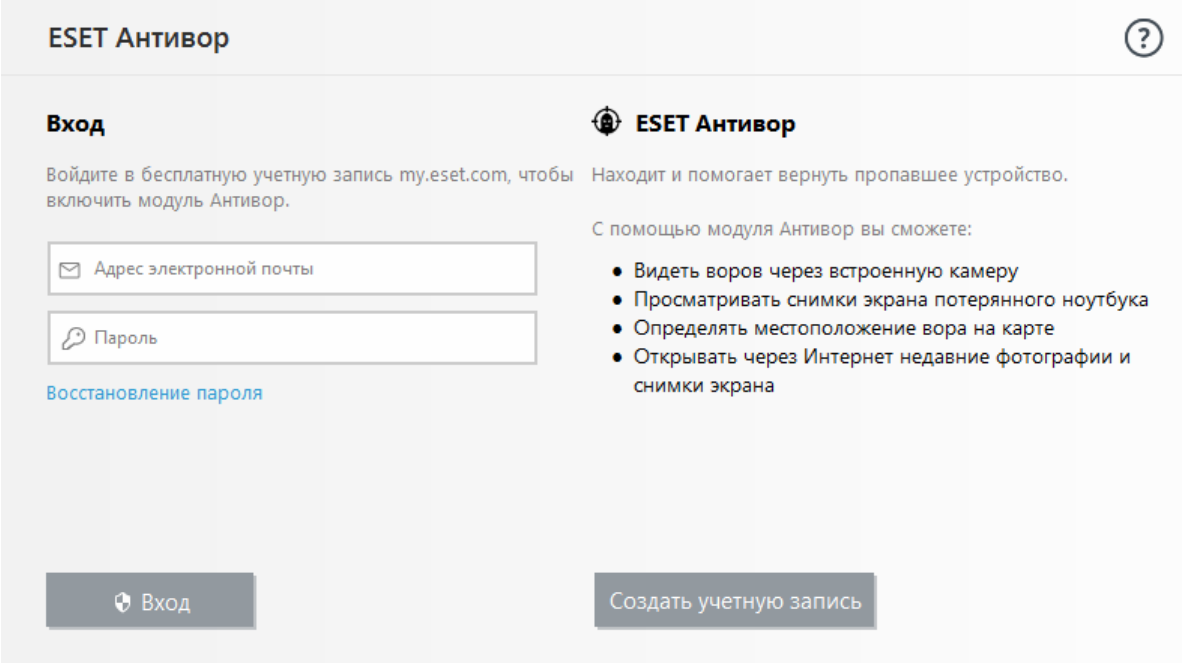
В вашей учетной записи пользователя включен автоматический вход в систему, поэтому ваша учетная запись не защищена от несанкционированного доступа. Вы получите это предупреждение об оптимизации, если по крайней мере для одной учетной записи пользователя включен автоматический вход в систему. Щелкните **Отключить автоматический вход**, чтобы решить эту проблему оптимизации.

Автоматический вход для фантомной учетной записи

На вашем устройстве включен автоматический вход в **фантомную учетную запись**. Мы не рекомендуем использовать автоматический вход в систему, когда устройство находится в нормальном состоянии, так как это может вызвать проблемы с доступом к вашей реальной учетной записи пользователя или привести к отправке ложных тревог о состоянии «Потерян» вашего компьютера. Нажмите **Отключить автоматический вход**, чтобы решить эту проблему оптимизации.

Вход в учетную ESET HOME запись.

Чтобы включить или отключить Антивор и получить доступ к сведениям о расположении устройства и информации о нем в ESET HOME, войдите в свою учетную запись ESET HOME.



Существует несколько способов авторизации в учетной записи ESET HOME.

• **Использовать адрес электронной почты и пароль ESET HOME**: введите **адрес электронной почты** и **пароль**, которые вы использовали для создания учетной записи ESET HOME, а затем щелкните **Авторизоваться**.

• **Использовать учетную запись Google/AppleID**: щелкните **Продолжить с Google** или **Продолжить с Apple** и авторизуйтесь в соответствующей учетной записи. После успешной авторизации вы будете перенаправлены на веб-страницу подтверждения ESET HOME. Чтобы продолжить, вернитесь в окно продукта ESET. Дополнительные сведения об авторизации с помощью учетной записи Google/AppleID см. в онлайн-справке ESET HOME.

• **Просканировать QR-код**: щелкните **Просканируйте QR-код**, чтобы отобразить QR-код. Откройте мобильное приложение ESET HOME и просканируйте QR-код или наведите камеру устройства на QR-код. Дополнительные сведения см. в онлайн-справке ESET HOME.

⚠ Не удалось войти — распространенные ошибки.

ℹ Если у вас нет учетной записи ESET HOME, щелкните **Создать учетную запись**, чтобы зарегистрироваться, или ознакомьтесь с инструкциями в онлайн-справке ESET HOME. Если вы забыли пароль, щелкните **Я не помню пароль** и следуйте инструкциям на экране или ознакомьтесь с инструкциями в онлайн-справке ESET HOME.

ℹ Приложение Антивор не поддерживает Microsoft Windows Home Server.

Задать имя устройства

В поле **Имя устройства** указывается имя компьютера (устройства), которое будет отображаться в качестве идентификатора во всех службах ESET HOME. По умолчанию используется имя вашего компьютера. Введите имя устройства или используйте имя по умолчанию и щелкните **Продолжить**.

Антивор включено или отключено

Это окно содержит подтверждение включения или отключения Антивор:

- Включено — теперь ваше устройство защищено Антивор, и вы можете удаленно управлять его безопасностью на портале ESET HOME, используя свою учетную запись.
- Отключено — Антивор отключено на этом устройстве и все данные, относящиеся к <%ESET_ANTTHEFT%> для этого устройства, удалены с портала ESET HOME.

Ошибка добавления устройства

При активации Антивор произошла ошибка.

Наиболее распространенные сценарии:

- Ошибка входа в ESET HOME
- Отсутствие подключения к Интернету (или «В данный момент Интернет не работает»)

Если вам не удается решить эту проблему, обратитесь в службу технической поддержки ESET.

Secure Data

Secure Data — это компонент решения ESET Security Ultimate, который позволяет шифровать данные на компьютере и съемных носителях для защиты ваших личных данных и предотвращения ненадлежащего использования. Для получения дополнительных сведений см. вопросы и ответы о ESET Secure Data.

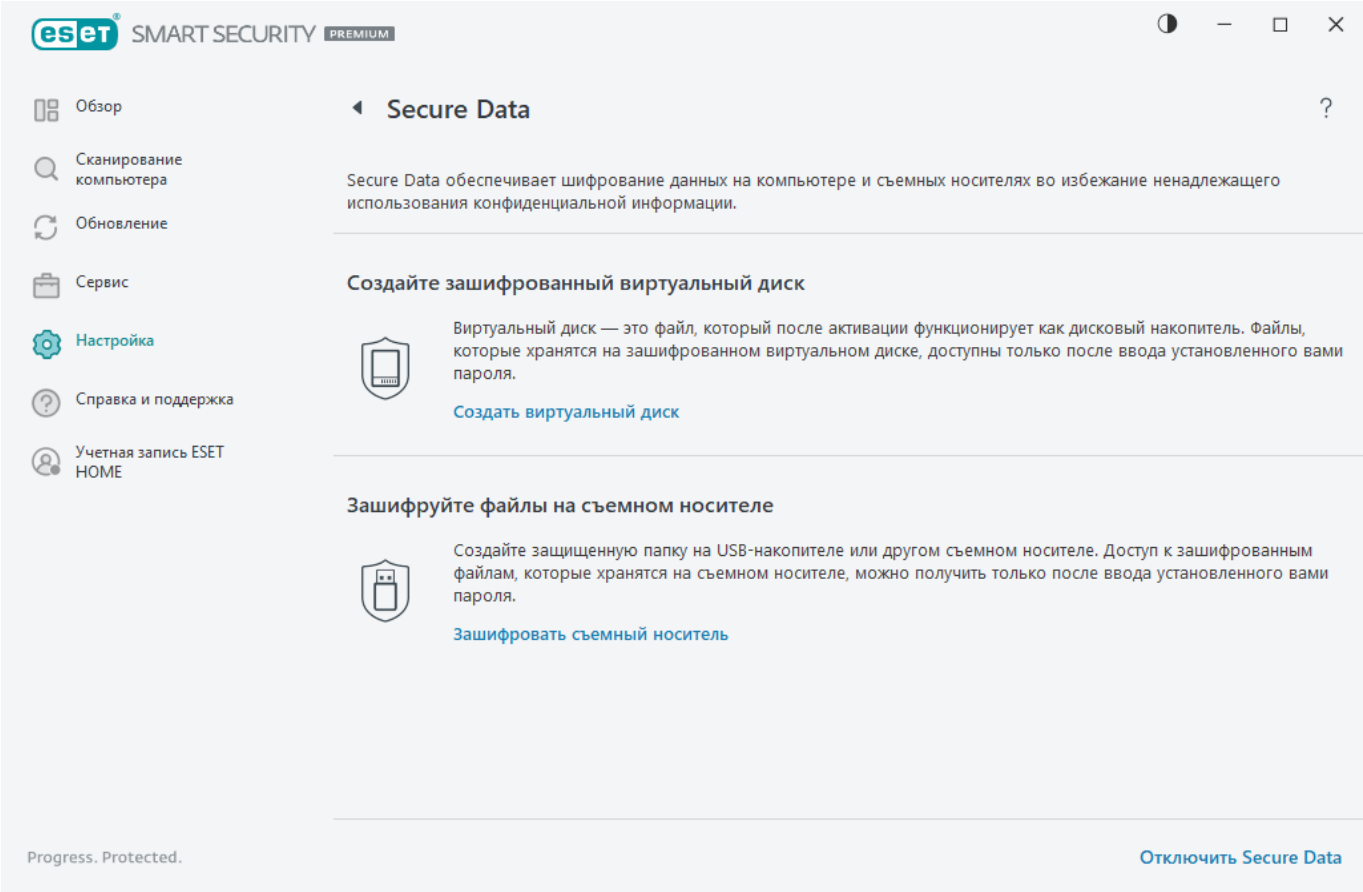
Чтобы включить Secure Data, выберите один из следующих вариантов.

- В главном окне программы в разделе **Обзор** щелкните **НАСТРОИТЬ** рядом с элементом **Secure Data**.
- В главном окне программы в разделе **Настройка** > **Средства безопасности** включите переключатель **Secure Data**.

> Вы не можете установить ESET Endpoint Encryption на тот же компьютер, на котором уже установлено решение Secure Data.

Если компонент Secure Data включен, в главном окне программы щелкните **Настройка** > **Средства безопасности** > **Secure Data** и выберите один из следующих вариантов шифрования:

- Создайте зашифрованный виртуальный диск
- Зашифруйте файлы на съемном носителе



Создайте зашифрованный виртуальный диск

С помощью Secure Data можно создавать зашифрованные виртуальные диски. Количество дисков, которые можно создать, ограничено только местом на жестком диске. Чтобы создать зашифрованный виртуальный диск, выполните следующие действия.

1. В главном окне программы щелкните **Параметры** > **Средства безопасности** > **Secure Data** > **Создать виртуальный диск**.

2. Щелкните **Обзор**, чтобы выбрать расположение, в котором необходимо сохранить виртуальный диск.

3. Введите имя виртуального диска и щелкните **Сохранить**.

4. Используйте раскрывающееся меню **Максимальная емкость**, чтобы задать размер виртуального диска, а затем щелкните **Продолжить**.

5. Задайте пароль для виртуального диска. Если вы не хотите, чтобы виртуальный диск автоматически расшифровывался при входе в учетную запись Windows, снимите флажок **Расшифровывать автоматически для этой учетной записи Windows**. Щелкните **Продолжить**.

6. Щелкните **Готово**. Ваш зашифрованный виртуальный диск создан и готов к использованию. Он будет отображаться как локальный диск в приложении **Этот компьютер**.

Чтобы получить доступ к зашифрованному диску после перезапуска компьютера, найдите созданный вами файл зашифрованного диска (тип файла .eed) и дважды щелкните его. Если появится запрос, введите пароль, который вы задали при создании зашифрованного диска. Диск будет подключен и будет отображаться как локальный диск в разделе «Этот компьютер». После того как зашифрованный диск будет подключен как локальный диск, этот локальный диск и его расшифрованное содержимое будут доступны другим пользователям на вашем компьютере до тех пор, пока вы не выйдете из системы или не перезапустите компьютер.

> **Могу ли я удалить виртуальный диск?**
> Да. Чтобы удалить зашифрованный виртуальный диск, следуйте инструкциям в часто задаваемых вопросах о ESET Secure Data.

Зашифруйте файлы на съемном носителе

С помощью Secure Data можно создавать зашифрованные папки на съемных носителях. Чтобы зашифровать файлы на съемном носителе, выполните указанные ниже действия.

1. Вставьте съемный носитель (USB-устройство флэш-памяти, жесткий диск с интерфейсом USB) в компьютер.

2. В главном окне программы щелкните **Параметры** > **Средства безопасности** > **Secure Data** > **Зашифровать съемный носитель**.

3. Выберите подключенный съемный носитель, который нужно зашифровать, и щелкните **Продолжить**.
Щелкните **Обновить**, чтобы обновить список дисков, доступных для шифрования. Зашифрованные и неподдерживаемые диски в списке не отображаются.
Если нужна возможность расшифровать защищенную папку, которая записана на выбранный съемный носитель, на любом устройстве с Windows без необходимости устанавливать ESET Security Ultimate, выберите **Расшифровывать папку на любом устройстве с Windows**.

4. Задайте пароль для зашифрованного каталога. Если вы не хотите, чтобы виртуальный диск автоматически расшифровывался при входе в учетную запись Windows, снимите флажок **Расшифровывать автоматически для этой учетной записи Windows**. Щелкните **Продолжить**.

5. Ваш съемный носитель защищен, и зашифрованный каталог на нем готов к использованию.

С этого момента, если вы подключите ваш съемный носитель к компьютеру, на котором не установлен продукт Secure Data, зашифрованная папка отображаться не будет. Если подключить съемный носитель к компьютеру, на котором установлен продукт Secure Data, отобразится предложение ввести пароль для расшифровки съемного носителя. Если пароль не ввести, зашифрованная папка будет отображаться, но останется недоступной.

Password Manager

Средство Password Manager входит в пакет ESET Security Ultimate.

Password Manager защищает и хранит ваши пароли и персональные данные. Это средство содержит функцию автоматического заполнения форм, которое помогает сэкономить время, точно заполняя веб-формы.

Дополнительные сведения см. в справке о решении Password Manager в Интернете:

- Password Manager установка
- Приступите к работе с Password Manager
- Управление хранилищами Password Manager в ESET HOME

VPN

ESET VPN входит в пакет ESET Security Ultimate. VPN дает вам возможность хранить свои данные в безопасности, избегать нежелательного отслеживания и повысить свою конфиденциальность в Интернете с помощью дополнительной защиты, которую обеспечивает анонимный IP-адрес.

Чтобы начать использовать VPN, щелкните **Загрузить и установить VPN**.

Дополнительные сведения см. в справке о решении ESET Virtual Private Network в Интернете:

- VPN Введение.
- VPN Установка.
- Работа с VPN.

Identity Protection

ESET Identity Protection — это решение по обеспечению безопасности, которое защищает вашу личную, кредитную и финансовую информацию. Identity Protection выявляет незаконную продажу вашей личной информации, проводя непрерывный мониторинг. При использовании Identity Protection вы будете получать уведомления на свой мобильный телефон, компьютер или планшет сразу после того, как ваши идентификационные данные окажутся под угрозой.

Дополнительные сведения см. в справке о решении ESET Identity Protection в Интернете:

Импорт и экспорт параметров

Можно импортировать и экспортировать пользовательский .xml-файл конфигурации ESET Security Ultimate с помощью меню **Настройка**.

Иллюстрированные инструкции

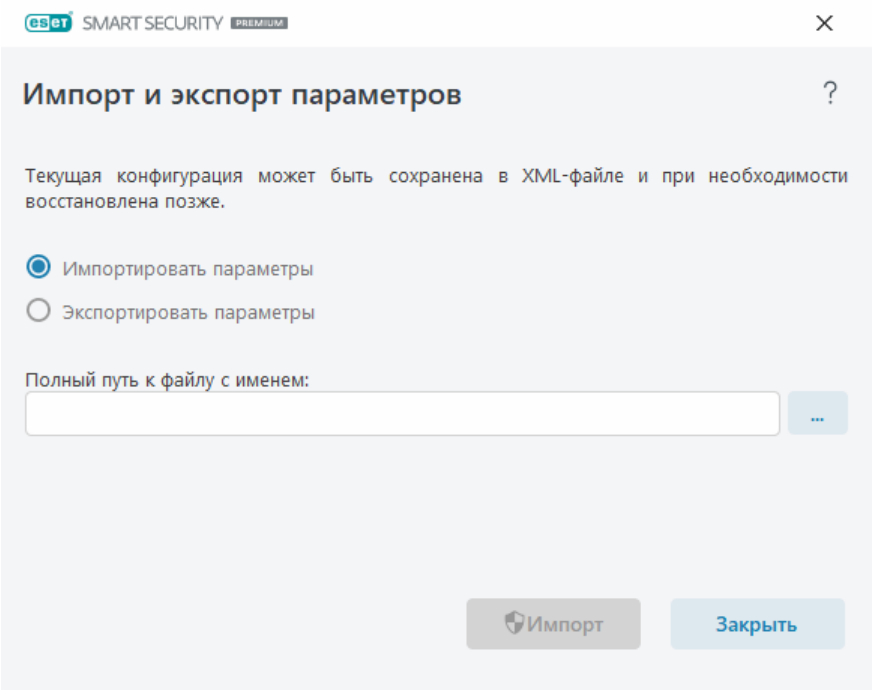
Иллюстрированные инструкции на английском и еще нескольких языках приведены в разделе Импорт и экспорт конфигурации ESET с помощью XML-файла.

Импорт и экспорт файлов конфигурации можно применять, если нужно создать резервную копию текущей конфигурации программы ESET Security Ultimate для использования в будущем. Экспорт параметров также удобен, если необходимо использовать предпочитаемую конфигурацию на нескольких компьютерах. Файл .xml можно импортировать для переноса нужных параметров.

Чтобы импортировать конфигурацию, в главном окне программы щелкните **Настройка** > **Импорт и экспорт параметров** и выберите **Импортировать параметры**. Введите имя файла конфигурации или нажмите кнопку **...**, чтобы выбрать файл конфигурации, который следует импортировать.

Чтобы экспортировать конфигурацию, в главном окне программы щелкните **Настройка** > **Импорт и экспорт параметров**. Выберите **Экспортировать параметры** и введите полный путь к файлу с именем. Щелкните **...**, чтобы перейти в расположение на вашем компьютере, в котором необходимо сохранить файл конфигурации.

При экспорте параметров может возникнуть ошибка, если у вас недостаточно прав для записи экспортируемого файла в указанный каталог.



Справка и поддержка

Щелкните **Справка и поддержка** в главном окне программы, чтобы отобразить сведения о поддержке и средствах устранения неполадок, которые помогут вам решить возможные проблемы.

Подписка

• Устранение проблем с подпиской: щелкните эту ссылку, чтобы найти решения для проблем с активацией или изменением подписки.

• Изменить подписку. Щелкните, чтобы открыть окно активации и активировать продукт. Если устройство подключено к ESET HOME, выберите подписку в своей учетной записи ESET HOME или добавьте новую.

Установленный продукт

• Новые возможности: щелкните этот элемент, чтобы открыть окно сведений о новых и улучшенных функциях.

• О программе ESET Security Ultimate: на экран выводится информация о вашей копии программы ESET Security Ultimate.

• Устранение проблем с продуктом: щелкните эту ссылку, чтобы найти решения часто встречающихся проблем.

• **Изменить программу**. Щелкните, чтобы узнать, можно ли сменить ESET Security Ultimate на другую линейку продуктов в рамках текущей подписки.

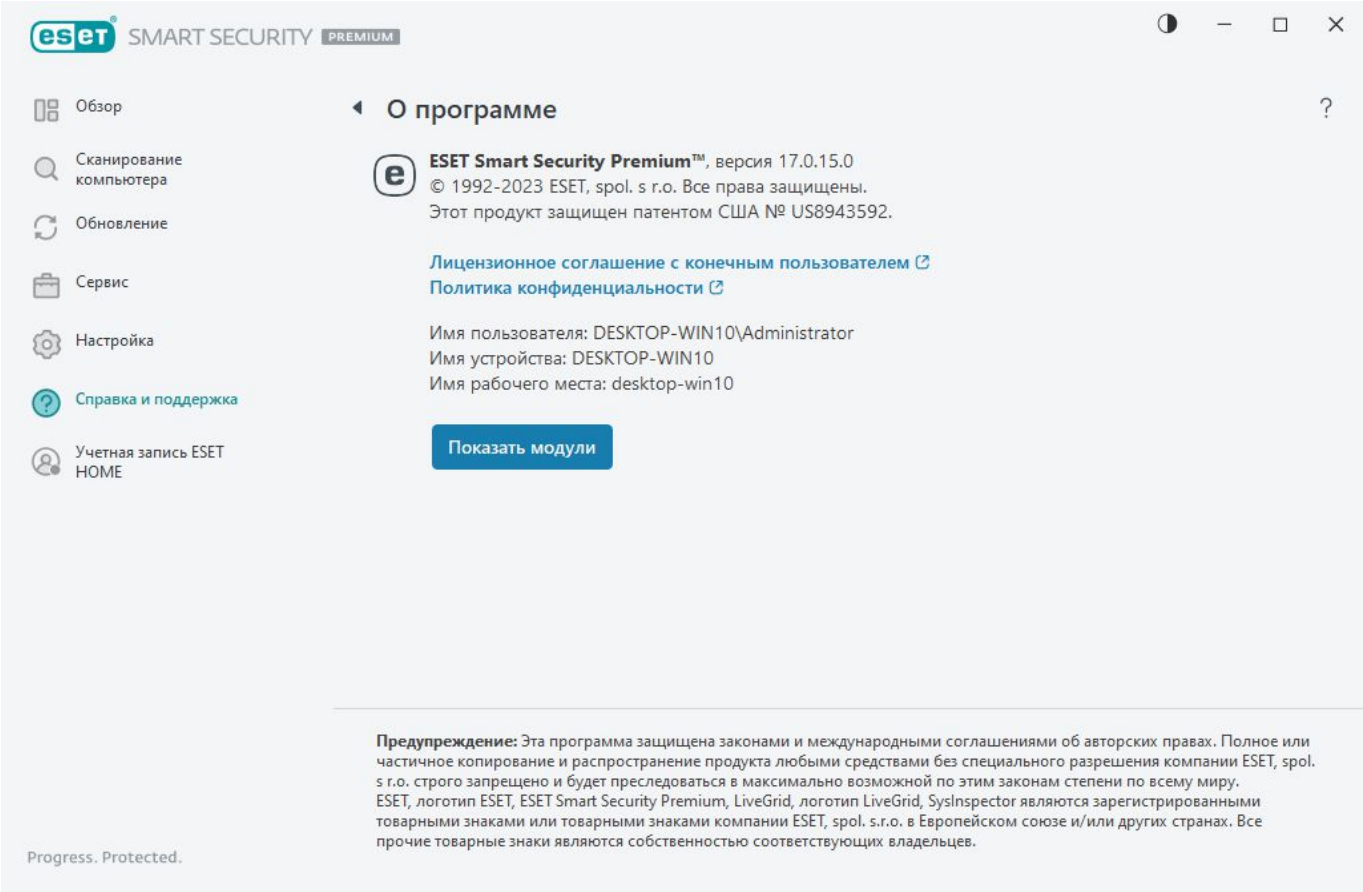
Страница справки – нажмите эту ссылку, чтобы открыть разделы справки ESET Security Ultimate.

Служба технической поддержки

База знаний: в базе знаний ESET содержатся ответы на наиболее часто задаваемые вопросы, а также рекомендуемые решения различных проблем. База знаний регулярно обновляется техническими специалистами ESET, что делает ее самым полезным инструментом для решения разнообразных проблем.

О программе ESET Security Ultimate

В этом окне содержатся сведения об установленной версии ESET Security Ultimate и о вашем компьютере.



Щелкните **Показать модули**, чтобы просмотреть информацию о списке загруженных модулей программы.

• Чтобы скопировать информацию о модулях в буфер обмена, используйте команду **Копировать**. Это может быть полезно при устранении проблем или обращении в службу технической поддержки.

• Щелкните **Модуль обнаружения** в окне «Модули», чтобы открыть сайт ESET Virus Radar, который содержит информацию о каждой версии модуля обнаружения ESET.

Новости ESET

В этом окне ESET Security Ultimate регулярно отображаются новости компании ESET.

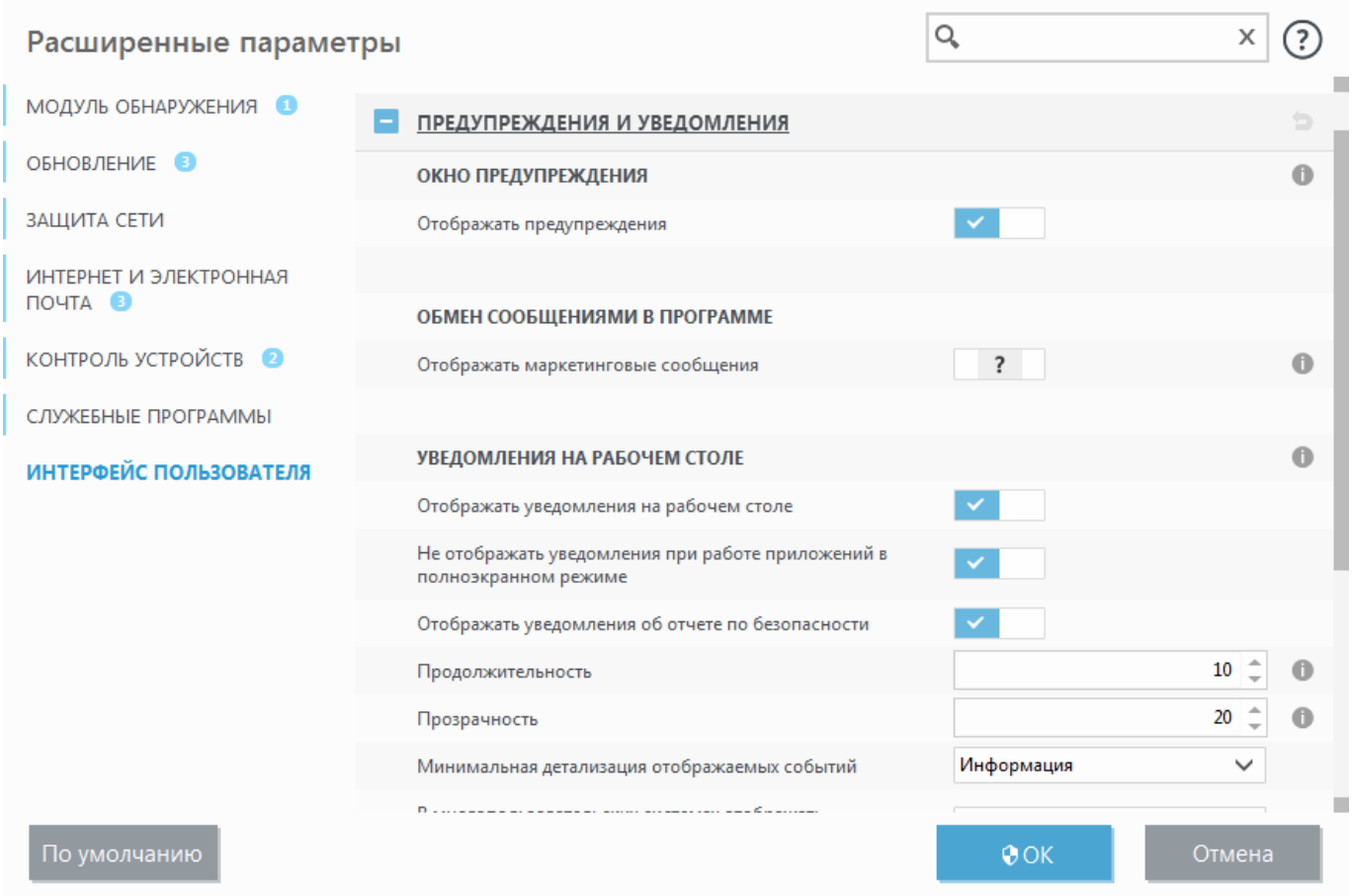
Функция внутрипрограммного обмена сообщениями предназначена для информирования пользователей о новостях ESET и для других сообщений. Для отправки маркетинговых сообщений требуется согласие пользователя. Маркетинговые сообщения по умолчанию не отправляются пользователю (отображается как вопрос). Включение этого параметра означает ваше согласие на получение маркетинговых сообщений ESET. Если вы не хотите получать маркетинговые материалы ESET, отключите параметр **Отображать маркетинговые сообщения**.

Чтобы включить или отключить получение маркетинговых сообщений в окне уведомления, выполните указанные ниже инструкции.

1. Вызов окна расширенных параметров.

2. Щелкните **Уведомления** > **Интерактивные предупреждения**.

3. Измените параметр **Отображать маркетинговые сообщения**.



Отправка данных о конфигурации системы

Чтобы иметь возможность максимально быстро и эффективно оказывать пользователям помощь, компании ESET требуется информация о конфигурации ESET Security Ultimate, подробные сведения о системе пользователя и запущенных в ней процессах (файл журнала ESET SysInspector) и данные реестра. Компания ESET использует эту информацию только для предоставления клиенту технической поддержки.

После отправки веб-формы в ESET будут отправлены данные о конфигурации вашей системы. Установите флажок **Всегда отправлять эти сведения**, если нужно запомнить данное действие для текущего процесса. При отправке веб-формы без отправки каких-либо данных щелкните **Не отправлять данные** и продолжите.

Настроить отправку данных о конфигурации системы можно в разделе Расширенные параметры > **Сервис** > **Диагностика** > Служба технической поддержки.

Если вы решили отправить данные о конфигурации системы, необходимо заполнить и отправить веб-форму. В противном случае ваша заявка не будет создана, и данные о конфигурации вашей системы будут потеряны. Если данные о конфигурации системы отправить не удается, заполните веб-форму и дождитесь инструкций от службы технической поддержки.

Служба технической поддержки

В главном окне программы щелкните **Справка и поддержка** > **Служба технической поддержки**.

Обратиться в службу технической поддержки

Запрос в службу поддержки: если не удается найти ответ на вопрос, можно обратиться в службу технической поддержки ESET с помощью формы, расположенной на веб-сайте ESET. В зависимости от настроек вашего продукта перед заполнением веб-формы может появиться окно для отправки данных о конфигурации системы.

Получение информации для службы технической поддержки

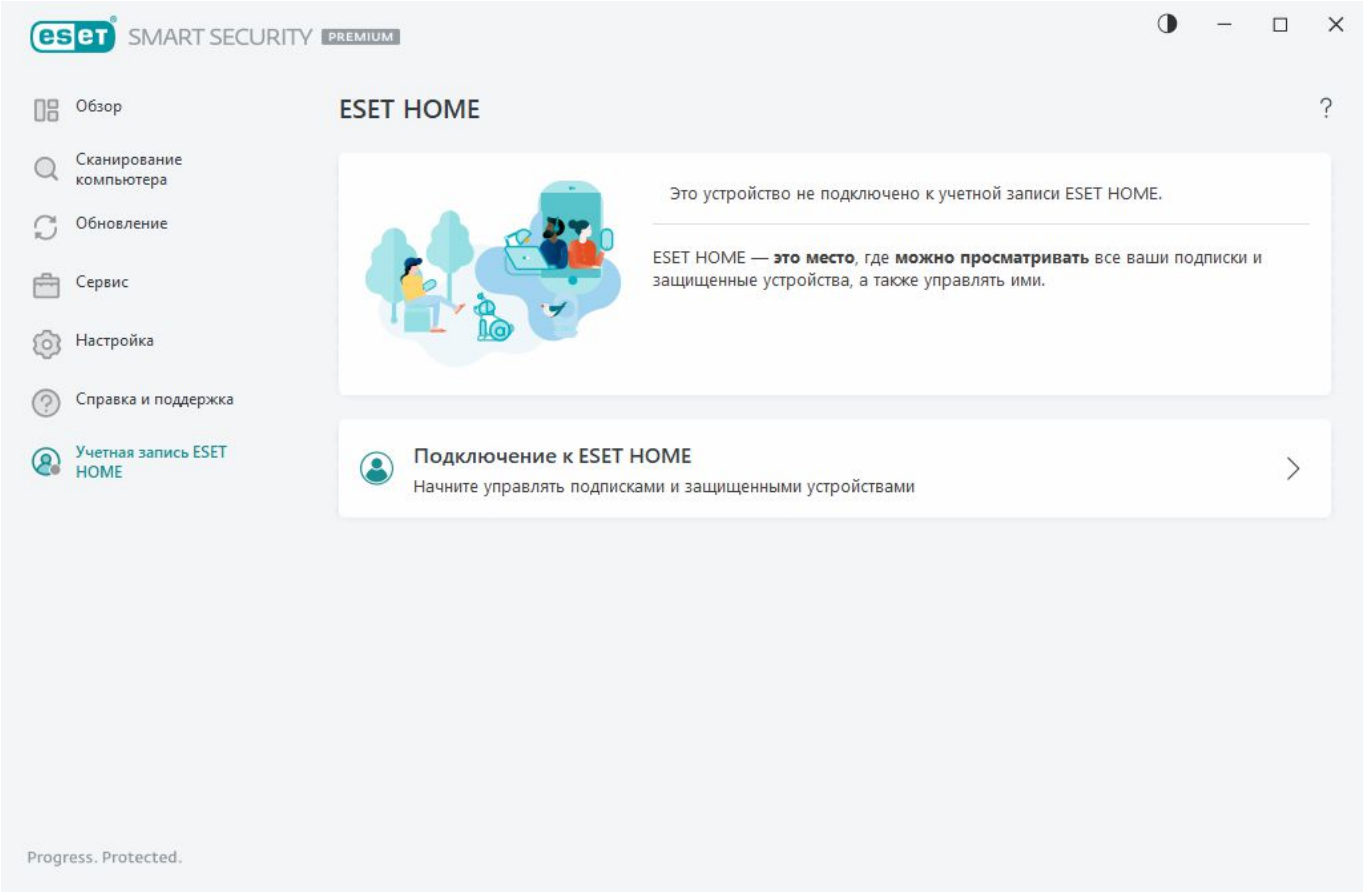
Информация для службы технической поддержки: в ответ на запрос скопируйте и отправьте информацию в службу технической поддержки ESET (например, сведения о подписке, имени продукта, версии продукта, операционной системе и компьютере).

ESET Log Collector — ссылка на статью в базе знаний ESET, откуда можно загрузить программу ESET Log Collector, которая автоматически собирает информацию и журналы с компьютера, чтобы ускорить решение проблем. Дополнительные сведения можно просмотреть в онлайн-руководстве пользователя ESET Log Collectorздесь.

Включите расширенное ведение журналов, чтобы создать расширенные журналы для всех доступных компонентов и помочь разработчикам в диагностике и решении проблем. Для минимальной степени детализации журнала установлен уровень **Диагностика**. Расширенное ведение журналов будет автоматически отключено через два часа, если вы не остановите его раньше, щелкнув **Остановить расширенное ведение журналов**. Когда все журналы будут созданы, отобразится окно уведомления для прямого доступа к папке диагностики, в которой содержатся созданные журналы.

Учетная запись ESET HOME

Состояние подключения учетной записи ESET HOME можно просмотреть в главном окне программы > **Учетная запись ESET HOME**.



Это устройство не подключено к учетной записи ESET HOME

Щелкните Подключение к ESET HOME, чтобы подключить устройство к ESET HOME и управлять своими подписками и защищенными устройствами. Вы можете продлить подписку, повысить ее уровень или расширить ее, а также просмотреть важные сведения. На портале управления или в мобильном приложении ESET HOME можно добавлять различные подписки, загружать продукты на свои устройства, проверять состояние безопасности продукта и делиться подпиской по электронной почте. Дополнительные сведения можно найти на онлайн-справке ESET HOME.

Это устройство подключено к учетной записи ESET HOME

Вы можете управлять безопасностью устройства удаленно с помощью мобильного приложения или портала ESET HOME. Щелкните **App Store** или **Google Play**, чтобы отобразился QR-код, который можно просканировать мобильным телефоном для загрузки мобильного приложения ESET HOME из магазина App Store или Google Play.

Учетная запись ESET HOME: имя вашей учетной записи ESET HOME.

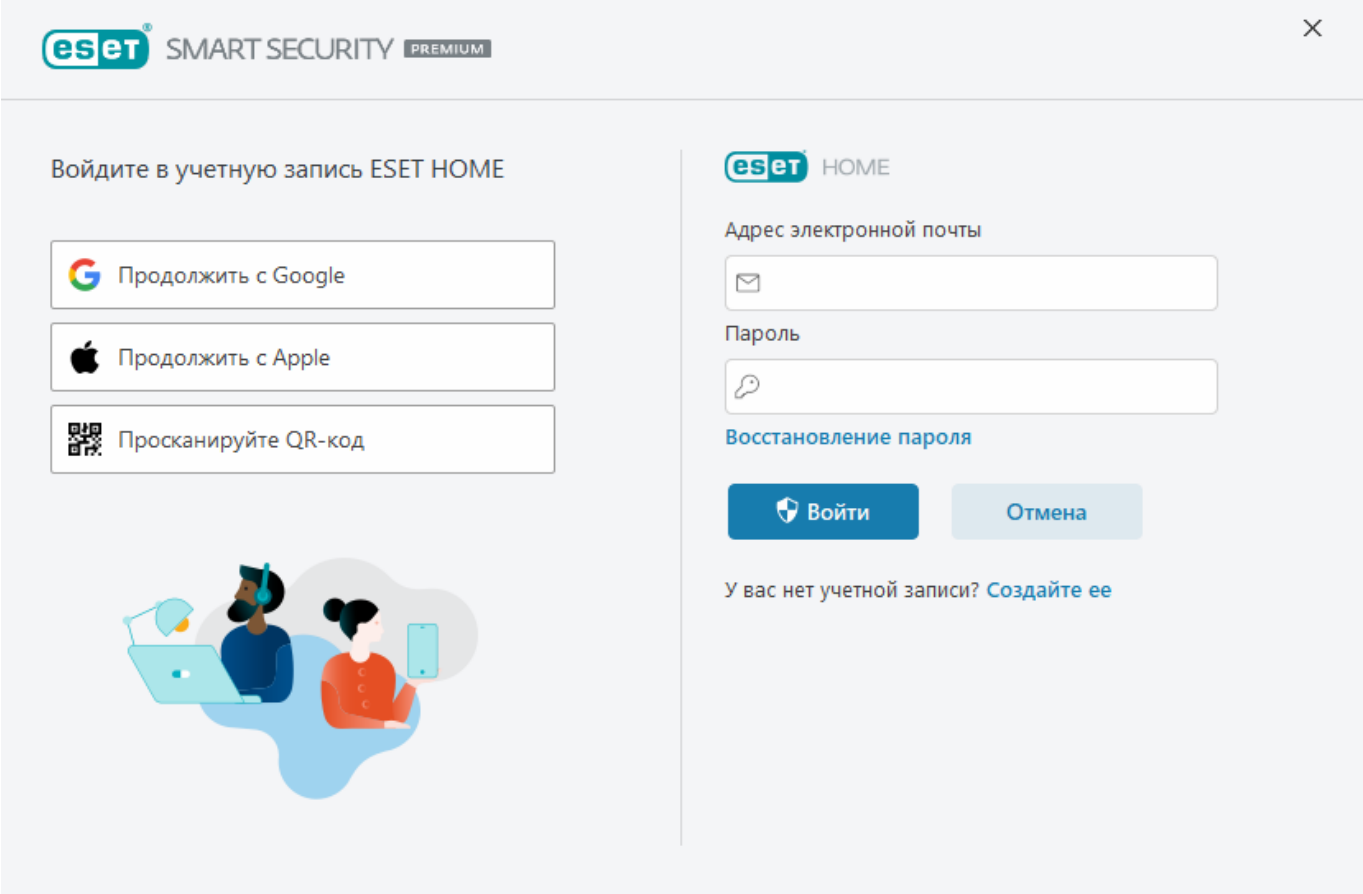
Имя устройства: имя этого устройства, отображаемое в учетной записи ESET HOME.

Открыть ESET HOME: открывает портал управления ESET HOME.

Чтобы отключить устройство от учетной записи ESET HOME, щелкните **Отключиться от ESET HOME** > **Отключить**. Подписка, использованная для активации, останется активной, и ваше устройство будет под защитой.

Подключение к ESET HOME

Подключите свое устройство к ESET HOME, чтобы получить возможность просматривать все активированные подписки и устройства ESET и управлять ими. Подписку можно продлить, расширить или повысить ее уровень, а также просмотреть важные сведения о ней. На портале управления или в мобильном приложении ESET HOME можно добавлять различные подписки, загружать продукты на свои устройства, проверять состояние безопасности продукта и делиться подписками по электронной почте. Дополнительные сведения можно найти на онлайн-справке ESET HOME.



Подключите устройство к решению ESET HOME:

> При подключении к ESET HOME во время установки или при выборе **Использовать учетную запись ESET HOME** в качестве метода активации следуйте инструкциям из раздела Использование учетной записи ESET HOME.
> Если вы уже установили и активировали ESET Security Ultimate с помощью подписки, добавленной в вашу учетную запись ESET HOME, устройство можно подключить к ESET HOME на портале ESET HOME. Следуйте инструкциям в онлайн-справке ESET HOME и разрешите подключение в ESET Security Ultimate.

1. В главном окне программы щелкните **учетную запись ESET HOME** > **Подключиться к ESET HOME** или щелкните **Подключиться к ESET HOME** в уведомлении **Подключение этого устройства к учетной записи ESET HOME**.

2. Вход в учетную ESET HOME запись.

Если у вас нет учетной записи ESET HOME, щелкните **Создать учетную запись**, чтобы зарегистрироваться, или ознакомьтесь с инструкциями в онлайн-справке ESET HOME. Если вы забыли пароль, щелкните **Я не помню пароль** и следуйте инструкциям на экране или ознакомьтесь с инструкциями в онлайн-справке ESET HOME.

3. Введите **имя устройства** и щелкните **Продолжить**.

4. После успешного подключения откроется окно со сведениями. Щелкните **Готово**.

Авторизация в ESET HOME

Существует несколько способов авторизации в учетной записи ESET HOME.

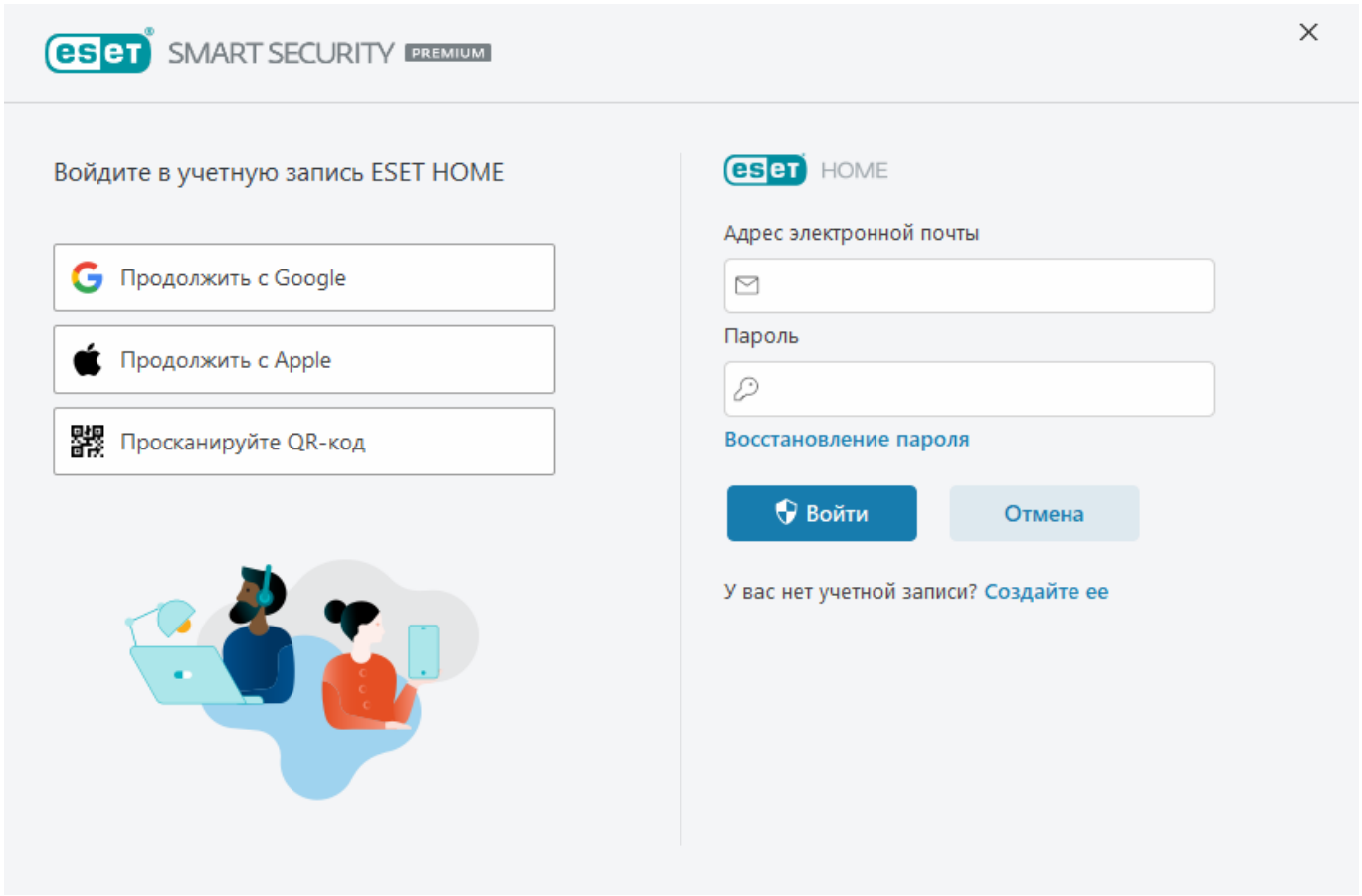
• **Использовать адрес электронной почты и пароль ESET HOME**: введите **адрес электронной почты** и **пароль**, которые вы использовали для создания учетной записи ESET HOME, а затем щелкните **Авторизоваться**.

• **Использовать учетную запись Google/AppleID**: щелкните **Продолжить с Google** или **Продолжить с Apple** и авторизуйтесь в соответствующей учетной записи. После успешной авторизации вы будете перенаправлены на веб-страницу подтверждения ESET HOME. Чтобы продолжить, вернитесь в окно продукта ESET. Дополнительные сведения об авторизации с помощью учетной записи Google/AppleID см. в онлайн-справке ESET HOME.

• **Просканировать QR-код**: щелкните **Просканируйте QR-код**, чтобы отобразить QR-код. Откройте мобильное приложение ESET HOME и просканируйте QR-код или наведите камеру устройства на QR-код. Дополнительные сведения см. в онлайн-справке ESET HOME.

Если у вас нет учетной записи ESET HOME, щелкните **Создать учетную запись**, чтобы зарегистрироваться, или ознакомьтесь с инструкциями в онлайн-справке ESET HOME. Если вы забыли пароль, щелкните **Я не помню пароль** и следуйте инструкциям на экране или ознакомьтесь с инструкциями в онлайн-справке ESET HOME.

Не удалось войти — распространенные ошибки.



Не удалось войти — распространенные ошибки

Не удалось найти учетную запись, которая соответствует введенному адресу электронной почты

Введенный адрес электронной почты не соответствует ни одной учетной записи ESET HOME. Щелкните **Назад** и введите правильный адрес электронной почты и пароль.

Чтобы авторизоваться, необходимо создать учетную запись ESET HOME. Если у вас нет учетной записи ESET HOME, щелкните **Назад** > **Создать учетную запись** или ознакомьтесь с разделом Создание новой учетной записи ESET HOME.

Имя пользователя и пароль не соответствуют друг другу

Введенный пароль не соответствует введенному адресу электронной почты. Щелкните **Назад**, введите правильный пароль и убедитесь в правильности введенного адреса электронной почты. Если вам все еще не удается авторизоваться, щелкните **Назад** > **Я не помню пароль**, чтобы сбросить пароль, а затем следуйте инструкциям на экране или ознакомьтесь с разделом Я не помню пароль ESET HOME.

Выбранный вариант входа не соответствует вашей учетной записи

Ваша учетная запись связана с вашей учетной записью в социальной сети. Чтобы авторизоваться в ESET HOME, щелкните **Продолжить с Google** или **Продолжить с Apple**, а затем авторизуйтесь в соответствующей учетной записи. После успешной авторизации вы будете перенаправлены на веб-страницу подтверждения ESET HOME. На портале ESET HOME вы можете отключить свою учетную запись в социальной сети от своей учетной записи ESET HOME.

Неправильный пароль

Эта ошибка может возникнуть, если ваш продукт ESET Security Ultimate уже подключен к ESET HOME и вы вносите изменения, которые требуют авторизации (например, отключаете модуль Антивор), а введенный вами пароль не соответствует вашей учетной записи. Щелкните **Назад** и введите правильный пароль. Если вам все еще не удается авторизоваться, щелкните **Назад** > **Я не помню пароль**, чтобы сбросить пароль, а затем следуйте инструкциям на экране или ознакомьтесь с разделом Я не помню пароль ESET HOME.

Добавление устройства в ESET HOME

Если вы уже установили и активировали ESET Security Ultimate с помощью подписки, добавленной в вашу учетную запись ESET HOME, устройство можно подключить к ESET HOME на портале ESET HOME.

1. Отправьте на свое устройство запрос на подключение.

2. В ESET Security Ultimate отобразится диалоговое окно **Подключение этого устройства к учетной записи ESET HOME** с именем вашей учетной записи ESET HOME. Щелкните **Разрешить**, чтобы подключить устройство к указанной учетной записи ESET HOME.

> Если взаимодействие не произойдет, запрос на подключение будет автоматически отменен примерно через 30 минут.

Дополнительные настройки

В разделе «Расширенные параметры» можно детально настроить ESET Security Ultimate в соответствии с вашими потребностями.

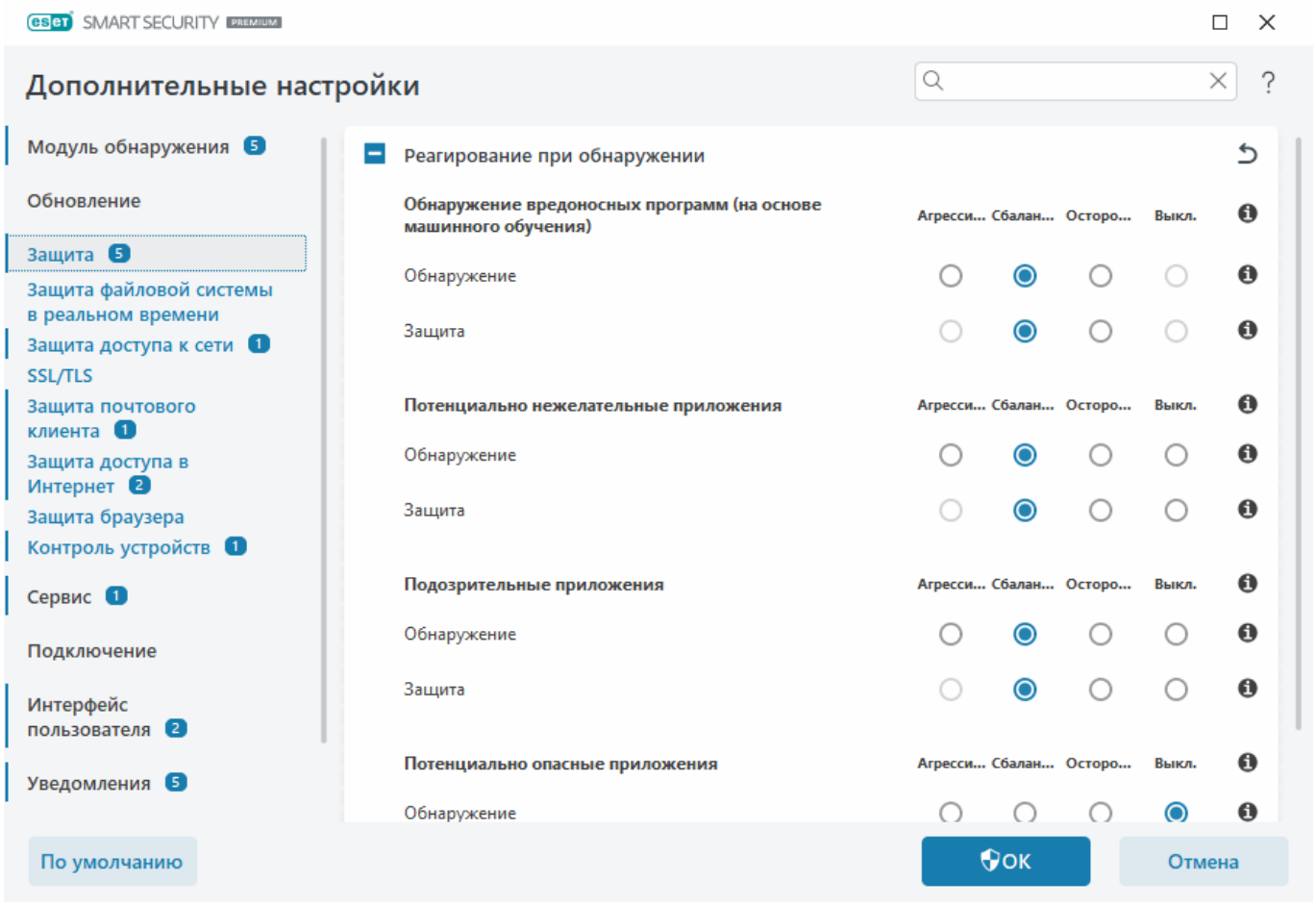
Чтобы получить доступ к расширенным параметрам, откройте главное окно программы и нажмите клавишу **F5** на клавиатуре или щелкните **Настройка** > **Расширенные параметры**.

> В зависимости от настроек доступа вам может быть предложено ввести пароль, чтобы открыть расширенные параметры.

В расширенных параметрах доступны настройки для следующих элементов:

- Модуль обнаружения

- обновление;
- Защита
- Служебные программы
- Подключение
- Интерфейс пользователя
- Уведомления
- Настройки конфиденциальности



Модуль обнаружения

В разделе Расширенные параметры > **Модуль обнаружения** можно настроить следующие опции:

- Исключения
- Расширенные параметры
- Сканер сетевого трафика

Исключения

Исключения позволяют исключить объекты из модуля обнаружения. Чтобы обеспечить сканирование всех объектов на наличие угроз, рекомендуется создавать исключения только в случае крайней необходимости. Случаи, в которых может понадобиться исключить объекты, включают сканирование баз данных большой емкости, которые замедляет работу или программное обеспечение, которое противоречит сканированию.

Исключения для быстродействия: исключение файлов и папок из сканирования. Исключения для быстродействия полезны для исключения при сканировании игровых приложений на уровне файлов, неправильном поведении системы или повышенной производительности.

Исключения из обнаружения позволяют исключить объекты из обнаружения, используя имя обнаружения, путь или хеш. Они не исключают файлы и папки из сканирования как делают исключения для быстродействия. Исключения обнаружения исключают объекты только при их обнаружении модулем обнаружения и если в списке исключений присутствует соответствующее правило.

Не стоить путать с другими типами исключений:

- Исключения из операции: все операции с файлами, относящиеся к исключенным из сканирования процессам приложения (может понадобится для повышения скорости резервного копирования и доступности служб).
- Исключенные расширения файлов
- Исключения системы HIPS
- Фильтр «Исключение» для защиты на основе облака

Исключения для быстродействия

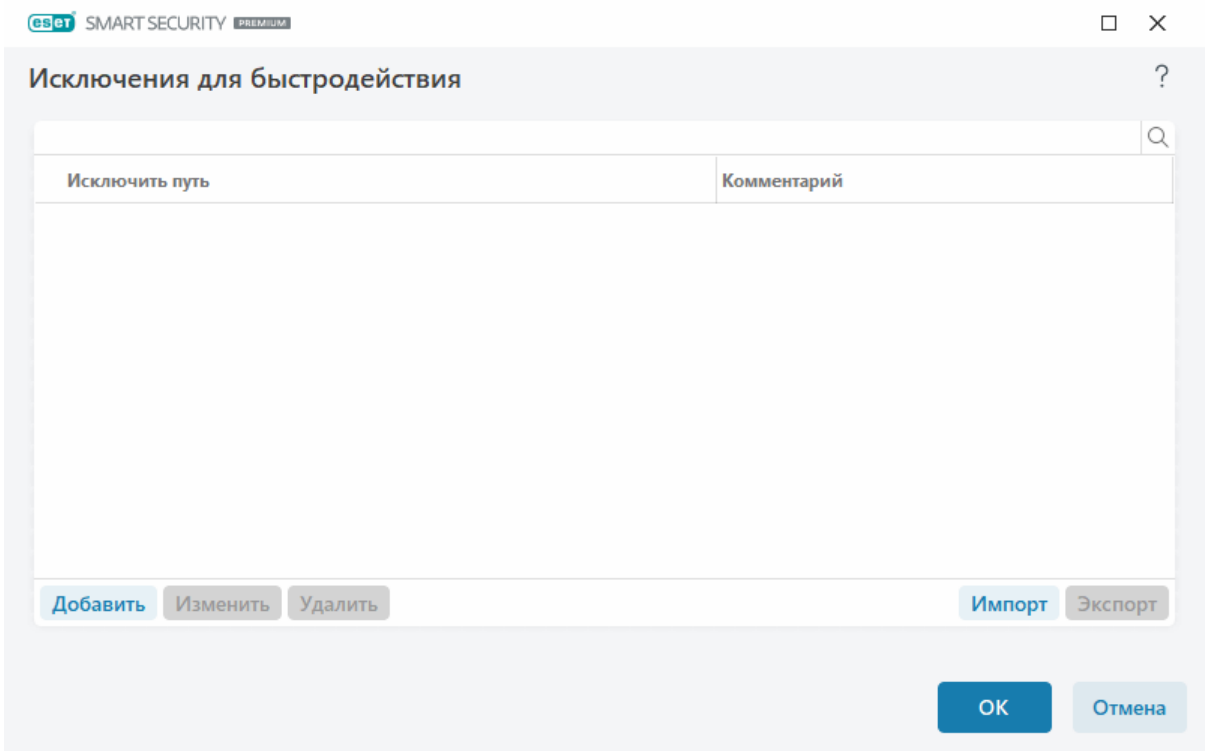
Исключения для быстродействия позволяют исключить файлы и папки из сканирования.

Мы рекомендуем создавать исключения для быстродействия только при абсолютной необходимости, чтобы гарантировать, что все объекты просканированы на наличие угроз. Однако, все же могут быть ситуации, когда вам понадобится исключить объект, например, данные базы данных большой емкости, которые замедляют компьютер во время сканирования, или ПО, которое создает препятствия для сканирования.

Файлы и папки можно исключить из сканирования и поместить в перечень исключений, выбрав Расширенные параметры > **Модуль обнаружения** > **Исключения** > **Исключения для быстродействия** > **Изменить**.

> Не следует путать эту функцию с другими возможностями исключения — Исключения из обнаружения, Исключенные расширения файлов, Исключения системы HIPS или Исключения для процессов.

Чтобы исключить объект (путь: файл или папка) из сканирования, щелкните **Добавить** и введите соответствующий путь или выделите его в древовидной структуре.



Угроза в файле не будет обнаружена модулем **Защиты файловой системы в реальном времени** или модулем **сканирования компьютера**, если файл соответствует критериям для исключения из сканирования.

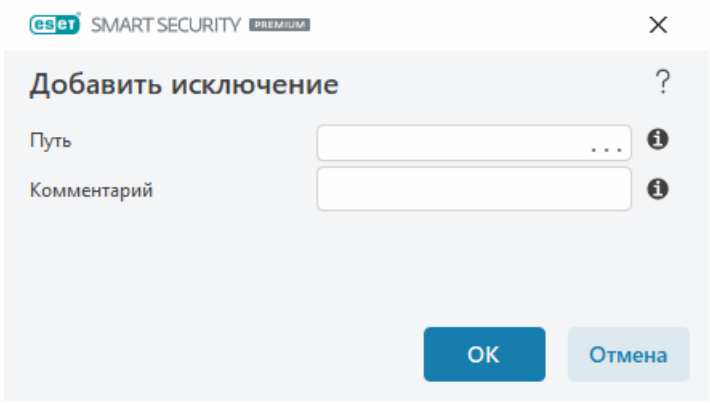
Элементы управления

- **Добавить**: команда, исключающая объекты из сканирования.
- **Изменить**: изменение выделенных записей.
- **Удалить**: удаление выбранных записей (чтобы выбрать несколько записей, щелкайте их, удерживая нажатой клавишу CTRL).

Добавление или изменение исключений для быстродействия

Диалоговое окно исключает определённый путь (файл или каталог) для этого компьютера.

Выберите путь или введите вручную
Чтобы выбрать нужный путь, выберите **...** в поле **Путь**.
При вводе вручную см. дополнительные примеры формата исключения ниже.



Для исключения групп файлов можно использовать символы подстановки. Вопросительный знак (*?*) обозначает один символ, а звездочка (***) — строку из любого количества символов.

Формат исключений

- Чтобы исключить все файлы и вложенные папки в определенной папке, укажите путь к папке и используйте маску *
- Если нужно исключить только файлы с расширением DOC, используйте маску **.doc*
- Если имя исполняемого файла содержит определенное число символов (и символы могут меняться), причем известна только первая буква имени (например, D), используйте следующий формат:

D????.exe (знаки вопроса заменяют отсутствующие или неизвестные символы)

Примеры

- *C:\Tools**: путь должен заканчиваться обратной косой чертой ((\)) и звездочкой ((*)), указывающими, что это папка, все содержимое которое (файлы и вложенные папки) следует исключить.
- *C:\Tools*.**: поведение будет аналогично варианту *C:\Tools**
- *C:\Tools*: папку *Tools* не будет исключено. С точки зрения модуля сканирования *Tools* может также быть именем файла.
- *C:\Tools*.dat*: это применяется для исключения файлов .dat в папке *Tools*.
- *C:\Tools\sg.dat*: применяется для исключения отдельного файла, размещенного в точном пути.

Системные переменные в исключениях

Для определения исключений из сканирования можно использовать системные переменные, например %PROGRAMFILES%.

• Чтобы исключить папку «Program Files» с помощью такой системной переменной, укажите в исключениях путь *%PROGRAMFILES%** (не забудьте добавить обратную косую черту и звездочку в конце пути).

• Чтобы исключить все файлы и папки в подкаталоге *%PROGRAMFILES%*, укажите путь *%PROGRAMFILES%\Excluded_Directory**

Развернуть список поддерживаемых системных переменных

Формат исключения пути поддерживает следующие переменные:

- *%ALLUSERSPROFILE%*
- *%COMMONPROGRAMFILES%*
- *%COMMONPROGRAMFILES(X86)%*
- *%COMSPEC%*
- *%PROGRAMFILES%*
- *%PROGRAMFILES(X86)%*
- *%SystemDrive%*
- *%SystemRoot%*
- *%WINDIR%*
- *%PUBLIC%*

Пользовательские системные переменные (например, *%TEMP%* или *%USERPROFILE%*) и переменные среды (например, *%PATH%*) не поддерживаются.

Подстановочные знаки в середине пути не поддерживаются

Программа иногда может правильно исключать из обработки пути с подстановочными знаками в середине (например, *C:\Tools*\Data\file.dat*), но официально эта возможность не поддерживается.

При использовании исключений из обнаружения ограничения на использование специальных символов в середине пути не применяются.

Порядок исключений

• Настройка уровня приоритета для исключений с помощью кнопок «В начало» и «В конец» (как в разделе Правила файервола, где правила последовательно выполняются сверху вниз) не предусмотрена.

• Когда модуль сканирования обнаруживает совпадение с первым применимым правилом, второе применимое правило не проверяется.

• Чем меньше правил, тем быстрее происходит сканирование.

• Не следует создавать совпадающие правила.

Формат исключения пути

Для исключения групп файлов можно использовать символы подстановки. Вопросительный знак (*?*) обозначает один символ, а звездочка (***) — строку из любого количества символов.

Формат исключений

• Чтобы исключить все файлы и вложенные папки в определенной папке, укажите путь к папке и используйте маску *

• Если нужно исключить только файлы с расширением DOC, используйте маску **.doc*

• Если имя исполняемого файла содержит определенное число символов (и символы могут меняться), причем известна только первая буква имени (например, D), используйте следующий формат:

D????.exe (знаки вопроса заменяют отсутствующие или неизвестные символы)

Примеры

• *C:\Tools**: путь должен заканчиваться обратной косой чертой ((\)) и звездочкой ((*)), указывающими, что это папка, все содержимое которое (файлы и вложенные папки) следует исключить.

• *C:\Tools*.**: поведение будет аналогично варианту *C:\Tools**

• *C:\Tools*: папку *Tools* не будет исключено. С точки зрения модуля сканирования *Tools* может также быть именем файла.

• *C:\Tools*.dat*: это применяется для исключения файлов .dat в папке *Tools*.

• *C:\Tools\sg.dat*: применяется для исключения отдельного файла, размещенного в точном пути.

Системные переменные в исключениях

Для определения исключений из сканирования можно использовать системные переменные, например %PROGRAMFILES%.

• Чтобы исключить папку «Program Files» с помощью такой системной переменной, укажите в исключениях путь *%PROGRAMFILES%** (не забудьте добавить обратную косую черту и звездочку в конце пути).

• Чтобы исключить все файлы и папки в подкаталоге *%PROGRAMFILES%*, укажите путь *%PROGRAMFILES%\Excluded_Directory**

Развернуть список поддерживаемых системных переменных

Формат исключения пути поддерживает следующие переменные:

• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*

Пользовательские системные переменные (например, *%TEMP%* или *%USERPROFILE%*) и переменные среды (например, *%PATH%*) не поддерживаются.

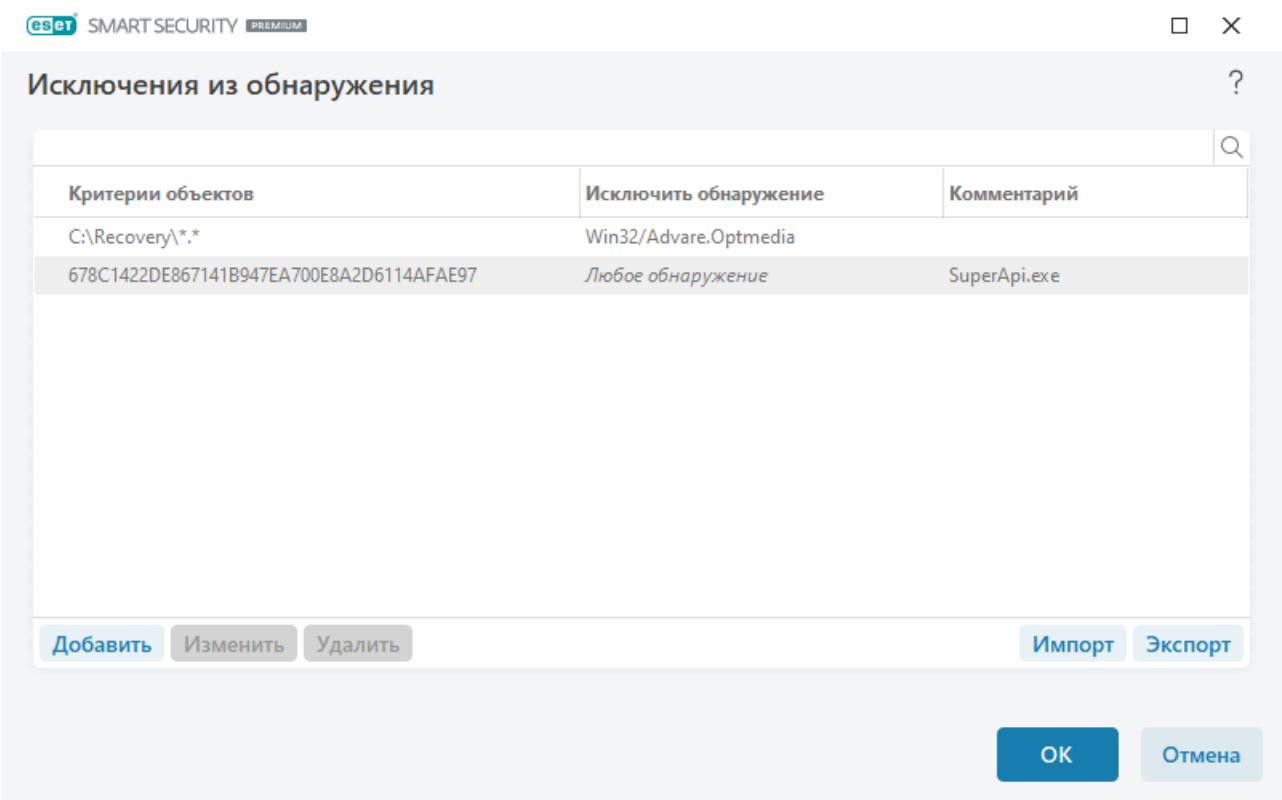
Исключения из обнаружения

Исключения из обнаружения позволяют исключить объекты из списка обнаружения путем фильтрации имени обнаружения, пути объекта или его хеша.

Как работает исключение обнаружения

Исключения из обнаружения не исключают файлы и папки из сканирования, как делают Исключения для быстродействия. Исключения обнаружения исключают объекты только при их обнаружении модулем обнаружения и если в списке исключений присутствует соответствующее правило.

Например (см. первый ряд на изображении ниже), когда объект определяется как Win32/Adware.Optmedia и обнаруженный файл — *C:\Recovery\file.exe*. Во второй строке, каждый файл, в котором есть подходящий хеш SHA-1, всегда будет исключен, несмотря на имя обнаружения.



Чтобы убедиться, что все угрозы обнаружены, мы рекомендуем создавать исключения из обнаружения только тогда, когда это абсолютно необходимо.

Чтобы добавить файлы и папки в список исключений, выберите Расширенные параметры > **Модуль обнаружения** > **Исключения** > **Исключения из обнаружения** > **Изменить**.

Не следует путать эту функцию с другими возможностями исключения — Исключения для быстродействия, Исключенные расширения файлов, Исключения системы HIPS или Исключения для процессов.

Чтобы исключить объект (по названию обнаружения или хешу) из модуля обнаружения, нажмите кнопку **Добавить**.

Для потенциально нежелательных и потенциально опасных приложений также можно создать исключение по имени обнаружения.

- В окне предупреждения, которое сообщает об обнаружении (щелкните **Показать расширенные параметры** и выберите **Исключить из обнаружения**).
- Из контекстного меню «Файлы журнала» с помощью Мастера создания исключения из

обнаружения.

• Щелкнув **Инструменты** > **Карантин**, после чего щелкнув правой кнопкой мыши находящийся на карантине файл и выбрав в контекстном меню команду **Восстановить и исключить из сканирования**.

Критерии объектов исключения из обнаружения

• **Путь**. Ограничение исключения из обнаружения для определенного пути (или любого другого пути).

• **Имя обнаружения**: если рядом с исключаемым файлом указано имя обнаружения, файл исключается только для этого обнаружения, а не полностью. Если этот файл впоследствии окажется зараженным другой вредоносной программой, он будет обнаружен.

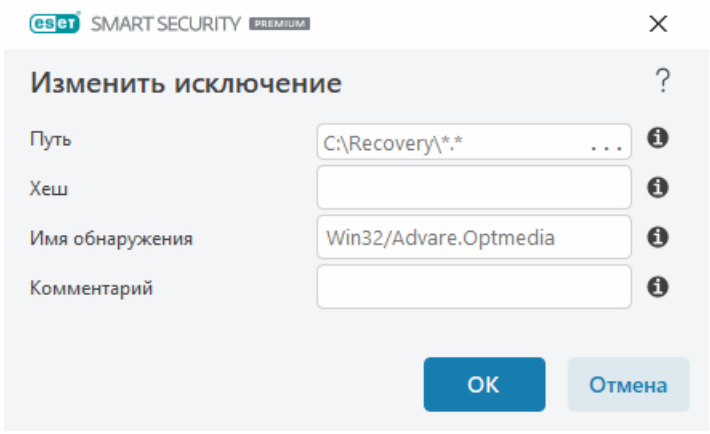
• **Хеш**: файл исключается на основании указанного хеша SHA-1 независимо от типа, расположения, имени или расширения.

Добавление или изменение исключений из обнаружения

Исключить обнаружение

Следует указать действительное имя для обнаружения ESET. Чтобы определить имя обнаружения, перейдите в раздел Файлы журнала и выберите элемент **Обнаружения** в раскрывающемся меню «Файлы журнала». Этот параметр полезен при обнаружении образца ложного срабатывания в ESET Security Ultimate. Добавлять в исключения реальные заражения крайне опасно. Рекомендуем исключать только затронутые файлы или каталоги, щелкнув элемент **...** в поле **Маска пути**, либо делать это только на ограниченный период времени. Исключения также применяются к потенциально нежелательным, потенциально опасным и подозрительным приложениям.

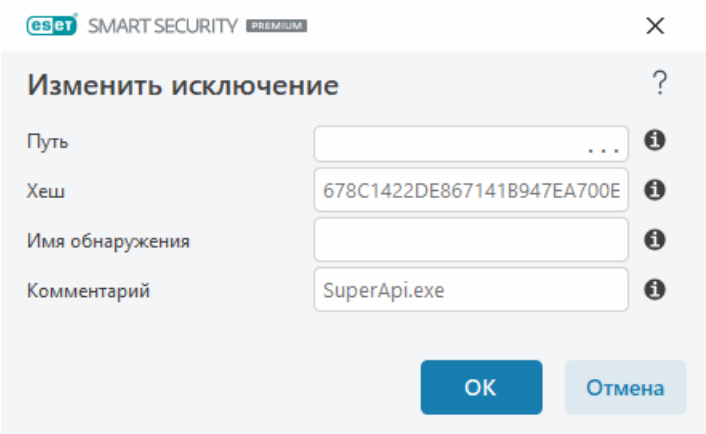
См. также Формат исключения пути.



См. также Пример исключения из обнаружения, который приведен ниже.

Исключить хеш

Файл исключается на основании указанного хеша SHA-1 независимо от типа, расположения, имени или расширения.



Исключения по имени обнаружения
Чтобы исключить определенное обнаружение по имени, введите правильное имя обнаружения:
Win32/Adware.Optmedia
Также для исключения обнаружения с помощью окна предупреждения ESET Security Ultimate можно воспользоваться приведенным далее форматом:
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

Элементы управления

- **Добавить**: команда, исключающая объекты из сканирования.
- **Изменить**: изменение выделенных записей.
- **Удалить**: удаление выбранных записей (чтобы выбрать несколько записей, щелкайте их, удерживая нажатой клавишу CTRL).

Создание исключения из обнаружения мастера

Исключение из обнаружения также можно создать из контекстного меню Файлы журнала (недоступно для обнаружения вредоносных программ):

1. В главном окне программы щелкните **Инструменты** > **Файлы журнала**.
2. Щелкните правой кнопкой мыши обнаружение в разделе **Журнал обнаружений**.
3. Выберите **Создать исключение**.

Чтобы исключить одно или несколько обнаружений на основе **критерии исключения**, щелкните элемент **Изменить критерии**:

- **Точные файлы**: исключение каждого файла по хешу SHA-1.
- **Обнаружение**: исключение каждого файла по имени обнаружения.
- **Путь + обнаружение**: исключение каждого файла по имени и пути обнаружения, включая имя файла (например, *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

Рекомендуемая опция выбирается предварительно в зависимости от типа обнаружения.

Кроме того, перед нажатием на элемент **Создать исключение** вы можете добавить **комментарий**.

Модуль обнаружения расширенных параметров

Включить расширенное сканирование с помощью AMSI — это средство Microsoft Antimalware Scan Interface, которое дает возможность сканировать сценарии PowerShell, сценарии, выполняемые сервером Windows Script Host, а также данные, которые сканируются с помощью пакета SDK AMSI.

Сканер сетевого трафика

Сканер сетевого трафика обеспечивает для протоколов приложений защиту от вредоносных программ, которая объединяет множество передовых методов сканирования на наличие вредоносных программ. Сканер сетевого трафика автоматически сканирует протоколы HTTP(S), POP3(S) и IMAP(S) независимо от используемого интернет-браузера или почтового клиента. Вы можете включить и отключить сканер сетевого трафика в разделе Расширенные параметры > **Модуль обнаружения** > **Сканер сетевого трафика**.

Включить сканер сетевого трафика: если эту опцию отключить, протоколы HTTP(S), POP3(S) и IMAP(S) сканироваться не будут. Обратите внимание, что для следующих функций ESET Security Ultimate сканер сетевого трафика должен быть включен:

- Защита доступа в Интернет
- Родительский контроль
- Конфиденциальность и безопасность браузера
- Защита банковских операций и браузера
- SSL/TLS
- Защита от фишинга
- Защита почтового клиента

Защита на основе облака

ESET LiveGrid®(основанная на передовой системе своевременного обнаружения ESET ThreatSense.Net) использует данные от пользователей ESET со всего мира и отправляет их в вирусную лабораторию ESET. Сеть ESET LiveGrid® позволяет получать подозрительные образцы и метаданные, поэтому мы можем незамедлительно реагировать на потребности пользователей и обеспечить готовность ESET к обезвреживанию новейших угроз.

ESET LiveGuard — это функция, добавляющая уровень защиты, специально разработанный для устранения невиданных ранее угроз. Если эта функция включена, подозрительные образцы, которые еще не подтверждены как вредоносные, но могут содержать вредоносные программы, будут автоматически отправляться в облако ESET.

Доступны следующие варианты:

Включение системы репутации ESET LiveGrid®, системы обратной связи ESET LiveGrid® и ESET LiveGuard

Система репутации ESET LiveGrid® работает на основе облачных белых и черных списков. Система обратной связи ESET LiveGrid® собирает информацию о компьютере пользователя, которая связана с новыми обнаруженными угрозами. Функция ESET LiveGuard обнаруживает новые, ранее не встречавшиеся угрозы, анализируя их поведение в песочнице.

Пользователь может проверить репутацию запущенных процессов и файлов непосредственно из интерфейса программы или с помощью контекстного меню, при этом доступна дополнительная информация из ESET LiveGrid®. Благодаря проактивной защите ESET LiveGuard исполнение новых файлов блокируется до получения результата анализа.

Включить систему репутации ESET LiveGrid®

Система репутации ESET LiveGrid® работает на основе облачных белых и черных списков.

Проверите репутацию запущенных процессов и файлов непосредственно в интерфейсе программы или в контекстном меню, благодаря чему становится доступна дополнительная информация из ESET LiveGrid®.

Включить систему обратной связи ESET LiveGrid®

Система обратной связи ESET LiveGrid®, дополняющая систему репутации ESET LiveGrid®, собирает информацию о компьютере пользователя, которая связана с новыми обнаруженными угрозами. Это может быть:

- Образец или копия файла, в котором возникла угроза
- Путь к файлу
- Имя файла
- Дата и время

• Процесс, с помощью которого угроза появилась на компьютере

• Информация об операционной системе компьютера

По умолчанию программа ESET Security Ultimate отправляет подозрительные файлы в вирусную лабораторию ESET для тщательного анализа. Всегда исключаются файлы с определенными расширениями, такими как *.doc* и *.xls*. Также можно добавить другие расширения, если политика вашей организации предписывает исключение из отправки.

Подробные сведения об отправке соответствующих данных приведены в Политике конфиденциальности.

Не включать ESET LiveGrid®

Функциональность программного обеспечения при этом не теряется, но в некоторых случаях ESET Security Ultimate может быстрее реагировать на новые угрозы, когда система ESET LiveGrid® включена. Если система ESET LiveGrid® использовалась ранее, но была отключена, могут оставаться некоторые пакеты данных, предназначенные для отправки. Эти пакеты будут отправлены в ESET даже после выключения системы. После отправки всей текущей информации новые пакеты создаваться не будут.

Дополнительную информацию о ESET LiveGrid® см. в глоссарии.
См. наши иллюстрированные инструкции на английском и еще нескольких языках по включению и отключению ESET LiveGrid® в ESET Security Ultimate.

Настройка облачной защиты в окне расширенных параметров

Чтобы получить доступ к настройкам ESET LiveGrid® и ESET LiveGuard, откройте раздел Расширенные параметры > **Модуль обнаружения** > **Облачная защита**.

• **Включить систему репутации ESET LiveGrid® (рекомендуется)**. Система репутации ESET LiveGrid® увеличивает эффективность решений ESET для защиты от вредоносных программ, так как благодаря ей сканируемые файлы сопоставляются с элементами «белого» и «черного» списков в облаке.

• **Включение средства ESET LiveGrid® системы отзывов** — отправляет соответствующие данные образцов (описанные в разделе **Отправка образцов**) вместе с отчетами о сбоях и статистическими данными в исследовательскую лабораторию ESET для дальнейшего анализа.

• **Включить ESET LiveGuard** — функция ESET LiveGuard обнаруживает новые, ранее не встречавшиеся угрозы, анализируя их поведение в песочнице. Включить ESET LiveGuard можно, только если включена система ESET LiveGrid®.

• **Отправлять отчеты об аварийном завершении и данные диагностики**: отправка относящихся к ESET LiveGrid® диагностических данных, таких как отчеты об аварийных завершениях и дампы памяти модулей. Рекомендуем не выключать этот параметр, чтобы помочь ESET выявлять проблемы, совершенствовать продукты и улучшать защиту конечных

пользователей.

• **Отправить анонимную статистическую информацию** — с помощью этого параметра можно разрешить продукту ESET собирать информацию о недавно обнаруженных угрозах: имя угрозы, дата и время обнаружения, способ обнаружения, связанные метаданные, версия и конфигурация продукта (включая информацию о системе).

• **Контактный адрес электронной почты (необязательно)** — вместе с подозрительными файлами можно отправить контактный адрес электронной почты, чтобы специалисты ESET могли обратиться к вам, если для анализа потребуется дополнительная информация. Имейте в виду, что компания ESET не отправляет ответы пользователям без необходимости.

Отправка образцов

Отправка образцов вручную — включение опции отправки образцов в ESET вручную из контекстного меню, карантина или раздела Сервис.

Автоматическая отправка обнаруженных образцов

Укажите, какие образцы будут отправляться в ESET для анализа и совершенствования механизмов обнаружения (максимальный размер образца по умолчанию составляет 64 МБ). Доступны следующие варианты:

• **Все обнаруженные образцы**: все объекты, обнаруженные модулем обнаружения (в том числе потенциально нежелательные приложения, если в настройках модуля сканирования включен соответствующий параметр).

• **Все образцы, кроме документов**: все обнаруженные объекты, кроме **документов** (см. ниже).

• **Не отправлять**: обнаруженные объекты не будут отправляться в компанию ESET.

Автоматическая отправка подозрительных образцов

Эти образцы также будут отправляться в ESET, если модуль обнаружения их не обнаруживает. Например, образцы, которые почти избежали обнаружения, признаны подозрительными одним из модулей защиты ESET Security Ultimate или демонстрируют неоднозначное поведение (максимальный размер образца по умолчанию составляет 64 МБ).

• **Исполняемые файлы**: включает исполняемые файлы, такие как .exe, .dll, .sys.

• **Архивы**: включает такие типы файлов, как .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.

• **Сценарии**: включает такие типы файлов сценариев, как .bat, .cmd, .hta, .js, .vbs, .ps1.

• **Другое**: включает такие типы файлов, как .jar, .reg, .msi, .sfw, .lnk.

• **Возможный спам**: эта функция позволяет отправлять потенциальный спам (целиком или частично) и вложения в ESET для анализа. Включив ее, вы поможете точнее обнаруживать спам — для себя и для всего мира.

• **Удалять исполняемые файлы, архивы, сценарии, прочие образцы и возможный**

спам с серверов ESET: определяет, когда нужно удалять образцы, отправленные на анализ функцией ESET LiveGuard.

• **Документы**: включает документы Microsoft Office и PDF с активным содержимым и без него.

• **Удалять документы с серверов ESET**: определяет, когда нужно удалять документы, отправленные на анализ функцией ESET LiveGuard.

Разверните, чтобы открыть список всех включаемых типов файлов документов

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

Исключения

Фильтр исключений позволяет исключить из отправки определенные файлы или папки (например, может понадобиться исключить файлы, которые могут содержать конфиденциальную информацию, такую как документы и электронные таблицы). Перечисленные в этом списке файлы никогда не будут передаваться в ESET на анализ, даже если они содержат подозрительный код. Файлы наиболее распространенных типов (.doc и т. п.) исключаются по умолчанию. При желании можно дополнять список исключенных файлов.

Чтобы исключить файлы, загруженные с адреса `download.domain.com`, откройте раздел Расширенные параметры > **Модуль обнаружения** > **Облачная защита** > **Отправка образцов** и нажмите кнопку **Изменить** рядом с пунктом **Исключения**. Добавьте исключение `.download.domain.com`.

Максимальный размер образцов (МБ): определяет максимальный размер автоматически отправляемых образцов (1–64 МБ).

ESET LiveGuard

Фильтр «Исключение» для защиты на основе облака

Фильтр «Исключение» позволяет исключить из отправки образцов определенные файлы или папки. Перечисленные в этом списке файлы никогда не будут передаваться в ESET на анализ, даже если они содержат подозрительный код. Файлы распространенных типов (DOC и т. п.) исключаются по умолчанию.

С помощью этой функции можно исключить файлы, в которых может присутствовать конфиденциальная информация, например документы и электронные таблицы.

Чтобы исключить файлы, загруженные с адреса download.domain.com, щелкните Расширенные параметры > **Модуль обнаружения** > **Облачная защита** > **Отправка образцов** > **Исключения** и добавьте исключение *download.domain.com*.

ESET LiveGuard

ESET LiveGuard — это функция, добавляющая уровень облачной защиты, специально предназначенный для устранения невиданных ранее угроз.

Если эта функция включена, подозрительные образцы, которые еще не подтверждены как вредоносные, но могут содержать вредоносные программы, будут автоматически отправляться в облако ESET. Отправленные образцы запускаются в песочнице и оцениваются нашими передовыми модулями обнаружения вредоносных программ. Вредоносные образцы или сообщения электронной почты с подозрением на спам отправляются в ESET LiveGrid®. Вложения электронной почты обрабатываются отдельно и подлежат отправке в ESET LiveGuard. Вы можете определять, какие файлы отправляются, и период хранения файлов в облаке ESET. Документы и PDF-файлы с активным содержимым (макросы, сценарии javascript) по умолчанию не отправляются.

ESET LiveGuard можно включить или отключить в следующих разделах:

- Главное окно программы > **Настройка** > **Защита компьютера**
- Расширенные параметры > **Модуль обнаружения** > **Облачная защита**

Чтобы получить доступ к расширенным настройкам ESET LiveGuard, откройте Расширенные параметры > **Модуль обнаружения** > **Облачная защита** > **ESET LiveGuard**.

Действие по обнаружении: выбор действия, которое следует предпринять, если анализируемый образец оценивается как угроза.

Проактивная защита: разрешает или блокирует исполнение файлов, которые анализируются системой ESET LiveGuard. Если файл является подозрительным, проактивная защита блокирует его выполнение до завершения анализа. Проактивная защита обнаруживает файлы из следующих источников:

- файлы, загруженные с помощью поддерживаемого веб-браузера;
- загрузки из почтового клиента;
- файлы, извлеченные из незашифрованного или зашифрованного архива с помощью одной из поддерживаемых программ архивации;
- запускаемые и открываемые файлы, расположенные на съемных устройствах.

В таблице ниже перечислены поддерживаемые приложения.

Веб-браузеры	Почтовые клиенты	Программы архивации	Съемные устройства
Internet Explorer	Microsoft Outlook	WinRAR	USB-устройство флэш-памяти
Microsoft Edge	Mozilla Thunderbird	WinZIP	Жесткий диск с интерфейсом USB
Chrome	Microsoft Mail	Встроенный распаковщик проводника Microsoft	Компакт-/DVD-диск

Веб-браузеры	Почтовые клиенты	Программы архивации	Съемные устройства
Firefox		7zip	Дискета
Opera			Встроенное устройство чтения карт
Brave Браузер			

> **Примечание**
> Файлы, скопированные с помощью проводника Windows из исключенного расположения в защищенное расположение, блокируются проактивной защитой, поскольку решение ESET Security Ultimate считает `explorer.exe` программой архивации.

> Если для проактивной защиты задан параметр **Заблокировать исполнение до получения результата анализа**, а вы хотите разблокировать анализируемый файл, щелкните его правой кнопкой мыши и выберите **Разблокировать файл, проанализированный службой ESET LiveGuard**.

Максимальное время ожидания результатов анализа (мин): задает время, по истечении которого анализируемые файлы будут разблокированы независимо от того, завершен ли анализ.

ESET LiveGuard сообщает о состоянии анализа с помощью уведомлений. Ниже перечислены доступные уведомления.

Название уведомления	Описание
Файл заблокирован из-за анализа	Файл заблокирован системой ESET LiveGuard. ESET LiveGuard анализирует файл, чтобы гарантировать, что он безопасен для использования. Вы можете подождать или выбрать один из следующих вариантов. • **Разблокировать файл**: файл будет разблокирован, но анализ продолжится. Вы получите уведомление о результате. Этот вариант не рекомендуется, если вы не уверены в целостности файла. • **Изменить настройку**: откроется окно настройки защиты компьютера, в котором можно отключить систему ESET LiveGuard и ее проактивную защиту.
Файл разблокирован	Файл больше не заблокирован. Анализ продолжается, и вы получите уведомление о результате. Файл можно открывать.
Файл все еще на анализе	Системе ESET LiveGuard требуется больше времени для завершения анализа. При необходимости можно открыть файл.
Угроза удалена	Система ESET LiveGuard завершила анализ и определила, что файл содержал угрозу. Файл очищен.
Файл безопасен для использования	Система ESET LiveGuard завершила анализ и определила, что файл безопасен для использования.

Если ESET LiveGuard работает ненадлежащим образом, вы получите уведомление в главном окне программы > **Обзор**. Для устранения проблемы следуйте инструкциям в уведомлении. Если вам не удается решить проблему, обратитесь в службу технической поддержки.

Процессы сканирования вредоносных программ

В разделе Расширенные параметры > **Модуль обнаружения** > **Процессы сканирования вредоносных программ** можно настроить параметры сканирования для профилей сканирования.

Сканирование по требованию

Выбранный профиль – конкретный набор параметров, используемых сканером по запросу. Чтобы создать новый профиль, нажмите **Изменить** возле элемента **Список профилей**. Дополнительные сведения см. в разделе Профили сканирования.

После выбора профиля сканирования можно настроить следующие опции:

Объекты сканирования: чтобы просканировать определенный объект или группу объектов, щелкните **Изменить** рядом с параметром **Объекты сканирования** и выберите вариант в структуре папок (дерева). Дополнительные сведения см. в разделе Объекты сканирования.

Защита по требованию и на основе машинного обучения: можно настроить уровни отчетности и защиты для каждого профиля сканирования. По умолчанию профили сканирования используют настройки, указанные в разделе Защита файловой системы в реальном времени. Отключите переключатель рядом с элементом **Использовать настройки защиты в реальном времени** для настройки пользовательских уровней отчетности и защиты. Подробные сведения об уровнях отчетности и защиты см. в разделе Защита.

ThreatSense — расширенные параметры, например расширения файлов, которые нужно контролировать, и используемые методы обнаружения. Для получения дополнительных сведений см. раздел ThreatSense.

Профили сканирования

В ESET Security Ultimate есть четыре предварительно заданных профиля сканирования:

• **Интеллектуальное сканирование** — это профиль расширенного сканирования по умолчанию. Для профиля интеллектуального сканирования используется технология интеллектуальной оптимизации, исключающая файлы, которые во время предыдущего сканирования были определены как чистые и с того времени не изменялись. Это обеспечивает сокращение времени сканирования при минимальном влиянии на безопасность системы.

• **Сканирование через контекстное меню** — вы можете запустить в контекстном меню сканирование по требованию для любого файла. Профиль «Сканирование через контекстное меню» позволяет определить конфигурацию сканирования, которая будет использоваться при запуске сканирования таким способом.

• **Глубокое сканирование** — Для профиля глубокого сканирования интеллектуальная оптимизация по умолчанию не используется, поэтому при использовании этого профиля никакие файлы из сканирования не исключаются.

• **Сканирование компьютера** — этот профиль по умолчанию используется при стандартном сканировании компьютера.

Предпочтительные параметры сканирования можно сохранить для использования в дальнейшем. Рекомендуется создать отдельный профиль для каждого регулярно используемого сканирования (с различными объектами, методами сканирования и прочими параметрами).

Чтобы создать профиль, откройте раздел Расширенные параметры > **Модуль обнаружения** > **Процессы сканирования вредоносных программ** > **Сканирование по требованию** > **Список профилей** > **Изменить**. В окне **Диспетчер профилей** доступно раскрывающееся меню **Выбранный профиль** со списком существующих профилей сканирования и опцией для создания нового. Для создания профиля сканирования в соответствии с конкретными потребностями см. раздел ThreatSense, где описывается каждый параметр, используемый для настройки сканирования.

Предположим, вам требуется создать собственный профиль сканирования. Хотя конфигурация **Сканировать компьютер** частично подходит, сканировать программы-упаковщики или потенциально опасные приложения не требуется и нужно применить **Всегда исправлять обнаружение**. Введите имя нового профиля в окне **Диспетчер профилей** и нажмите кнопку **Добавить**. Выберите новый профиль в раскрывающемся меня **Выбранный профиль** и настройте остальные параметры в соответствии со своими требованиями, а затем нажмите кнопку **ОК**, чтобы сохранить новый профиль.

Объекты сканирования

В раскрывающемся меню **Объекты сканирования** можно выбрать предварительно определенные объекты сканирования.

• **По параметрам профиля**: выбираются объекты сканирования, указанные в выбранном профиле сканирования.
• **Сменные носители**: выбираются дискеты, USB-устройства хранения, компакт- и DVD-диски.

• **Жесткие диски**: выбираются все жесткие диски системы.

• **Сетевые диски**: выбираются все подключенные сетевые диски.

• **Пользовательский выбор**: отмена всех предыдущих выборов.

Структура папок (дерево) также содержит определенные объекты сканирования.

• **Оперативная память**: сканирование всех процессов и данных, которые в данный момент используются оперативной памятью.

• **Загрузочные секторы/UEFI**: сканирование загрузочных секторов и UEFI на наличие вредоносных программ. Дополнительные сведения о модуле сканирования UEFI приведены в глоссарии.

• **База данных WMI**: сканирование всей базы данных Windows Management Instrumentation (WMI), всех пространств имен, экземпляров классов и всех свойств. Поиск ссылок на зараженные файлы или вредоносные программы, внедренные в виде данных.

• **Системный реестр**: сканирование всего системного реестра, всех разделов и подразделов. Поиск ссылок на зараженные файлы или вредоносные программы, внедренные в виде данных. При очистке обнаружений ссылка остается в реестре во избежание потери каких-либо важных данных.

Чтобы быстро перейти к объекту сканирования (файлу или папке), введите его путь в текстовом поле под древовидной структурой. Путь вводится с учетом регистра. Чтобы включить объект в сканирование, установите его флажок в древовидной структуре.

Сканирование в состоянии простоя

Вы можете разрешить сканирование в состоянии простоя, выбрав Расширенные параметры в меню **Модуль обнаружения**, а затем **Процессы сканирования вредоносных программ** > **Сканирование в состоянии простоя**.

Сканирование в состоянии простоя

Включите переключатель рядом с элементом **Включить сканирование в состоянии простоя**, чтобы включить эту функцию. Когда компьютер находится в состоянии простоя, автоматически выполняется сканирование компьютера на всех жестких дисках.

По умолчанию сканирование в состоянии простоя не работает, если компьютер (ноутбук) работает от батареи. Этот параметр можно изменить, включив ползунок рядом с элементом **Сканировать даже в случае работы компьютера от аккумулятора** в разделе «Расширенные параметры».

В дополнительных настройках выберите параметр **Включить ведение журналов**, чтобы результаты сканирования компьютера регистрировались в разделе Файлы журналов (в главном окне программы перейдите в **Служебные программы** > **Файлы журналов** и выберите **Сканирование компьютера** в раскрывающемся меню **Журнал**).

Сканирование в состоянии простоя

Полный список условий для запуска сканирования в состоянии простоя см. в разделе Сканирование в состоянии простоя.

ThreatSense — расширенные параметры, например расширения файлов, которые нужно контролировать, и используемые методы обнаружения. Дополнительные сведения см. в разделе ThreatSense.

Сканирование в состоянии простоя

Настройки сканирования в состоянии простоя можно изменить в меню Расширенные параметры > **Модуль обнаружения** > **Процессы сканирования вредоносных программ** > **Сканирование в состоянии простоя** > **Сканирование в состоянии простоя**. Эти параметры позволяют указать условие запуска обнаружения в состоянии простоя, например:

- **Выключенный экран или заставка**

- **блокировка компьютера;**
- **Выход пользователя**

Используйте флажки для каждого состояния, чтобы включить или отключить различные условия обнаружения в состоянии простоя.

сканирование при запуске

При загрузке компьютера и обновлении модуля обнаружения автоматически проверяются файлы, исполняемые при запуске системы. Это сканирование зависит от конфигурации и задач планировщика.

Сканирование файлов, исполняемых при запуске системы, входит в задачу планировщика **Проверка файлов, исполняемых при запуске системы**. Для изменения ее настроек перейдите в раздел **Инструменты** > **Планировщик**, щелкните элемент **Автоматическая проверка файлов при запуске системы**, а затем — **Изменить**. На последнем этапе отобразится окно Автоматическая проверка файлов при запуске системы. Более подробные инструкции по созданию задач в планировщике и управлению ими см. в разделе Создание новой задачи.

ThreatSense — расширенные параметры, например расширения файлов, которые нужно контролировать, и используемые методы обнаружения. Дополнительные сведения см. в разделе ThreatSense.

Автоматическая проверка файлов при запуске системы

При создании запланированной задачи «Проверка файлов, исполняемых при запуске системы» предоставляется несколько вариантов настройки следующих параметров.

В раскрывающемся меню **Объекты сканирования** указывается глубина сканирования файлов, исполняемых при запуске системы. Сканирование выполняется на основе секретного сложного алгоритма. Файлы упорядочены по убыванию в соответствии со следующими критериями.

- **Все зарегистрированные типы файлов** (наибольшее количество сканируемых файлов)
- **Редко используемые файлы**
- **Обычно используемые файлы**
- **Часто используемые файлы**
- **Только наиболее часто используемые файлы** (наименьшее количество сканируемых файлов)

Также существуют две особые группы.

- **Файлы, которые запускаются перед входом пользователя**: содержит файлы из таких папок, которые можно открыть без входа пользователя в систему (в том числе

большинство элементов, исполняемых при запуске системы: службы, объекты модуля поддержки браузера, уведомления Winlogon, задания в планировщике Windows, известные библиотеки DLL и т. д.).

• **Файлы, запускающиеся после входа пользователя**: содержит файлы из таких папок, которые можно открыть только после входа пользователя в систему (в том числе файлы, запускаемые под конкретными учетными записями: обычно файлы из папки *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Списки файлов, которые нужно просканировать, являются фиксированными для каждой вышеприведенной группы. Если выбрать меньшую глубину сканирования для файлов, исполняемых при запуске системы, файлы, которые не были просканированы, будут сканироваться при открытии или исполнении.

Приоритет сканирования: уровень приоритетности, используемый для определения условий начала сканирования.

• **При бездействии**: задача будет выполняться только при бездействии системы.

• **Самый низкий**: минимальная нагрузка на систему.

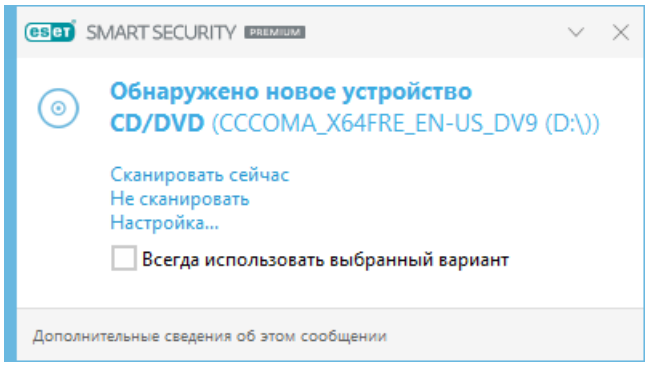
• **Более низкий**: низкая нагрузка на систему.

• **Средний**: средняя нагрузка на систему.

Съемные носители

ESET Security Ultimate обеспечивает автоматическое сканирование съемных носителей (компакт- и DVD-дисков, USB-устройств и т. п.) при их подключении к компьютеру. Это может быть удобно, если администратор компьютера хочет предотвратить подключение пользователями съемных носителей с нежелательным содержимым.

Если в разделе Расширенные параметры > **Модуль обнаружения** > **Процессы сканирования вредоносных программ** > **Съемные носители** включен параметр **Показать параметры сканирования**, то при подключении съемного носителя отображается следующее диалоговое окно:



Параметры этого диалогового окна:

• **Сканировать сейчас**: запуск сканирования съемного носителя.

• **Не сканировать**: съемные носители сканироваться не будут.

• **Настройка**: вызов расширенных параметры.

• **Всегда использовать выбранный вариант**: если установить этот флажок, выбранное действие будет выполняться каждый раз, когда вставляется съемный носитель.

Кроме того, в ESET Security Ultimate есть модуль контроля устройств, дающий возможность задавать правила использования внешних устройств на указанном компьютере. Дополнительные сведения об этом модуле см. в разделе Контроль устройств.

Чтобы изменить настройки сканирования съемных носителей, последовательно выберите элементы Расширенные параметры > **Модуль обнаружения** > **Процессы сканирования вредоносных программ** > **Съемные носители**.

Действие, которое следует предпринять после подключения съемного носителя: выбор действия по умолчанию, которое выполняется при подключении съемного носителя (компакт-диска, DVD-диска, USB-устройства) к компьютеру. Выберите действие, которое нужно выполнять при подключении съемного носителя к компьютеру.

• **Не сканировать**: действия не будут выполняться, окно **Обнаружено новое устройство** открываться не будет.

• **Автоматическое сканирование устройств**: выполняется сканирование подключенного к компьютеру съемного носителя.

• **Показать параметры сканирования**: переход в раздел, где настраиваются действия со **съемными носителями**.

Защита документов

Функция защиты документов сканирует документы Microsoft Office перед их открытием, а также проверяет файлы, автоматически загружаемые браузером Internet Explorer, такие как элементы Microsoft ActiveX. Функция защиты документов обеспечивает безопасность в дополнение к функции защиты файловой системы в реальном времени. Ее можно отключить, чтобы улучшить производительность систем, которые не содержат большое количество документов Microsoft Office.

Чтобы активировать функцию защиты документов, откройте Расширенные параметры () > **Модуль обнаружения** > **Процессы сканирования вредоносных программ** > **Защита документов** и щелкните ползунок рядом с элементом **Включить защиту документов**.

ThreatSense — расширенные параметры, например расширения файлов, которые нужно контролировать, и используемые методы обнаружения. Дополнительные сведения см. в разделе ThreatSense.

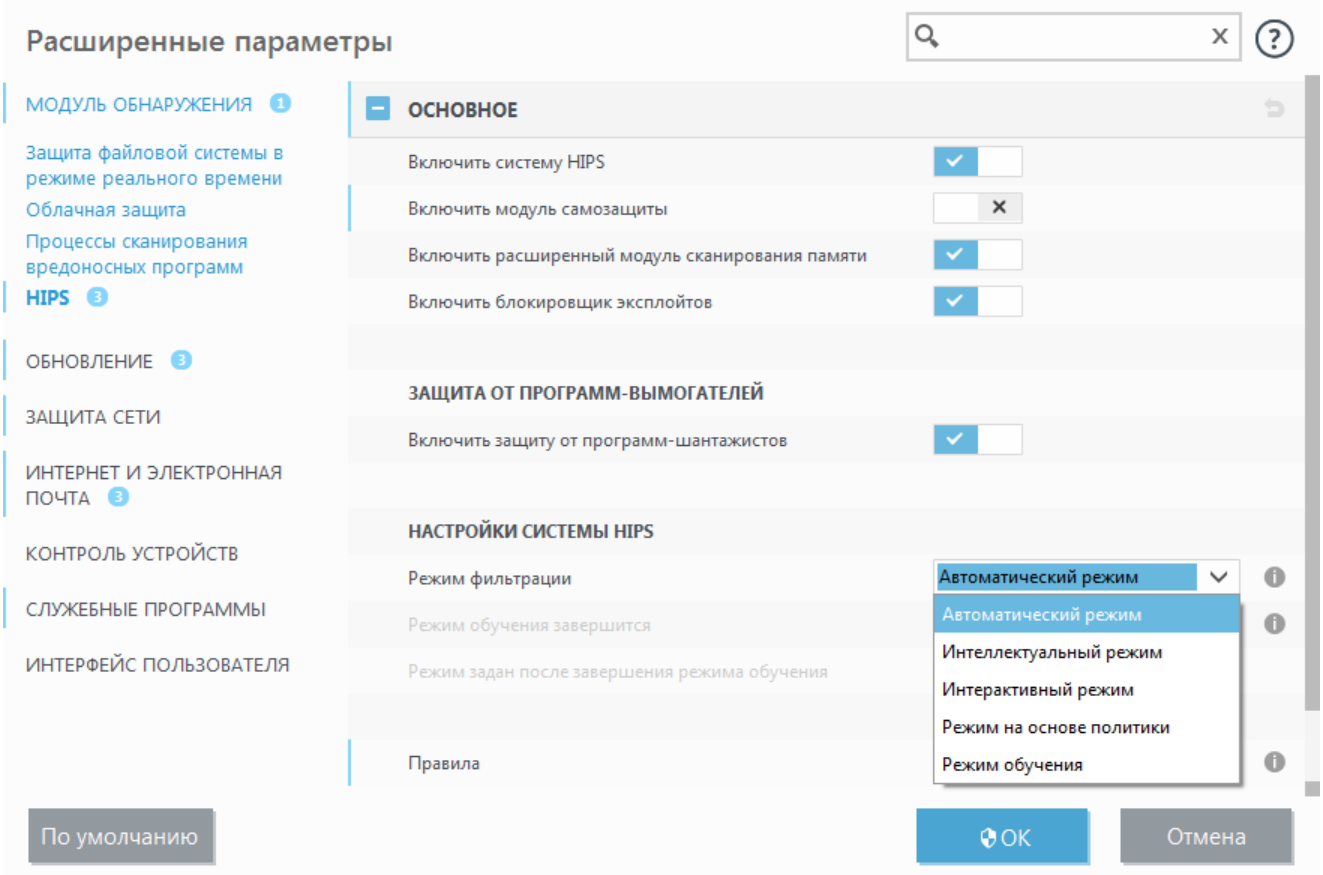
> Эта функция активируется приложениями, в которых используется Microsoft Antivirus API (например, Microsoft Office 2000 и более поздних версий или Microsoft Internet Explorer 5.0 и более поздних версий).

Система HIPS

Изменения в параметры системы HIPS должны вносить только опытные пользователи. Неправильная настройка этих параметров может привести к нестабильной работе системы.

Система предотвращения вторжений на узел (HIPS) защищает от вредоносных программ и другой нежелательной активности, которые пытаются отрицательно повлиять на безопасность компьютера. В системе предотвращения вторжений на узел используется расширенный анализ поведения в сочетании с возможностями сетевой фильтрации по обнаружению, благодаря чему отслеживаются запущенные процессы, файлы и разделы реестра. Система предотвращения вторжений на узел отличается от защиты файловой системы в режиме реального времени и не является файерволом; она только отслеживает процессы, запущенные в операционной системе.

Параметры системы HIPS можно настроить в разделе Расширенные параметры > **Модуль обнаружения** > **Система HIPS** > **Система HIPS**. Состояние HIPS (включено/отключено) отображается в главном окне программы ESET Security Ultimate, в разделе **Настройка** > **Защита компьютера**.



Система HIPS

Включить систему HIPS. В ESET Security Ultimate система HIPS включена по умолчанию. Отключение системы HIPS приведет к отключению ее функций, Блокировщика эксплойтов.

Включить модуль самозащиты — В ESET Security Ultimate используется встроенная в систему

HIPS технология **самозащиты**, которая не позволяет вредоносным программам повредить или отключить защиту от вирусов и шпионских программ. Модуль самозащиты обеспечивает защиту самых важных процессов системы и программы ESET, разделов реестра и файлов от вмешательства.

Включить защищенную службу — Включается защита службы ESET (ekrn.exe). Если параметр включен, служба запускается в виде защищенного процесса Windows для защиты от атак вредоносных программ.

Включить расширенный модуль сканирования памяти работает в сочетании с блокировщиком эксплойтов для усиления защиты от вредоносных программ, которые могут избегать обнаружения продуктами для защиты от вредоносных программ за счет использования умышленного запутывания или шифрования. Расширенный модуль сканирования памяти по умолчанию включен. Дополнительную информацию об этом типе защиты см. в глоссарии.

Блокировщик эксплойтов предназначен для защиты приложений, которые обычно уязвимы для эксплойтов, например браузеров, программ для чтения PDF-файлов, почтовых клиентов и компонентов MS Office. Блокировщик эксплойтов по умолчанию включен. Дополнительную информацию об этом типе защиты см. в глоссарии.

Глубокая поведенческая проверка

Включить глубокую поведенческую проверку — это еще один уровень защиты, используемый системой HIPS. Это расширение системы HIPS анализирует поведение всех программ, запущенных на компьютере, и предупреждает вас, если процесс ведет себя, как вредоносный.

Исключения системы HIPS из глубокой поведенческой проверки позволяют исключить из анализа определенные процессы. Чтобы обеспечить сканирование всех процессов на наличие угроз, рекомендуется создавать исключения только в случае крайней необходимости.

Защита от программ-шантажистов

Защита от программ-шантажистов: это еще один уровень защиты, функционирующий как компонент системы HIPS. Для работы модуля защиты от программ-шантажистов необходимо, чтобы система репутации ESET LiveGrid® была включена. Дополнительную информацию об этом типе защиты.

Включить Intel® Threat Detection Technology: помогает обнаруживать атаки программ-вымогателей, используя уникальную телеметрию процессора Intel для повышения эффективности обнаружения, уменьшения количества ложных предупреждений об угрозах и расширения возможностей противодействия передовым методам уклонения от обнаружения. См. информацию о поддерживаемых процессорах.

Настройки системы HIPS

Режим фильтрации можно выполнять в одном из следующих режимов:

Режим фильтрации	Описание
Автоматический режим	Включены все операции за исключением тех, которые заблокированы предварительно заданными правилами, защищающими компьютер.
Интеллектуальный режим	Пользователь будет получать уведомления только об очень подозрительных событиях.
Интерактивный режим	Пользователь будет получать запросы на подтверждение операций.
Режим на основе политики	блокируются все операции, кроме тех, что разрешены определенным правилом.
Режим обучения	Операции включены, и после каждой операции создается правило. Правила, создаваемые в таком режиме, можно просмотреть в редакторе **Правила HIPS**, но их приоритет ниже, чем у правил, создаваемых вручную или в автоматическом режиме. При выборе элемента **Режим обучения** в раскрывающемся меню **Режим фильтрации** становится доступным параметр **Режим обучения завершится**. Выберите длительность для режима обучения. Максимальная длительность — 14 дней. Когда указанный период завершится, вам будет предложено изменить правила, созданные системой HIPS в режиме обучения. Кроме того, вы можете выбрать другой режим фильтрации или отложить решение и продолжить использовать режим обучения.

Режим задан после завершения режима обучения. Выберите этот режим фильтрации, который будет действовать по окончании использования режима обучения. Чтобы после завершения режима обучения изменить режим фильтрация HIPS на **Спросить пользователя**, нужны права администратора.

Система HIPS отслеживает события в операционной системе и реагирует на них соответствующим образом на основе правил, которые аналогичны правилам файервола. Нажмите кнопку **Настроить** рядом с элементом **Правила**, чтобы открыть редактор **правил системы HIPS**. В этом окне можно выбирать, создавать, изменять и удалять правила. Дополнительные сведения о создании правил и операциях системы HIPS см. в разделе Изменение правила системы предотвращения вторжений на узел.

Исключения системы HIPS

С помощью исключений можно исключать процессы из глубокой поведенческой проверки системы HIPS.

Чтобы изменить исключения системы HIPS, откройте раздел Расширенные параметры > **Модуль обнаружения** > **Система HIPS** > **Система HIPS** > **Исключения** > **Изменить**.

> Не следует путать эту функцию с другими возможностями исключения — Исключенные расширения файлов, Исключения из обнаружения, Исключения для быстродействия или Исключения для процессов.

Чтобы исключить объект, щелкните **Добавить** и введите путь к объекту или выделите его в древовидной структуре. Выбранные записи также можно изменять и удалить.

Расширенные параметры HIPS

Перечисленные далее параметры полезны для отладки и анализа поведения приложения.

Драйверы, загрузка которых разрешена всегда: загрузка выбранных драйверов разрешена всегда, независимо от настроенного режима фильтрации, если они не заблокированы в явном виде правилом пользователя.

Регистрировать все заблокированные операции: все заблокированные операции будут записываться в журнал HIPS. Используйте эту функцию только при устранении неполадок или по запросу службы технической поддержки ESET, так как она может создать очень большой файл журнала и замедлить работу компьютера.

Сообщать об изменениях приложений, загружаемых при запуске системы: при добавлении или удалении приложения, загружаемого при запуске системы, на рабочем столе отображается уведомление.

Драйверы, загрузка которых разрешена всегда

Загрузка драйверов, отображенных в этом списке, разрешена всегда вне зависимости от режима фильтрации HIPS. Это не касается случаев, когда загрузка драйвера явным образом заблокирована правилом пользователя.

Добавить: добавление нового драйвера.

Изменить: изменение выбранного драйвера.

Удалить: удаление драйвера из списка.

Сброс: перезагрузка системных драйверов.

Если щелкнуть элемент **Сброс**, драйверы, добавленные вручную, будут удалены из списка. Это может пригодиться, если вы добавили несколько драйверов и не можете удалить их из списка вручную.

После установки список драйверов пуст. ESET Security Ultimate заполняет список автоматически с течением времени.

Интерактивное окно HIPS

В окне уведомлений HIPS можно создать правило на основе новых действий, обнаруженных системой HIPS, и определить условия, при которых такое действие будет разрешено или запрещено.

Правила, создаваемые в окне уведомлений, считаются равнозначными правилам, созданным вручную. Правило, созданное в окне уведомлений, может быть менее подробным, чем правило, которое вызвало появление этого диалогового окна. Это значит, что после создания такого

правила в диалоговом окне эта же операция может вызвать появление такого же окна. Дополнительные сведения см. в разделе Приоритетность для правил HIPS.

Если для правила по умолчанию установлено действие **Спрашивать каждый раз**, то при каждом запуске правила будет отображаться диалоговое окно. Для операции также можно выбрать другие действия: **Запретить** или **Разрешить**. Если пользователь не выбирает действие в течение определенного времени, на основе правил выбирается новое действие.

Выбор параметра **Запомнить до закрытия приложения** приводит к использованию действия (**Разрешить/Запретить**) до тех пор, пока не будут изменены правила или режимы фильтрации, не будет обновлен модуль системы HIPS или не будет выполнена перезагрузка компьютера. После выполнения любого из этих трех действий временные правила удаляются.

Если выбрать параметр **Создать правило и запомнить навсегда**, будет создано новое правило HIPS, которое позже можно изменить в разделе Управление правилами HIPS (нужны права администратора).

Внизу щелкните **Сведения**, чтобы узнать, какое приложение запускает операцию, какова репутация файла и какую операцию нужно разрешить или запретить.

Чтобы установить параметры правила более детально, щелкните **Расширенные параметры**. Если выбран параметр **Создать правило и запомнить навсегда**, доступны перечисленные ниже варианты.

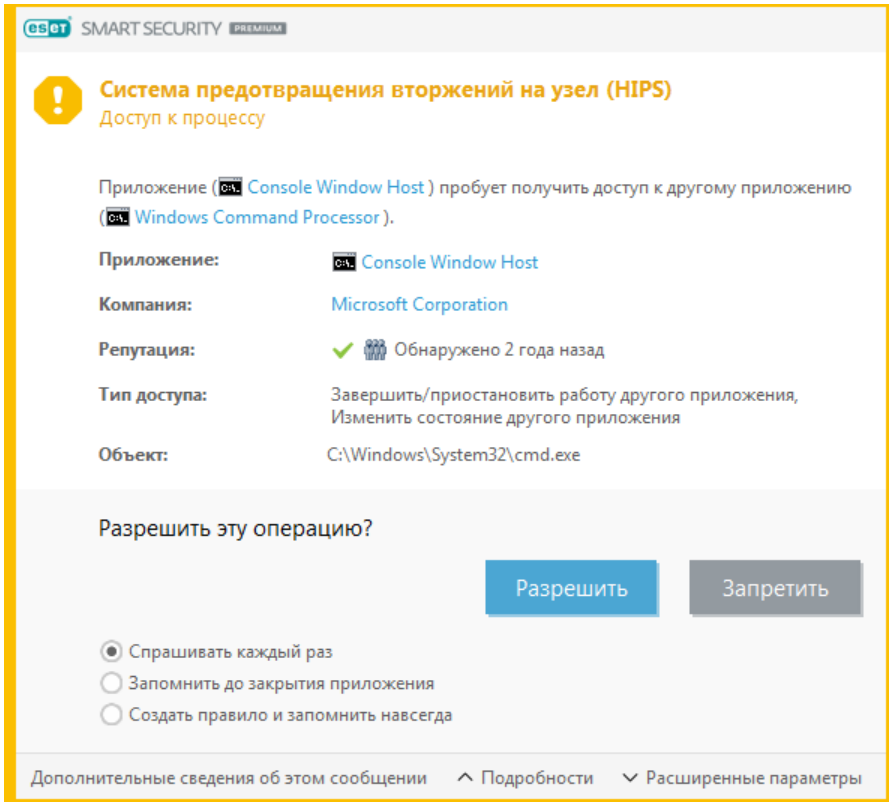
- **Создать правило, действительное только для этого приложения**. Если установлен этот флажок, правило будет создано для всех исходных приложений.

- **Только для операции**. Выберите операции для файла, приложения или реестра правила. См. описания всех операций HIPS.

- **Только для цели**. Выберите целевые объекты для файла, приложения или реестра правила.

Постоянно появляются уведомления HIPS?

Чтобы уведомления не отображались, установите **автоматический** режим фильтрации в разделе Расширенные параметры > **Модуль обнаружения** > **Система HIPS** > **Система HIPS**.



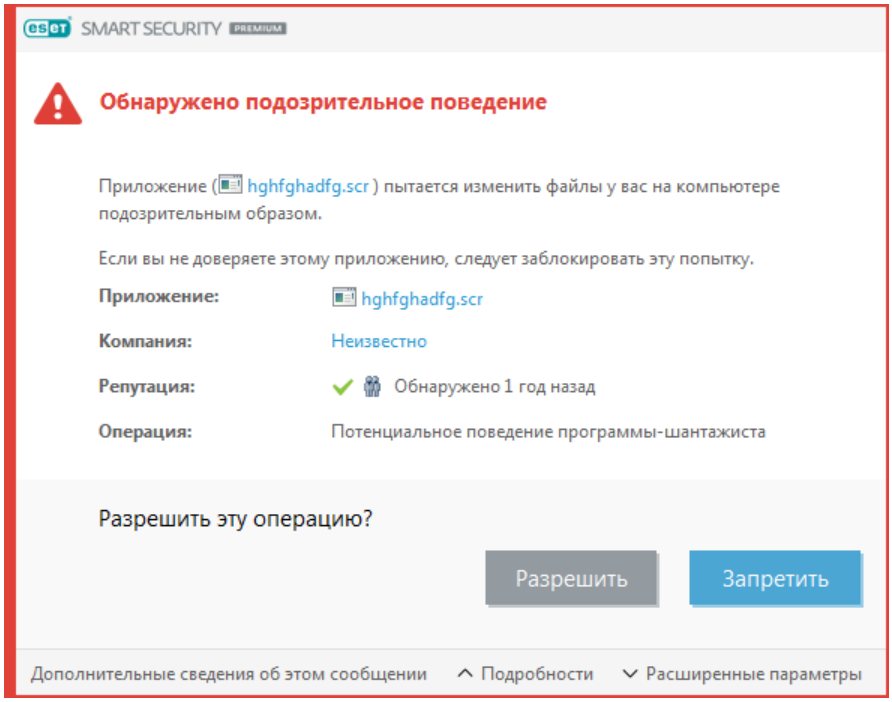
Режим обучения завершен

Режим обучения автоматически создает и сохраняет правила. Проверить все созданные правила можно в настройках правил системы HIPS. Этот режим лучше всего использовать для первоначальной настройки системы HIPS, и он должен быть включен только в течение короткого времени. Участие пользователя не требуется, потому что ESET Security Ultimate сохраняет правила согласно предварительно настроенным параметрам. Во избежание угроз безопасности переключитесь на **интерактивный режим** или **режим на основе политики** после того, как будут созданы все правила для необходимых процессов, выполняемых в операционной системе.

Вы можете отложить это решение, если не хотите менять настройки.

Потенциальное поведение Программ-вымогателей обнаружено

При обнаружении потенциального поведения, характерного для программы-шантажиста, отображается диалоговое окно. Для операции также можно выбрать другие действия: **Запретить** или **Разрешить**.



Щелкните **Сведения**, чтобы просмотреть конкретные параметры обнаружения. В этом диалоговом окне можно выбрать **Передать на анализ** или **Исключить из проверки**.

Для правильной работы модуля защиты от программ-вымогателей система ESET LiveGrid® должна быть включена.

Управление правилами HIPS

Список созданных пользователем и добавленных автоматически правил из системы HIPS. Дополнительные сведения о создании правил и операциях системы HIPS приводятся в главе Параметры правил HIPS. См. также Общие принципы работы системы HIPS.

Столбцы

Правило: указанное пользователем или автоматически выбранное имя правила.

Включено: отключите этот ползунок, чтобы оставить правило в списке, но при этом не использовать его.

Действие: правило задает действие (**Разрешить**, **Блокировать** или **Запросить**), которое должно быть выполнено при соблюдении условий.

Исходные объекты: правило будет использоваться только в том случае, если событие вызывается этими приложениями.

Целевые объекты: правило будет использоваться, только если операция связана с определенным файлом, приложением или записью реестра.

Серьезность регистрируемых событий: если активировать этот параметр, информация об указанном правиле будет записываться в журнал HIPS.

Уведомить: если запускается событие, в правом нижнем углу экрана отображается

небольшое окно уведомления.

Элементы управления

Добавить: создание правила.

Изменить: изменение выделенных записей.

Удалить. Удаление выбранных записей.

Приоритетность для правил HIPS

Настройка уровня приоритета для правил системы HIPS с помощью кнопок «В начало» и «В конец» (как в разделе Правила файервола, где правила последовательно выполняются сверху вниз) не предусмотрена.

- Все правила, которые вы создаете, имеют одинаковый приоритет.
- Чем более подробное правило, тем выше его приоритет (например, правило для конкретного приложения имеет более высокий приоритет, чем правило для всех приложений).
- Система HIPS содержит внутренние правила с более высоким приоритетом, которые недоступны пользователю (например, нельзя переопределить правила самозащиты).
- Созданное пользователем правило, которое может заморозить работу операционной системы, не применяется (имеет самый низкий приоритет).

Изменение правила HIPS

Сначала см. Управление правилами HIPS.

Имя правила: указанное пользователем или автоматически выбранное имя правила.

Действие: правило задает действие (**Разрешить**, **Блокировать** или **Запросить**), которое должно быть выполнено при соблюдении условий.

Операции влияния: выберите тип операции, к которому будет применяться правило. Правило будет использоваться только для этого типа операции и для выбранного объекта.

Включено: отключите этот переключатель, если правило нужно оставить в списке, но при этом не применять его.

Серьезность регистрируемых событий: если активировать этот параметр, информация об указанном правиле будет записываться в журнал HIPS.

Уведомить пользователя: если запускается событие, в правом нижнем углу отображается небольшое окно уведомления.

Правило состоит из частей, в которых описываются условия выполнения правила.

Исходные приложения: правило будет использоваться только в том случае, если событие вызывается этими приложениями. Выберите пункт **Определенные приложения** в раскрывающемся меню и нажмите кнопку **Добавить**, чтобы добавить новые файлы, или выберите пункт **Все приложения**, чтобы добавить все приложения.

Целевые файлы: это правило будет использоваться, только если операция относится к данному целевому объекту. Выберите пункт **Определенные файлы** в раскрывающемся меню и щелкните **Добавить**, чтобы добавить новые файлы или папки, или выберите пункт **Все файлы**, чтобы добавить все файлы.

Приложения: это правило будет использоваться, только если операция относится к данному целевому объекту. Выберите пункт **Определенные приложения** в раскрывающемся меню и нажмите кнопку **Добавить**, чтобы добавить новые файлы или папки, или выберите пункт **Все приложения**, чтобы добавить все приложения.

Записи реестра: это правило будет использоваться, только если операция относится к данному целевому объекту. Выберите в раскрывающемся списке пункт **Определенные записи** и нажмите кнопку**Добавить** для ввода вручную или кнопку **Открыть редактор реестра** для выбора параметра в реестре. Можно также выбрать в раскрывающемся списке пункт **Все записи**, чтобы добавить все приложения.

> Некоторые операции определенных правил, предварительно заданных системой HIPS, невозможно заблокировать, они разрешены по умолчанию. Кроме того, не все системные операции отслеживаются системой HIPS. Система HIPS отслеживает операции, которые могут считаться небезопасными.

Описание важных операций

Операции с файлами

• **Удалить файл**: приложение запрашивает разрешение на удаление целевого файла.

• **Выполнить запись в файл**: приложение запрашивает разрешение на запись в целевой файл.

• **Непосредственный доступ к диску**: приложение пытается выполнить чтение с диска или запись на диск нестандартным образом, в обход стандартных алгоритмов Windows. Это может привести к изменению файлов без применения соответствующих правил. Такая операция может выполняться вредоносной программой, пытающейся избежать обнаружения, или же программным обеспечением для резервного копирования, которое пытается создать точную копию диска, либо диспетчером разделов, пытающимся реорганизовать тома диска.

• **Установить глобальную ловушку**: вызов функции SetWindowsHookEx из библиотеки MSDN.

• **Загрузить драйвер**: загрузка и установка драйверов в системе.

Операции с приложениями

• **Выполнить отладку другого приложения**: прикрепление отладчика к процессу. При отладке приложения можно просмотреть и изменить многие сведения о его поведении и

получить доступ к его данным.

• **Перехватывать события другого приложения**: исходное приложение пытается записать события, направленные на другое приложение (например, клавиатурный шпион, пытающийся записать события браузера).

• **Завершить/приостановить работу другого приложения**: приостановка, возобновление или завершение процесса (можно получить доступ непосредственно из обозревателя процессов или панели «Процессы»).

• **Запустить новое приложение**: запуск новых приложений или процессов.

• **Изменить состояние другого приложения**: исходное приложение пытается осуществить запись в память целевого приложения или выполнить код от его имени. Эта функциональность может быть полезна для защиты важного приложения путем его настройки как целевого в правиле, блокирующем использование данной операции.

Операции с реестром

• **Изменить параметры запуска**: любые изменения параметров, которые определяют, какие приложения будут выполнены при запуске ОС Windows. Их можно найти, например, выполнив поиск раздела Run в реестре Windows.

• **Удалить из реестра**: удаление раздела реестра или его значения.

• **Переименовать раздел реестра**: переименование разделов реестра.

• **Изменить реестр**: создание новых значений разделов реестра, изменение существующих значений, перемещение данных в древовидной структуре базы данных или настройка прав пользователя или группы для разделов реестра.

При вводе объекта можно использовать подстановочные знаки с определенными ограничениями. Вместо конкретного раздела в пути реестра можно использовать символ звездочки («*»). Например, *HKEY_USERS*\software* может означать *HKEY_USER\.default\software*, но не *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*. *HKEY_LOCAL_MACHINE\system\ControlSet** не является допустимым путем раздела реестра. Путь, в котором содержится сочетание символов «*», означает «этот путь или любой путь на любом уровне после этого символа». Это единственный способ, которым можно использовать подстановочные знаки, для объектов файлов. Сначала оценивается точный путь, а затем путь после подстановочного знака (*).

Если созданное правило будет слишком общим, появится соответствующее предупреждение.

В следующем примере будет показано, как ограничить нежелательное поведение конкретного приложения.

1. Присвойте правилу имя и выберите **Блокировать** (или **Запросить**, если вы хотите выбрать действие позже) в раскрывающемся меню **Действие**.

2. Активируйте переключатель **Уведомить пользователя**, чтобы уведомление отображалось при каждом применении правила.

3. Выберите хотя бы одну операцию в разделе **Операции влияния**, для которой будет применяться правило.

4. Щелкните **Далее**.

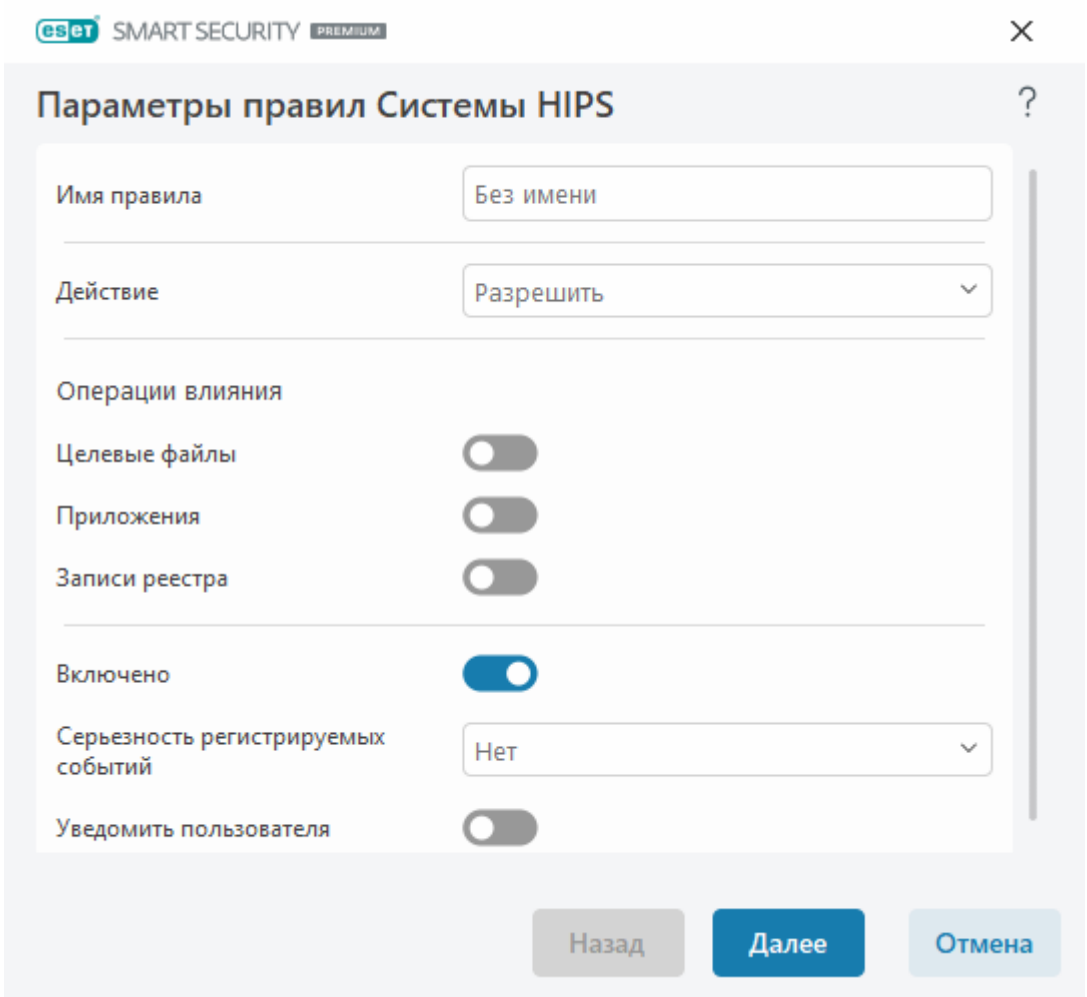
5. В окне **Исходные приложения** выберите в раскрывающемся списке вариант **Определенные приложения**. Новое правило будет применяться ко всем приложениям, которые будут пытаться выполнить любое из выбранных действий с указанными приложениями.

6. Нажмите кнопку **Добавить** и **...**, чтобы выбрать путь к определенному приложению. Затем нажмите кнопку **ОК**. При необходимости добавьте дополнительные приложения.
Например: *C:\Program Files (x86)\Untrusted application\application.exe*

7. Выберите операцию **Выполнить запись в файл**.

8. Выберите **Все файлы** в раскрывающемся меню. Это позволит заблокировать все попытки записи в файлы приложениями, которые были выбраны на предыдущем шаге.

9. Нажмите кнопку **Готово**, чтобы сохранить новое правило.



Добавление пути к приложению или реестру для системы HIPS

Выберите путь к файлу приложения, нажав **...**. При выборе папки все расположенные в ней приложения будут включены.

Параметр **Открыть редактор реестра** запускает редактор реестра Windows (regedit). При добавлении пути реестра нужно правильно ввести расположение в поле **Значение**.

Примеры пути к файлу или реестру:

- *C:\Program Files\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

Обновление

Опции настройки обновления доступны в разделе Расширенные параметры > **Обновление**. В этом разделе указывается информация об источниках обновлений, таких как серверы обновлений и данные аутентификации для них.

Обновление

Текущий профиль обновления отображается в раскрывающемся меню **Выбрать профиль обновления по умолчанию**.

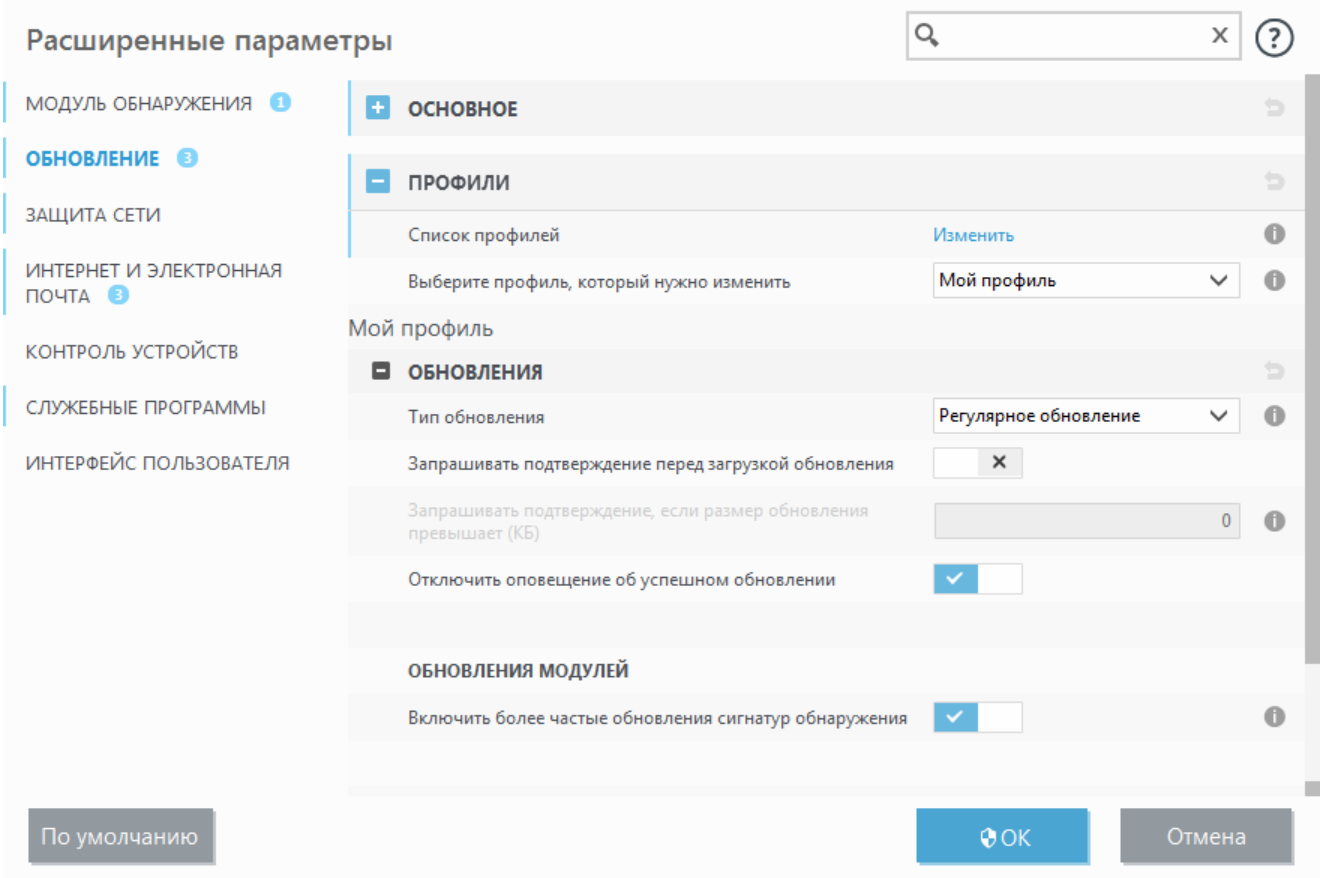
Чтобы создать профиль, см. сведения в разделе Профили обновления.

Автоматическое переключение профилей: позволяет назначить профиль обновления определенному профилю сетевого подключения.

Если во время загрузки обновлений модуля обнаружения возникли проблемы, рядом с параметром **Очистить кэш обновлений** щелкните **Очистить**, чтобы удалить временные файлы обновлений (очистить кэш).

Откат модулей

Если вы подозреваете, что последнее обновление модуля обнаружения и/или программных модулей повреждено или работает нестабильно, вы можете выполнить откат до предыдущей версии и отключить обновления на установленный период времени.



Для обеспечения правильной загрузки обновлений необходимо корректно задать все параметры обновлений. Если используется файервол, программе должно быть разрешено обмениваться данными через Интернет (например, передача данных по протоколу HTTP).

Профили

Профили обновления можно создавать для различных конфигураций и задач обновления. Создание профилей обновления особенно полезно для пользователей мобильных устройств, которым необходимо создать вспомогательный профиль для регулярно меняющихся свойств подключения к Интернету.

В раскрывающемся меню **Выберите профиль, который нужно изменить** отображается текущий профиль. По умолчанию для него задано значение **Мой профиль**. Чтобы создать профиль, рядом с элементом **Список профилей** щелкните **Изменить**, введите **имя профиля** и нажмите кнопку **Добавить**.

Обновления

По умолчанию для параметра **Тип обновлений** задано значение **Регулярное обновление**. Это означает, что файлы обновлений будут автоматически загружаться с сервера ESET с минимальным расходом трафика. Тестовые обновления (параметр **Тестовое обновление**) — это обновления, которые уже прошли полное внутреннее тестирование и в ближайшее время будут доступны всем пользователям. Преимущество их использования заключается в том, что у вас появляется доступ к новейшим методам обнаружения и исправлениям. Однако такие обновления иногда могут быть недостаточно стабильны и НЕ ДОЛЖНЫ использоваться на производственных серверах и рабочих станциях, где необходимы максимальные работоспособность и стабильность.

Запрашивать подтверждение перед загрузкой обновления: в программе отобразится уведомление, в котором можно подтвердить или отклонить загрузку файла обновления.

Запрашивать подтверждение, если размер обновления превышает (КБ): в программе отобразится диалоговое окно подтверждения, если размер файла обновления превышает заданное значение. Если размер файла обновления задан равным 0 КБ, диалоговое окно подтверждения в программе будет отображаться в любом случае.

Обновления модулей

Включить более частые обновления сигнатур обнаружения: будет уменьшен интервал обновления сигнатур обнаружения. Отключение этого параметра может негативно отразиться на скорости обнаружения.

Обновление программы

Обновления функций приложения — автоматическая установка новых версий ESET Security Ultimate.

Параметры подключения

Чтобы использовать прокси-сервер для загрузки обновлений, см. раздел Параметры подключения.

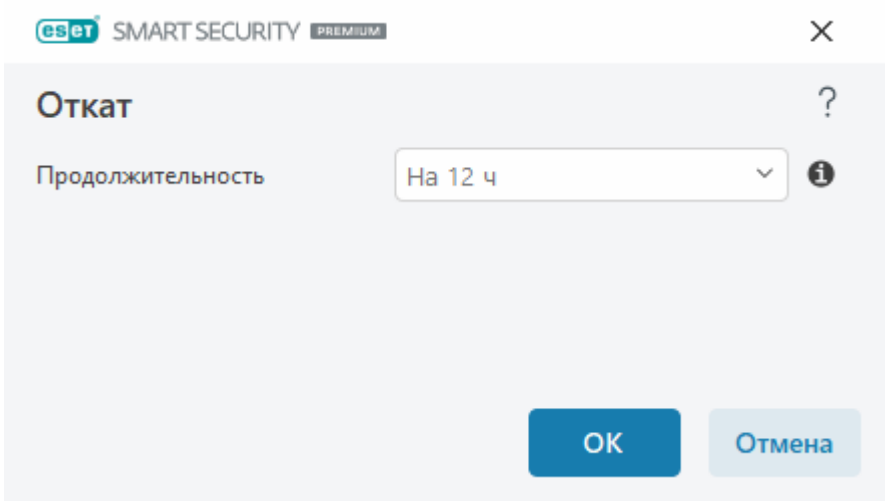
Откат обновления

Если вы подозреваете, что последнее обновление модуля обнаружения или новые модули программы повреждены или работают нестабильно, вы можете выполнить откат до предыдущей версии и временно отключить обновления. Или же можно включить ранее отключенные обновления, если они отложены на неопределенный период времени.

Программа ESET Security Ultimate создает снимки модуля обнаружения и модулей программы. Эти снимки используются функцией отката. Для создания снимков базы данных вирусов оставьте флажок **Создать снимки модулей** установленным. Когда флажок **Создать снимки модулей** установлен, первый снимок создается при первом обновлении. Следующий снимок создается через 48 часов. В поле **Количество локально хранимых снимков** указывается количество хранимых снимков модуля обнаружения.

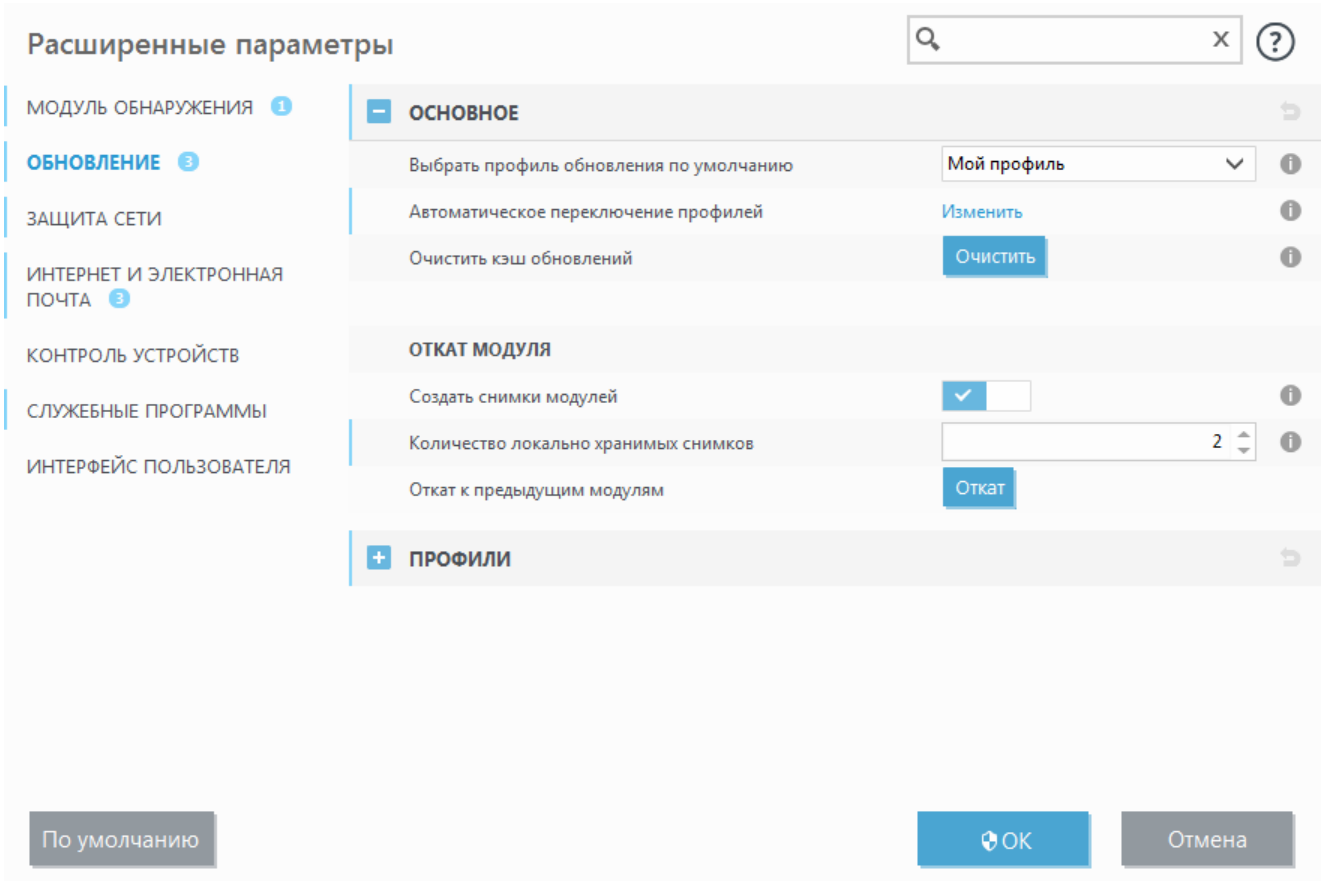
> Когда достигается максимальное количество снимков (например, три), самый старый снимок заменяется новым снимком каждые 48 часов. ESET Security Ultimate откатывает версии обновления модуля обнаружения и модуля программы до самого старого снимка.

После нажатия кнопки **Откатить** Расширенные параметры > **Обновление** > **Основная информация** нужно выбрать в раскрывающемся списке **Длительность** период времени, на который будет приостановлено обновление модуля обнаружения и программных модулей.



Выберите вариант **До отзыва**, чтобы отложить регулярные обновления на неопределенный период, пока функция обновления не будет восстановлена вручную. Поскольку это подвергает систему опасности, ESET не рекомендует использовать этот параметр.

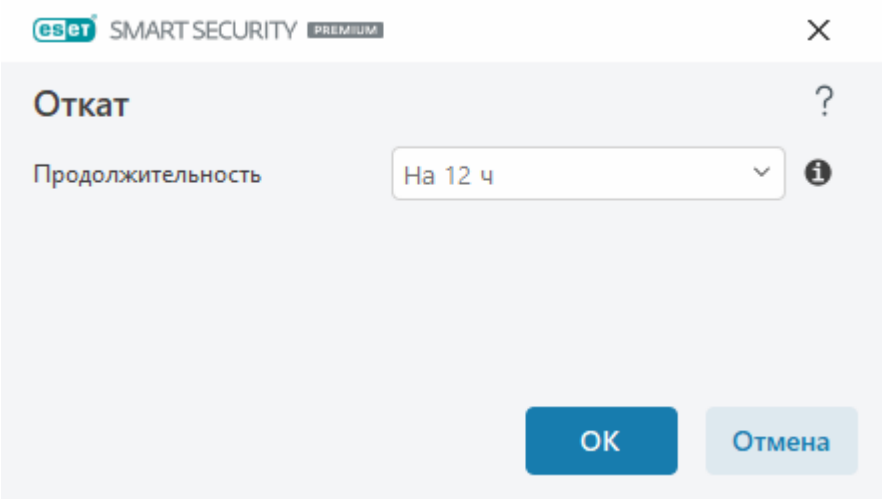
После отката кнопка **Откат** заменяется на **Разрешить обновления**. На протяжении периода, выбранного в раскрывающемся меню **Приостановить обновления**, обновления не производятся. Программа возвращается к самой старой версии модуля обнаружения, которая хранится в качестве снимка в файловой системе локального компьютера.



Предположим, последней версии модуля обнаружения присвоен номер 22700. Версии 22698 и 22696 хранятся в качестве снимков модуля обнаружения. Обратите внимание, что версия 22697 недоступна. В этом примере компьютер был выключен во время обновления 22697, и более новая версия обновления стала доступна до того, как была загружена версия 22697. Если в поле **Количество локально хранимых снимков** установлено значение 2 и пользователь щелкнет **Откат**, модуль обнаружения (включая модули программы) вернется к версии 22696. Это может занять некоторое время. Чтобы проверить, произведен ли откат до предыдущей версии модуля обнаружения, откройте окно Обновление.

Интервал времени отката

После нажатия кнопки **Откатить** Расширенные параметры > **Обновление** > **Основная информация** нужно выбрать в раскрывающемся списке **Длительность** период времени, на который будет приостановлено обновление модуля обнаружения и программных модулей.



Выберите вариант **До отзыва**, чтобы отложить регулярные обновления на неопределенный период, пока функция обновления не будет восстановлена вручную. Поскольку это подвергает систему опасности, ESET не рекомендует использовать этот параметр.

Обновление программы

В разделе **Обновления программы** можно автоматически устанавливать новые обновления функций, если они доступны.

Обновления функций приложения добавляют новые функции или изменяют уже существующие из предыдущих версий. Обновление может выполняться как в автоматическом режиме без вмешательства пользователя, так и с отображением уведомления для пользователя. После установки обновления функций приложения может потребоваться перезапуск компьютера.

Обновления функций приложения — если этот параметр включен, обновления функций приложения будут выполняться автоматически.

Параметры подключения

Чтобы получить доступ к опциям настройки прокси-сервера для определенного профиля обновления, откройте раздел Расширенные параметры > **Обновление** > **Профили** > **Обновления** > **Параметры подключения**. Откройте раскрывающееся меню **Режим прокси-сервера** и выберите один из трех перечисленных далее вариантов.

- Не использовать прокси-сервер
- Соединение через прокси-сервер
- Использовать общие параметры прокси-сервера

Выберите вариант **Использовать глобальные параметры прокси-сервера**, чтобы использовать конфигурацию прокси-сервера, уже заданную в разделе Расширенные параметры > **Подключение** > **Прокси-сервер**.

Выберите вариант **Не использовать прокси-сервер**, чтобы указать, что прокси-сервер не будет использоваться для обновления ESET Security Ultimate.

Флажок **Подключение через прокси-сервер** должен быть установлен в следующих случаях.

- Для обновления ESET Security Ultimate используется прокси-сервер, отличный от указанного в разделе Расширенные параметры > **Подключение**. При такой конфигурации нужно указать параметры нового прокси-сервера: адрес **прокси-сервера**, **порт передачи данных** (по умолчанию 3128), а также **имя пользователя** и **пароль** для прокси-сервера (если необходимо).
- Общие параметры прокси-сервера не заданы глобально, однако ESET Security Ultimate будет подключаться к прокси-серверу для получения обновлений.
- Компьютер подключается к Интернету через прокси-сервер. Параметры берутся из Internet Explorer в процессе установки программы, но при их изменении (например, при смене поставщика услуг Интернета) нужно убедиться в том, что указанные в этом окне параметры прокси-сервера верны. Если этого не сделать, программа не сможет подключаться к серверам обновлений.

По умолчанию установлен вариант **Использовать общие параметры прокси-сервера**.

Использовать прямое подключение, если прокси-сервер недоступен: прокси-сервер не будет использоваться при обновлении, если он недоступен.

> Поля **Имя пользователя** и **Пароль** в этом разделе относятся только к прокси-серверу. Заполняйте эти поля только в том случае, если для доступа к прокси-серверу требуются имя пользователя и пароль. Указанные поля следует заполнять только в том случае, если для подключения к Интернету через прокси-сервер нужен пароль.

Защита

Защита предотвращает вредоносные атаки на компьютер путем контроля файлов, электронной почты и связи через Интернет. Например, при обнаружении объекта, который классифицируется как «вредоносная программа» начнется процесс исправления. Функция защиты может устранить угрозу, сначала заблокировав его, а затем очистив, удалив или переместив в карантин.

Чтобы детально настроить защиту, откройте раздел Расширенные параметры > **Защита**.

Изменения в настройки защиты должны вносить только опытные пользователи. Неправильная настройка этих параметров может привести к снижению уровня защиты.

В этом разделе:

- Реагирование при обнаружении
- Настройка обнаружения
- Настройка защиты

Реагирование при обнаружении

В разделе «Реагирование при обнаружении» можно настроить уровни отчетности и защиты для следующих категорий:

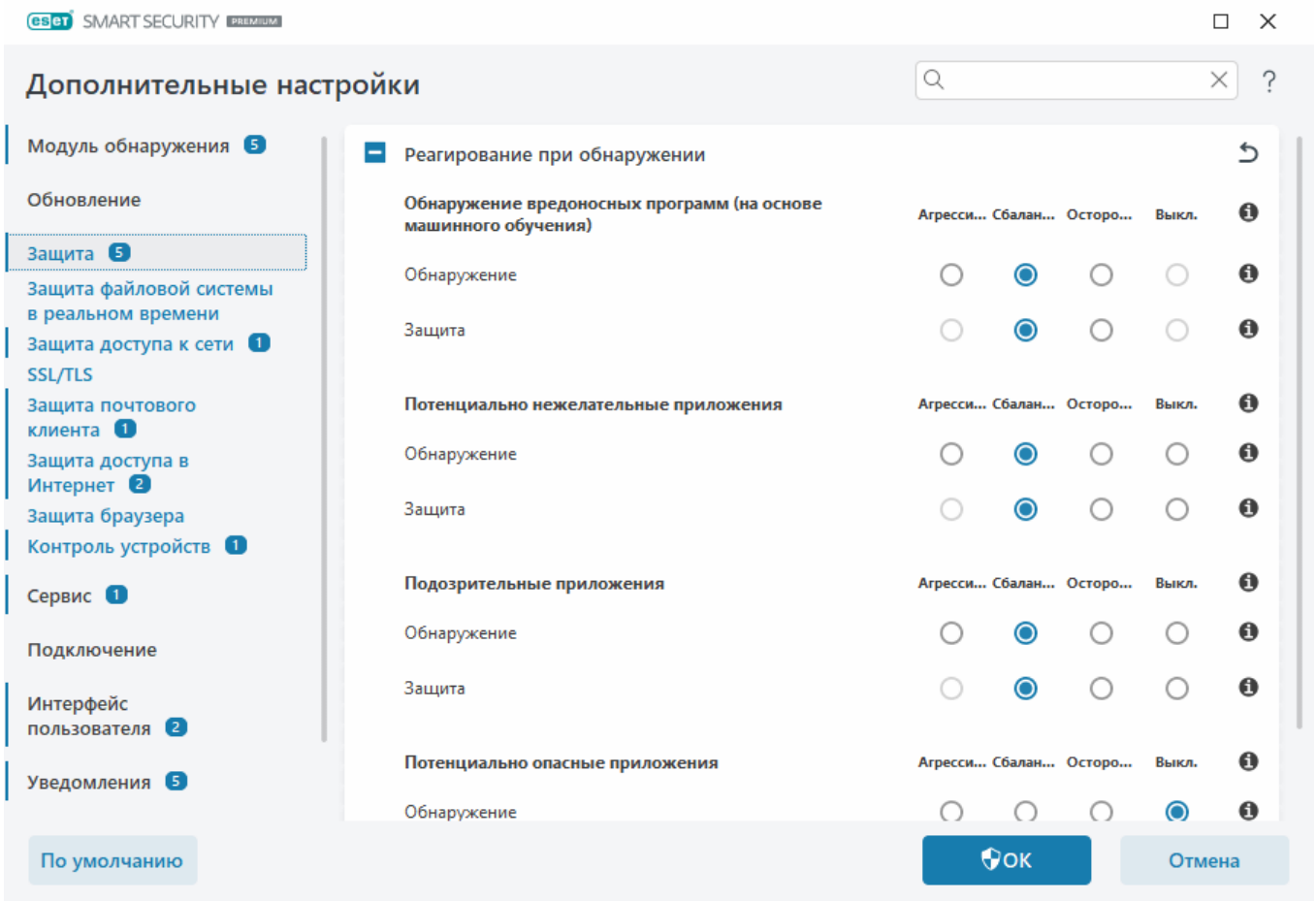
- **Обнаружение вредоносных программ (на основе машинного обучения)** – Компьютерный вирус — это фрагмент вредоносного кода, который добавляется в начало или конец файлов на компьютере. Тем не менее термин «вирус» часто используется не по назначению. Более точный термин — «вредоносная программа» («вредоносное ПО»). Обнаружение вредоносных программ осуществляется модулем обнаружения в сочетании с компонентом машинного обучения. Дополнительную информацию о приложениях этого типа см. в глоссарии.

- **Потенциально нежелательные приложения**. Потенциально нежелательные приложения представляют собой довольно широкую категорию программного обеспечения, задачей которого не является однозначно вредоносная деятельность в отличие от других типов вредоносных программ, таких как вирусы или троянские программы. Однако такое приложение может устанавливать дополнительное нежелательное программное обеспечение, изменять поведение цифрового устройства, а также выполнять действия без запроса или разрешения пользователя. Дополнительную информацию о приложениях этого типа см. в глоссарии.

- К **подозрительным приложениям** относятся программы, сжатые с помощью программ-упаковщиков или средств защиты. Средства защиты такого типа часто используются злоумышленниками, чтобы избежать обнаружения.

- **Потенциально опасные приложения**: это определение относится к законному коммерческому программному обеспечению, которое может быть использовано для

причинения вреда. К потенциально опасным приложениям относятся средства удаленного доступа, приложения для взлома паролей и клавиатурные шпионы (программы, регистрирующие каждое нажатие пользователем клавиш на клавиатуре). Дополнительную информацию о приложениях этого типа см. в глоссарии.



> **Улучшенная защита**
> Расширенное машинное обучение – это часть защит, к качестве дополнительного уровня защиты на основе машинного обучения, который улучшает работу функции обнаружения. Дополнительную информацию об этом типе защиты см. в глоссарии.

Настройка обнаружения

При обнаружении (например, угроза обнаруживается и классифицируется, как вредоносная программа) информация передается в Журнал обнаружения и появляются Уведомления на рабочем столе, если они настроены в меню ESET Security Ultimate.

Пороговое значение обнаружения настраивается для каждой категории (далее – «КАТЕГОРИЯ»):

1. Обнаружение вредоносных программ
2. Потенциально нежелательные приложения
3. Потенциально опасный

4.Подозрительные приложения

Обнаружения выполняются с помощью модуля обнаружения, включая компонент машинного обучения. Можно установить более высокое пороговое значение отчетности по сравнению с текущим значением защиты. Эти настройки отчетности не влияют на блокировку, очищение или удаление объектов.

Перед изменением порогового значения (или уровня) отчетности для КАТЕГОРИИ ознакомьтесь со следующим:

Пороговое значение	Описание
Агрессивный	Функция обнаружения КАТЕГОРИИ настроена на максимальную чувствительность. Случаев обнаружения будет больше. При уровне **Агрессивный** функция может ошибочно считать объекты КАТЕГОРИЯМИ.
Сбалансированный	Установлен сбалансированный уровень функции обнаружения КАТЕГОРИИ. Эта настройка должна обеспечивать оптимальный баланс производительности, точности обнаружения и количества ложных обнаружений.
Осторожный	Уровень функции обнаружения КАТЕГОРИИ настроен таким образом, чтобы уменьшить количество ложных обнаружений, но при этом сохранить достаточный уровень защиты. Объекты считаются такими, только если их поведение явно соответствует поведению КАТЕГОРИИ.
Выкл.	Функция обнаружения для КАТЕГОРИИ не активна, и обнаружения такого рода не обнаруживаются, не регистрируются и не очищаются. В результате, данная настройка отключает защиту от этого типа обнаружения. Значение «Выкл» недоступно для оповещения о вредоносных программах и по умолчанию используется для потенциально опасных приложений.

Доступность модулей защиты ESET Security Ultimate

Доступность (включено или выключено) модуля защиты для выбранного порогового значения КАТЕГОРИИ выглядит следующим образом:

	Агрессивный	Сбалансированный	Осторожный	Выкл*
Модуль расширенного машинного обучения	✓ (агрессивный режим)	✓ (консервативный модуль)	X	X
Модуль обнаружения	✔	✔	✔	X
Другие модули защиты	✔	✔	✔	X

* Не рекомендуется.

Определение версии продукта, версий модуля программы и даты сборки

1. Щелкните элемент **Справка и поддержка** > **О продукте ESET Security Ultimate**.
2. На экране **О продукте** в первой строке текста отображается номер версии вашего продукта ESET.
3. Щелкните элемент **Установленные компоненты** для доступа к информации о конкретных модулях.

Ключевые моменты

Несколько ключевых моментов при установке соответствующего порогового значения для вашей среды:

• **Сбалансированное** пороговое значение рекомендуется для большинства настроек.

• Более высокий порог отчетности — более высокий уровень обнаружения, но более высокий шанс ложно идентифицированных объектов.

• С реальной точки зрения, нет гарантии 100 % обнаружения, а также 0 % шансов избежать неправильной классификации чистых объектов как вредоносных программ.

• Сохраняйте ESET Security Ultimate и его модули в актуальном состоянии, чтобы обеспечить максимальный баланс между производительностью и точностью обнаружения и количеством ошибочно зарегистрированных объектов.

Настройка защиты

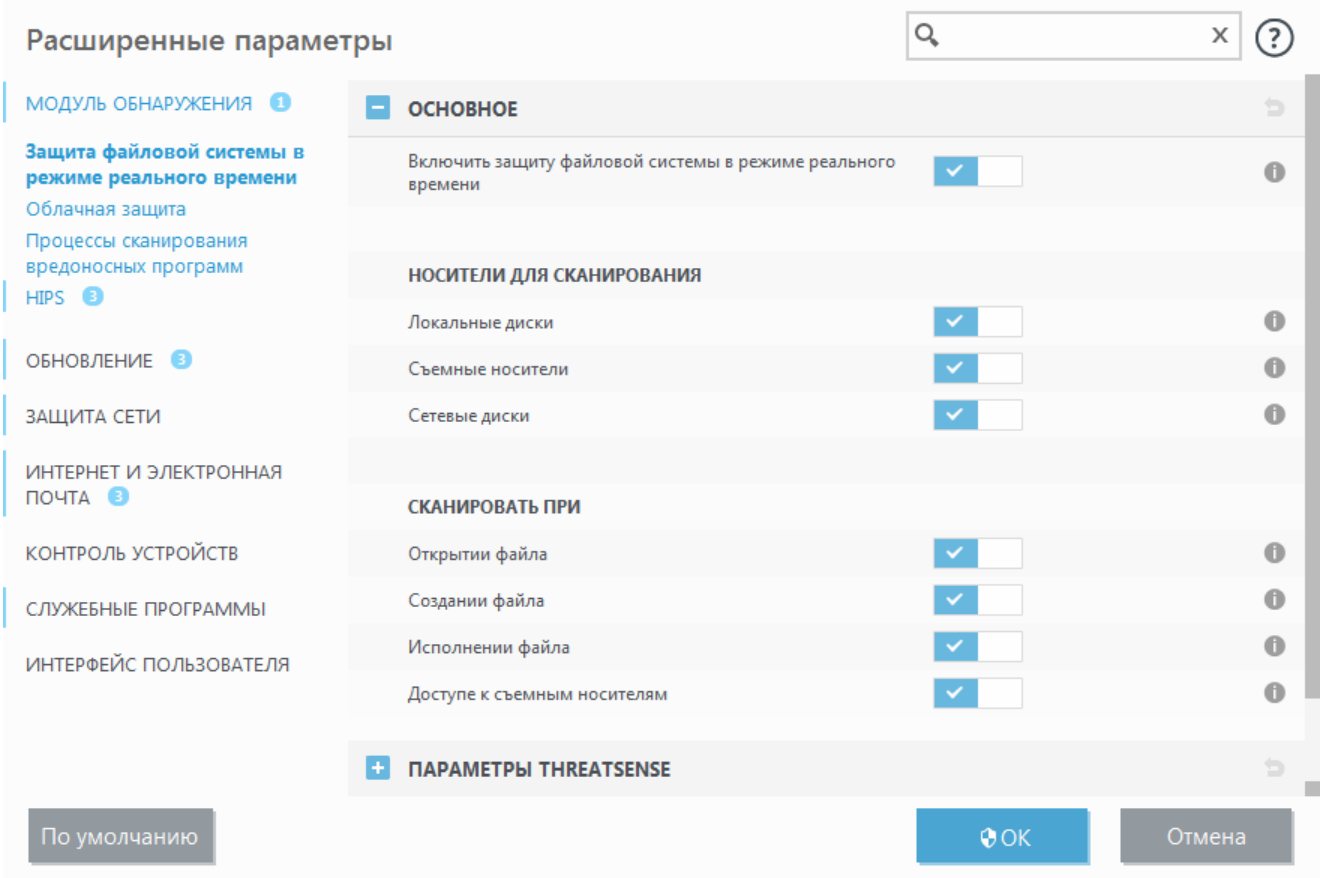
Если объект, классифицированный как КАТЕГОРИЯ, отображается в отчете, программа блокирует объект и затем очищает, удаляет или перемещает его в карантин.

Перед изменением порогового значения (или уровня) защиты для КАТЕГОРИИ ознакомьтесь со следующим:

Пороговое значение	Описание
Агрессивный	Сообщения об обнаружении агрессивного (или более низкого) уровня блокируются, и запускается автоматическое устранение неисправностей (т. е. очистка). Этот параметр рекомендуется, если все конечные точки были отсканированы с агрессивными настройками и в исключения обнаружения были добавлены объекты с ложным классифицированием.
Сбалансированный	Обнаружения сбалансированного (или более низкого) уровня блокируются, после чего запускается автоматическое исправление (т. е. очистка).
Осторожный	Обнаружения осторожного уровня блокируются, и запускается автоматическое исправление (т. е. очистка).
Выкл.	Полезно для идентификации и исключения ложных сообщений об объектах. Значение «Выкл» недоступно для защиты вредоносных программ и по умолчанию используется для потенциально опасных приложений.

Защита файловой системы в режиме реального времени

Защита файловой системы в режиме реального времени контролирует все файлы в системе на наличие вредоносного кода при открытии, создании или запуске.



По умолчанию функция защиты файловой системы в реальном времени запускается при загрузке системы и обеспечивает постоянное сканирование. Мы не рекомендуем отключать параметр **Включить защиту файловой системы в реальном времени** в разделе Расширенные параметры > **Защита** > **Защита файловой системы в реальном времени** > **Защита файловой системы в реальном времени**.

Носители для сканирования

По умолчанию все типы носителей сканируются на наличие возможных угроз.

- **Жесткие диски** — Сканирование всех системных и стационарных жестких дисков (например: *C:*\, *D:*\).
- **Съемные носители**: сканирование съемных носителей CD/DVD, USB-хранилища, карт памяти и т д.
- **Сетевые диски**: сканирование подключенных сетевых дисков (пример: *H:*\ как *store04*) или сетевых дисков прямого доступа (пример: *store08*).

Рекомендуется оставить параметры по умолчанию, а изменять их только в особых случаях (например, если сканирование определенных носителей приводит к значительному замедлению обмена данными).

Сканировать при

По умолчанию все файлы сканируются при открытии, создании или выполнении. Рекомендуется не изменять настройки по умолчанию, поскольку они обеспечивают максимальную защиту компьютера в режиме реального времени.

• **Открытии файла**: сканирование при открытии файла.

• **Создании файла**: сканирование созданного или измененного файла.

• **Исполнении файла**: сканирование при выполнении или запуске файла.

• **Доступ к загрузочному сектору съемных носителей**: сканирование сразу при вставке съемного носителя, содержащего загрузочный сектор, в устройство. Этот параметр не включает сканирование файлов на съемных носителях. Сканирование файлов на съемных носителях можно включить в разделе **Носители для сканирования** > **Съемные носители**. Чтобы **доступ к загрузочному сектору съемных носителей** работал корректно, включите настройку **Загрузочные секторы/UEFI** в ThreatSense.

Исключения для процессов

Исключения для процессов.

ThreatSense

Защита файловой системы в режиме реального времени проверяет все типы носителей и запускается различными событиями, такими как доступ к файлу. За счет использования методов обнаружения **ThreatSense** (как описано в разделе ThreatSense) защиту файловой системы в режиме реального времени можно настроить для создаваемых и уже существующих файлов по-разному. Например, можно настроить защиту файловой системы в режиме реального времени так, чтобы она более тщательно отслеживала вновь созданные файлы.

Чтобы снизить влияние на производительность компьютера при использовании защиты в режиме реального времени, повторное сканирование файлов, которые уже были просканированы, не выполняется (если файлы не были изменены). Файлы повторно сканируются сразу после каждого обновления модуля обнаружения. Управление этим режимом осуществляется с помощью параметра **Оптимизация Smart**. Если **оптимизация Smart** отключена, все файлы сканируются каждый раз при получении доступа к ним. Чтобы изменить эту настройку, откройте раздел Расширенные параметры > **Защита** > **Защита файловой системы в реальном времени**. Последовательно щелкните элементы **ThreatSense** > **Другое** и снимите или установите флажок **Включить интеллектуальную оптимизацию**.

Защита файловой системы в реальном времени также позволяет настраивать дополнительные параметры ThreatSense.

Исключения для процессов

Функция исключений для процессов позволяет исключать процессы приложений из Защиты файловой системы в реальном времени. Некоторые методики, используемые при резервном копировании и призванные повысить его скорость, улучшить целостность процессов и доступность служб, вызывают конфликт с защитой от вредоносных программ на уровне файлов. Единственный действенный способ избежать таких проблем — отключить антивирусное ПО. При исключении отдельных процессов (например, отвечающих за резервное копирование) все операции с файлами таких процессов игнорируются и считаются безопасными, что снижает отрицательное влияние на процесс резервного копирования. Создавать исключения следует с осторожностью — добавленное в исключение средство

резервного копирования может получить доступ к зараженным файлам, не выдав при этом оповещения, поэтому расширенные разрешения доступны только для модуля защиты в реальном времени.

Не следует путать эту функцию с другими возможностями исключения — Исключенные расширения файлов, Исключения системы HIPS, Исключения из обнаружения или Исключения для быстродействия.

Исключения для процессов позволяют снизить риск возникновения конфликтов и повысить производительность исключенных приложений, что положительно сказывается на производительности и стабильности операционной системы в целом. Исключение для процесса или приложения предполагает исключение и для его исполняемого файла (*.exe*).

Добавить исполняемые файлы в список исключенных процессов можно в разделе Расширенные параметры > **Защита** > **Защита файловой системы в реальном времени** > **Защита файловой системы в реальном времени** > **Исключения для процессов**.

Эта функция предназначена для добавления в исключения средств резервного копирования. Исключение из сканирования процессов, выполняемых средством резервного копирования, обеспечивает стабильность системы и способствует лучшей производительности резервного копирования, не замедляя его.

Щелкните **Изменить**, чтобы открыть окно управления **Исключения для процессов**, в котором можно добавить исключения и выбрать исполняемые файлы (например *Backup-tool.exe*), которые будут исключены из сканирования.
Если файл *.exe* добавлен в перечень исключений, ESET Security Ultimate не выполняет мониторинг его действий, как и не сканируются любые операции с файлами, выполняемые этим процессом.

Если исполняемый файл не выбран с помощью функции обзора, необходимо указать полный путь к файлу. Иначе исключение не будет работать правильно, а система HIPS может выдавать сообщения об ошибке.

Для существующих процессов также доступны функции **изменения** и **удаления** из исключений.

Защита доступа в Интернет не принимает во внимание такие исключения. Если вы добавили в исключение исполняемый файл своего веб-браузера, скачиваемые файлы по-прежнему будут сканироваться. Это позволит обнаружить зараженные файлы. Это разъяснение дано в познавательных целях, и мы не рекомендуем добавлять в исключение веб-браузер.

Добавление или изменение исключений процессов

В этом диалоговом окне можно **добавлять** процессы, исключаемые из модуля обнаружения. Исключения для процессов позволяют снизить риск возникновения конфликтов и повысить производительность исключенных приложений, что положительно сказывается на производительности и стабильности операционной системы в целом. Исключение для процесса или приложения предполагает исключение и для его исполняемого файла (*.exe*).

Выберите путь к файлу исключенного приложения, щелкнув ... (например, *C:\Program Files\Firefox\Firefox.exe*). НЕ вводите имя приложения.
Если файл *.exe* добавлен в перечень исключений, ESET Security Ultimate не выполняет мониторинг его действий, как и не сканируются любые операции с файлами, выполняемые этим процессом.

Если исполняемый файл не выбран с помощью функции обзора, необходимо указать полный путь к файлу. Иначе исключение не будет работать правильно, а система HIPS может выдавать сообщения об ошибке.

Для существующих процессов также доступны функции **изменения** и **удаления** из исключений.

Момент изменения конфигурации защиты в режиме реального времени

Защита в режиме реального времени является наиболее существенным элементом всей системы обеспечения безопасности. Необходимо быть внимательным при изменении ее параметров. Рекомендуется изменять параметры только в особых случаях.

После установки ESET Security Ultimate все параметры оптимизированы для максимальной защиты системы. Чтобы восстановить настройки по умолчанию, щелкните ↩ рядом с элементом Расширенные параметры > **Защита** > **Реагирование при обнаружении**.

Проверка модуля защиты в режиме реального времени

Чтобы убедиться, что защита в реальном времени работает и обнаруживает вирусы, используйте проверочный файл *www.eicar.com*. Этот тестовый файл является безвредным, и его обнаруживают все программы защиты от вирусов. Файл создан компанией EICAR (European Institute for Computer Antivirus Research) для проверки функционирования программ защиты от вирусов.

Файл доступен для загрузки с веб-сайта http://www.eicar.org/download/eicar.com.
После ввода этого URL-адресса в браузере вы должны увидеть сообщение об удалении угрозы.

Решение проблем, возникающих при работе защиты файловой системы в режиме реального времени

В этом разделе описаны проблемы, которые могут возникнуть при использовании защиты в режиме реального времени, и способы их устранения.

Защита файловой системы в режиме реального времени отключена

Если пользователь непреднамеренно отключит защиту в реальном времени, необходимо повторно активировать эту функцию. Чтобы повторно активировать защиту в реальном времени, перейдите в раздел **Настройка** в главном окне программы и щелкните **Защита компьютера** > **Защита файловой системы в реальном времени**.

Если защита файловой системы в режиме реального времени не запускается при загрузке системы, обычно это связано с тем, что отключен параметр **Включить защиту файловой системы в реальном времени**. Чтобы убедиться, что эта опция включена, откройте раздел Расширенные параметры > **Защита** > **Защита файловой системы в реальном времени**.

Защита в режиме реального времени не обнаруживает и не очищает заражения

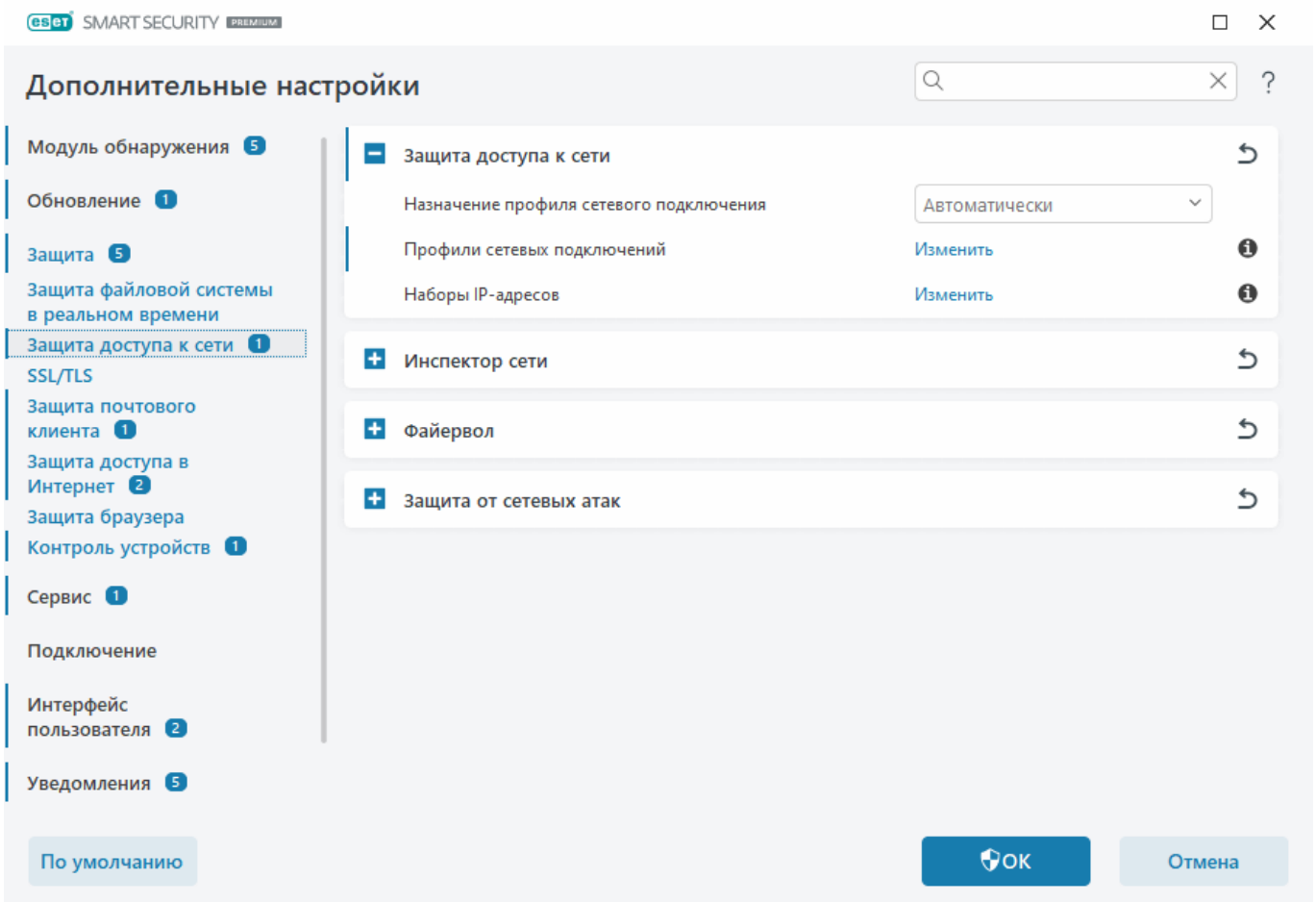
Убедитесь в том, что на компьютере не установлены другие программы защиты от вирусов. Если на компьютере установлено сразу две антивирусных программы, они могут конфликтовать между собой. Перед установкой ESET рекомендуется удалить с компьютера все прочие программы защиты от вирусов.

Защита в режиме реального времени не запускается

Если защита в реальном времени не запускается при загрузке системы (но функция **Включить защиту файловой системы в реальном времени** включена), возможно, возник конфликт с другими приложениями. Чтобы решить эту проблему, создайте журнал ESET SysInspector и отправьте его в службу технической поддержки ESET для анализа.

Защита доступа к сети

В разделе «Защита доступа к сети» можно детально настроить все сетевые подключения. Вы можете разрешить или запретить доступ к компьютеру в определенных сетях, разрешить или запретить доступ к сетевым устройствам с компьютера и сделать многое другое в соответствии с конфигурацией. По умолчанию в ESET Security Ultimate есть предварительно заданные правила файервола и включен максимальный уровень защиты доступа к сети. Однако для определенных сред может потребоваться пользовательская настройка. Изменять настройки по умолчанию должны только опытные пользователи.



В разделе Расширенные параметры > **Защита** > **Защита доступа к сети** можно настроить указанные ниже параметры. (Щелкайте ссылки ниже для получения подробного описания каждой опции защиты доступа к сети.)

Защита доступа к сети

Профили сетевых подключений: профили можно использовать, чтобы управлять работой файервола для определенных сетевых подключений.

Наборы IP-адресов: можно определить наборы IP-адресов, которые создают одну логическую группу IP-адресов и которые можно использовать для правил файервола.

Инспектор сети

Файервол

Защита от сетевых атак

Профили сетевых подключений

С помощью профилей можно управлять поведением функции защиты сети в ESET Security Ultimate для определенных сетевых подключений. При создании или изменении правила файервола, правила IDS или правила защиты от атак методом подбора его можно назначить определенному профилю или применить ко всем профилям. Когда определенный профиль действует для сетевого подключения, к нему применяются только глобальные правила

(правила без указания профиля) и правила, назначенные этому профилю. Можно создать несколько профилей с разными правилами, назначаемыми сетевым подключениям, чтобы легко изменять поведение файервола.

Настроить назначения и профили сетевых подключений можно в разделе Расширенные параметры > **Защита** > **Защита доступа к сети** > **Защита доступа к сети**.

Назначение профиля сетевого подключения: позволяет выбрать, будет ли вновь обнаруженным сетевым подключениям автоматически (выберите **Автоматически** в раскрывающемся меню) назначаться предварительно заданный или пользовательский профиль согласно активаторам, настроенным в профилях сетевых подключений, или программа должна отображать запрос (выберите **Запросить** в раскрывающемся меню) о необходимости настроить защиту сети и назначить профиль вручную при каждом обнаружении нового сетевого подключения.

Кроме того, вы можете вручную назначить определенный профиль сетевого подключения в главном окне программы в разделе **Настройка** > **Защита сети** > **Сетевые подключения**.

Наведите курсор на конкретное сетевое подключение и щелкните значок меню > **Изменить**, чтобы открыть окно Настройка защиты сети и выбрать профиль.

Профили сетевых подключений: щелкните **Изменить**, чтобы добавить или изменить профили сетевых подключений.

Следующие профили предварительно заданы и не могут быть изменены или удалены:

Конфиденциально — для доверенной сети (домашней или офисной сети). Ваш компьютер и общие файлы, хранящиеся на нем, видны для других пользователей сети, а также другим пользователям сети доступны системные ресурсы (доступ к общим файлам и принтерам включен, входящее подключение RPC включено, общий доступ к удаленному рабочему столу предоставлен). Этот параметр рекомендуется использовать при доступе к безопасной локальной сети. Этот профиль автоматически назначается сетевому подключению, если оно настроено как доменная или частная сеть в Windows.

Общедоступная — для недоверенных (общедоступных) сетей. Файлы и папки в вашей системе не являются общими для других пользователей в сети, и другие пользователи сети их не видят, а общий доступ к системным ресурсам отключен. Этот параметр рекомендуется использовать при доступе к беспроводным сетям. Этот профиль автоматически назначается любому сетевому подключению, которое не настроено как доменная или частная сеть в Windows.

При переключении сетевого подключения на другой профиль в правом нижнем углу экрана отображается уведомление.

Добавление и изменение профилей сетевых подключений

Добавлять или изменять профили сетевых подключений можно в разделе Расширенные параметры > **Защита** > **Защита доступа к сети** > **Защита доступа к сети** > **Профили сетевых подключений** > **Изменить**. Чтобы изменить профиль, его необходимо выбрать из списка в окне **Профили сетевых подключений**.

Следующие профили предварительно заданы и не могут быть изменены или удалены:

Конфиденциально — для доверенной сети (домашней или офисной сети). Ваш компьютер и общие файлы, хранящиеся на нем, видны для других пользователей сети, а также другим пользователям сети доступны системные ресурсы (доступ к общим файлам и принтерам включен, входящее подключение RPC включено, общий доступ к удаленному рабочему столу предоставлен). Этот параметр рекомендуется использовать при доступе к безопасной локальной сети. Этот профиль автоматически назначается сетевому подключению, если оно настроено как доменная или частная сеть в Windows.

Общедоступная — для недоверенных (общедоступных) сетей. Файлы и папки в вашей системе не являются общими для других пользователей в сети, и другие пользователи сети их не видят, а общий доступ к системным ресурсам отключен. Этот параметр рекомендуется использовать при доступе к беспроводным сетям. Этот профиль автоматически назначается любому сетевому подключению, которое не настроено как доменная или частная сеть в Windows.

В начало/Вверх/Вниз/В конец  : позволяет настроить уровень приоритета для профилей сетевых подключений. (Профили сетевых подключений оцениваются и применяются согласно их приоритету. Всегда применяется первый соответствующий профиль.)

Добавление или изменение профиля

Пользовательский профиль сетевого подключения позволяет применять правила файервола и указывать дополнительные настройки для определенных сетевых подключений. Указать, каким сетевым подключениям будет назначен пользовательский профиль, можно в разделе Активаторы.

Чтобы открыть редактор профиля, в окне **Профили сетевых подключений** выполните следующие действия.

- Нажмите кнопку **Добавить**.
- Выберите один из существующих профилей и щелкните **Изменить**.
- Выберите один из существующих профилей и щелкните **Копировать**.

Имя: пользовательское имя для вашего профиля.

Описание: описание профиля, помогающее его идентифицировать.

Дополнительные доверенные адреса: адреса, указанные здесь, добавляются в доверенную зону сетевого подключения, к которому применяется этот профиль (независимо от типа защиты сети).

Доверенное подключение: ваш компьютер и общие файлы, хранящиеся на нем, видны для других пользователей сети, а также другим пользователям сети доступны системные ресурсы (доступ к общим файлам и принтерам включен, входящее подключение RPC включено, общий доступ к удаленному рабочему столу предоставлен). Рекомендуем использовать эту настройку при создании профиля для безопасного подключения к локальной сети. Все напрямую подключенные сетевые подсети также считаются доверенными. Например, если сетевой адаптер подключен к этой сети с IP-адресом 192.168.1.5 и маской подсети 255.255.255.0,

подсеть 192.168.1.0/24 будет добавлена в доверенную зону такой сети. Если у адаптера есть больше адресов/подсетей, все они будут доверенными.

Сообщать о слабом шифровании Wi-Fi: ESET Security Ultimate отобразит уведомление на рабочем столе при подключении к незащищенной беспроводной сети или сети со слабой защитой.

Активаторы: пользовательские условия, которые должны быть выполнены для назначения этого профиля сетевому подключению. Подробное объяснение см. в разделе Активаторы.

Активаторы

Активаторы — это пользовательские условия, которые должны быть выполнены, чтобы профиль сетевого подключения был назначен сетевому подключению. Если атрибуты подключенной сети совпадают с атрибутами, которые определены в активаторах для профиля подключенной сети, такой профиль будет применен к сети. У профиля сетевого подключения может быть один или несколько активаторов. При наличии нескольких активаторов применяется логика ИЛИ (должно быть выполнено хотя бы одно условие). Определять активаторы можно в редакторе профилей сетевых подключений. Создавать пользовательские профили сетевых подключений должны опытные пользователи.

Доступны следующие активаторы (чтобы получить подробные сведения о текущей сети, см. раздел Сетевые подключения):

Адаптер

Тип адаптера: применить профиль, если сетевое подключение установлено на выбранном типе адаптера.
Имя адаптера: применить профиль, если совпадает имя сетевого адаптера.
IP-адрес адаптера: применить профиль, если совпадает IP-адрес сетевого адаптера.

DNS

DNS-суффикс: применить профиль, если совпадает доменное имя.
IP-адрес DNS: применить профиль, если совпадает IP-адрес DNS-сервера.

WINS

Применить профиль, если совпадает сопоставленный IP-адрес Windows Internet Name Service (WINS).

DHCP

IP-адрес DHCP: совпадение IP-адреса DHCP-сервера.

Шлюз по умолчанию

IP-адрес: применить профиль, если совпадает IP-адрес шлюза по умолчанию.
MAC-адрес: применить профиль, если совпадает MAC-адрес шлюза по умолчанию.

Wi-Fi

SSID: применить профиль, если совпадает SSID (имя сети Wi-Fi).
Имя профиля: применить профиль, если совпадает имя профиля Wi-Fi.
Тип защиты: применить профиль, если тип защиты совпадает с типом, который выбран с помощью раскрывающегося меню. (Если необходимо совпадение с несколькими типами, создайте больше активаторов.)
Тип шифрования: применить профиль, если тип шифрования совпадает с типом, который выбран с помощью раскрывающегося меню. (Если необходимо совпадение с несколькими типами, создайте больше активаторов.)
Безопасность сети: применить профиль, если сеть **открыта**/**защищена**.

Профиль Windows

Применить профиль, если сеть настроена в Windows как **доменная**/**частная**/**общедоступная**.

Аутентификация

В рамках аутентификации сети выполняется поиск определенного сервера в сети, а для аутентификации сервера используется асимметричное шифрование (RSA). Имя сети, для которой проводится аутентификация, должно совпадать с именем, заданным в настройках сервера аутентификации. Имя вводится с учетом регистра. Имя сервера может быть введено как IP-адрес, DNS-имя или NetBIOS-имя.
Загрузите сервер аутентификации ESET.
Открытым ключом может быть файл одного из указанных ниже типов.
• Открытый ключ с шифрованием PEM (.pem). Этот ключ можно создать с помощью сервера аутентификации ESET.
• Зашифрованный открытый ключ.
• Сертификат открытого ключа (.crt).
Чтобы проверить настройки, нажмите кнопку **Проверить**. Если аутентификация прошла успешно, на экране появится сообщение Аутентификация сервера завершена. Если аутентификация не настроена должным образом, на экране появится одно из указанных ниже сообщений об ошибке.
Сбой аутентификации сервера. Недопустимая или несовпадающая подпись.
Подпись сервера не отвечает введенному открытому ключу.
Сбой аутентификации сервера. Не соответствует имя сети.
Настроенное имя сети не соответствует имени сети сервера аутентификации. Проверьте оба имени и убедитесь, что они одинаковы.
Сбой аутентификации сервера. Нет ответа от сервера, или получен недопустимый ответ.
Ответ отсутствует, если сервер не работает или недоступен. Недопустимый ответ может быть получен в случае, если запущен другой HTTP-сервер с указанным адресом.
Указан недействительный открытый ключ.
Проверьте, не поврежден ли файл открытого ключа.

Наборы IP-адресов

Набор IP-адресов — это ряд IP-адресов, создающих одну логическую группу, которая может быть полезна при повторном использовании одного и того же набора адресов в нескольких правилах файервола или правилах защиты от атак методом подбора. Кроме того, ESET Security Ultimate содержит предварительно заданные наборы IP-адресов, к которым применяются внутренние правила. Примером такой группы является **доверенная зона**. Доверенная зона представляет собой группу сетевых адресов, где ваш компьютер и общие файлы, хранящиеся на нем, видны для других пользователей сети, а также другим пользователям сети доступны системные ресурсы.

Чтобы добавить набор IP-адресов, выполните следующие действия.

1. Откройте раздел Расширенные параметры > **Защита** > **Защита доступа к сети** > **Наборы IP-адресов** > **Изменить**.

2. Щелкните **Добавить**, введите **имя** и **описание** зоны и укажите удаленный IP-адрес в поле **Адрес удаленного компьютера (IPv4, IPv6, диапазон, маска)**.

3. Нажмите кнопку **OK**.

Дополнительные сведения см. в разделе Изменение наборов IP-адресов.

Редактирование наборов IP-адресов

Дополнительные сведения о наборах IP-адресов см. в разделе Наборы IP-адресов.

Столбцы

Имя: имя группы удаленных компьютеров.

Описание: общее описание группы.

IP-адреса: удаленные IP-адреса, которые принадлежат набору IP-адресов.

Элементы управления

При **добавлении** или **изменении** набора IP-адресов доступны следующие поля.

Имя: имя группы удаленных компьютеров.

Описание: общее описание группы.

Адрес удаленного компьютера (IPv4, IPv6, диапазон, маска): возможность добавления удаленного адреса, диапазона адресов или подсети.

Удалить: удаление зоны из списка.

> Предварительно заданные наборы IP-адресов не могут быть удалены.

Примеры IP-адресов

Добавить адрес IPv4:

Один адрес: добавляет IP-адрес отдельного компьютера (например, *192.168.0.10*).

Диапазон адресов: введите начальный и конечный IP-адреса, чтобы задать диапазон IP-адресов нескольких компьютеров (например, *192.168.0.1–192.168.0.99*).

Подсеть: подсеть (группа компьютеров), заданная IP-адресом и маской. Например, 255.255.255.0 — это маска сети для подсети 192.168.1.0. Чтобы исключить всю подсеть, введите *192.168.1.0/24*.

Добавить адрес IPv6:

Один адрес: добавляет IP-адрес отдельного компьютера (например, *2001:718:1c01:16:214:22ff:fec9:ca5*).

Подсеть: подсеть (группа компьютеров), заданная IP-адресом и маской (например, *2002:c0a8:6301:1::1/64*).

Инспектор сети

Инспектор сети может помочь выявить уязвимости в вашей доверенной (домашней или офисной) сети (например, открытые порты или ненадежный пароль маршрутизатора). Кроме того, вы получаете список подключенных устройств, в котором устройства упорядочены по типам (например, принтер, маршрутизатор, мобильное устройство и т. п.) и который позволяет узнать, какие устройства подключены к вашей сети (например, игровая консоль, устройство IoT или другие устройства «умного» дома). Настроить средство «Инспектор сети» можно в разделе Расширенные параметры > **Защита** > **Защита доступа к сети** > **Инспектор сети**.

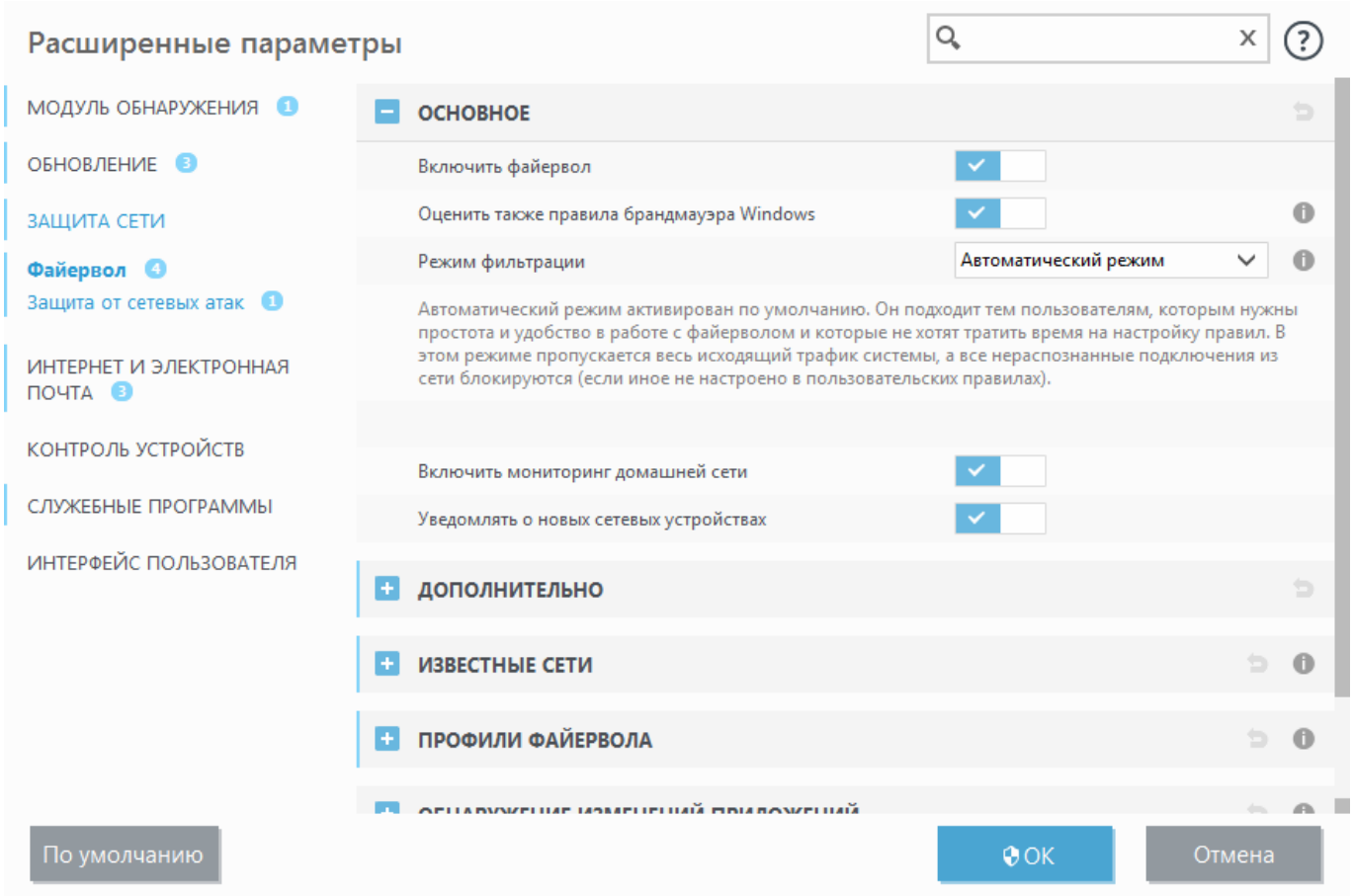
Включить Инспектор сети — **Инспектор сети** позволяет выявлять уязвимости в домашней сети, например открытые порты или ненадежный пароль маршрутизатора, а также предоставляет список подключенных устройств, упорядоченных по типу устройства.

Уведомлять о новых сетевых устройствах: уведомляет вас, когда в сети обнаруживается новое устройство.

Файервол

Файервол контролирует весь входящий и исходящий сетевой трафик на компьютере согласно внутренним правилам и правилам, которые определены пользователем. Процесс основан на разрешении или запрете отдельных сетевых соединений. Файервол обеспечивает защиту от атак со стороны удаленных устройств и может блокировать потенциально опасные службы.

Чтобы настроить файервол, откройте раздел Расширенные параметры > **Защита** > **Защита доступа к сети** > **Файервол**.



Файервол

Включить файервол

рекомендуется оставить эту функцию включенной, чтобы обеспечить защиту системы. При включенном файерволе сетевой трафик сканируется в обоих направлениях.

Правила

В разделе настройки правил можно просматривать и изменять все правила файервола, которые применяются к трафику, создаваемому отдельными приложениями в пределах доверенных подключений и сети Интернет.

> Вы можете создать правило IDS, когда ботнет атакует ваш компьютер. Правило можно изменить в разделе Расширенные параметры > **Защиты** > **Защита сети** > **Защита от сетевых атак** > **Правила IDS**, щелкнув **Изменить**.

Оценить также правила файервола Windows

В автоматическом режиме фильтрации разрешать также входящий трафик, допускаемый правилами брандмауэра Windows и не заблокированный явным образом правилами ESET.

Режим фильтрации

Поведение файервола зависит от выбранного режима фильтрации. От него также зависит степень участия пользователя в процессе.

Для файервола ESET Security Ultimate доступны следующие режимы фильтрации:

Режим фильтрации	Описание
Автоматический режим	Режим по умолчанию. Этот режим подходит для пользователей, которым нравится простота и удобство использования персонального файервола, а также отсутствие необходимости создавать правила. В режиме по умолчанию можно создавать пользовательские правила, однако это не является необходимым в **Автоматическом режим**. В автоматическом режиме разрешен весь исходящий трафик системы и блокируется большая часть входящего трафика — кроме некоторого трафика из доверенной зоны (как указано в разделе IDS и расширенные параметры/Разрешенные службы) и ответов на недавний исходящий трафик.
Интерактивный режим	Интерактивный режим: позволяет создать собственную конфигурацию файервола. Если обнаружено соединение, на которое не распространяется ни одно из существующих правил, на экран выводится диалоговое окно с уведомлением о неизвестном подключении. В этом диалоговом окне можно разрешить или запретить соединение, а также на основе этого решения создать правило для применения в будущем. Если принимается решение о создании нового правила, в соответствии с этим правилом все будущие соединения этого типа будут разрешены или запрещены.
Режим на основе политики	Блокирует все соединения, которые не соответствуют ни одному из ранее определенных разрешающих правил. Этот режим предназначен для опытных пользователей, которые могут создавать правила, разрешающие только нужные и безопасные соединения. Все прочие неуказанные соединения будут блокироваться файерволом.
Режим обучения	Автоматическое создание и сохранение правил. Этот режим удобен для первоначальной настройки файервола, но его не следует использовать длительное время. Участие пользователя не требуется, потому что ESET Security Ultimate сохраняет правила согласно предварительно настроенным параметрам. Чтобы избежать рисков, режим обучения рекомендуется использовать только до момента создания правил для всех необходимых соединений.

Режим обучения завершится: установите дату и время, когда режим обучения закончится автоматически. Кроме того, режим обучения можно в любой момент отключить вручную.

Режим задан после завершения режима обучения: определите режим фильтрации, который будет восстановлен файерволом программы по завершении периода режима обучения. Подробнее о режимах фильтрации читайте в таблице выше. Чтобы после завершения режима обучения изменить режим фильтрации файервола на **Спросить пользователя**, нужны права администратора.

Настройки режима обучения: щелкните **Изменить**, чтобы настроить параметры сохранения правил, созданных в режиме обучения.

Обнаружение изменения приложений

Функция обнаружения изменений приложений отображает уведомления, если измененные приложения, для которых существует правило, пытаются установить подключения.

Настройки режима обучения

В режиме обучения правила для каждого соединения, установленного системой, создаются и сохраняются автоматически. Участие пользователя не требуется, потому что ESET Security Ultimate сохраняет правила согласно предварительно настроенным параметрам.

Использование этого режима может представлять риск для системы, и его рекомендуется использовать только для первоначальной настройки файервола.

Выберите **Обучение** в раскрывающемся меню в разделе Расширенные параметры > **Защита** > **Защита доступа к сети** > **Файервол** > **Файервол** > **Режим фильтрации**, чтобы активировать опции режима обучения. Щелкните **Изменить** рядом с элементом **Настройки режима обучения**, чтобы настроить следующие опции:

> ⚠ В режиме обучения файервол не фильтрует соединения. Разрешены все исходящие и входящие соединения. В этом режиме компьютер защищен файерволом не полностью.

Входящий трафик из доверенной зоны: примером входящего соединения в доверенной зоне является удаленное устройство, находящееся в пределах доверенной зоны, которое пытается установить соединение с локальным приложением, запущенным на вашем компьютере.

Исходящий трафик в доверенную зону: приложение на локальном компьютере пытается установить соединение с другим устройством в пределах локальной сети или сети в доверенной зоне.

Входящий интернет-трафик: удаленное устройство пытается установить соединение с приложением, запущенным на компьютере.

Исходящий интернет-трафик: приложение на локальном компьютере пытается установить соединение с другим устройством.

В каждом разделе определяются параметры, которые будут добавляться к новым правилам.

Добавить локальный порт: включает номер локального порта сетевого соединения. Для исходящих соединений обычно создаются случайные номера. В связи с этим рекомендуется включать эту настройку только для входящих подключений.

Добавить приложение: включает имя локального приложения. Данный параметр предназначен для использования в будущих правилах на уровне приложений (правилах, определяющих соединения для всего приложения). Например, можно разрешить соединения только для веб-браузера или почтового клиента.

Добавить удаленный порт: включает номер удаленного порта сетевого соединения. Например, можно разрешить или запретить подключение определенной службы, связанной со стандартным номером порта (HTTP — 80, POP3 — 110 и т. д.).

Добавить удаленный IP-адрес или удаленную доверенную зону: удаленный IP-адрес или удаленная зона могут использоваться в качестве параметра новых правил, регулирующих все соединения между локальной системой и соответствующим удаленным адресом или зоной. Этот параметр используется при определении действий для конкретного устройства или

группы сетевых устройств.

Максимальное количество разных правил для одного приложения: если приложение подключается к разным IP-адресам через разные порты, файервол в режиме обучения создаст для этого приложения соответствующее количество правил. Данный параметр позволяет ограничить число правил, которые могут быть созданы для одного приложения.

Правила файервола

Правило файервола содержит набор параметров и условий, которые позволяют целенаправленно проверять сетевые соединения и выполнять необходимые действия в соответствии с этими условиями. С помощью правил файервола можно задать действия, которые выполняются при установке сетевых соединений различных типов.

Правила оцениваются сверху вниз, и их приоритет отображается в первом столбце. Действие, определяемое первым соответствующим правилом, используется для каждого обрабатываемого сетевого соединения.

Подключения можно разделить на входящие и исходящие. Входящее подключение инициируется удаленным устройством, который пытается установить соединение с локальной системой. При исходящем соединении локальный компьютер пытается подключиться к удаленному устройству.

Обнаружив новое неизвестное подключение, хорошо подумайте, прежде чем разрешать или запрещать его. Нежелательные, небезопасные или неизвестные соединения несут угрозу безопасности для компьютера. При установлении такого соединения рекомендуется обратить внимание на удаленное устройство и приложение, которые пытаются подключиться к вашему компьютеру. При многих видах заражений осуществляются попытки получения и отправки конфиденциальных данных и загрузки других вредоносных приложений на рабочие станции. Файервол дает пользователю возможность обнаружить и разорвать такие подключения.

Правила файервола можно просматривать и изменять в разделе Расширенные параметры > **Защита** > **Защита доступа к сети** > **Файервол** > **Правила** > **Изменить**.

Если у вас много правил файервола, с помощью фильтра можно отобразить только некоторые из них. Чтобы отфильтровать правила файервола, щелкните **Больше фильтров** над списком «Правила файервола». Фильтровать правила можно по следующим критериям:

- Источник
- Направление
- Действие
- Доступность

По умолчанию предварительно заданные правила файервола скрыты. Чтобы отобразить все предварительно заданные правила, отключите переключатель рядом с элементом **Скрыть встроенные (предварительно заданные) правила**. Эти правила можно отключить, но не удалить.

Щелкните значок поиска в верхней правой части экрана, чтобы искать правила.

Столбцы

Приоритет: правила оцениваются сверху вниз, и их приоритет отображается в первом столбце.

Включено: сведения о том, включено ли правило. Чтобы активировать правило, установите соответствующий флажок.

Приложение: приложение, к которому применяется правило.

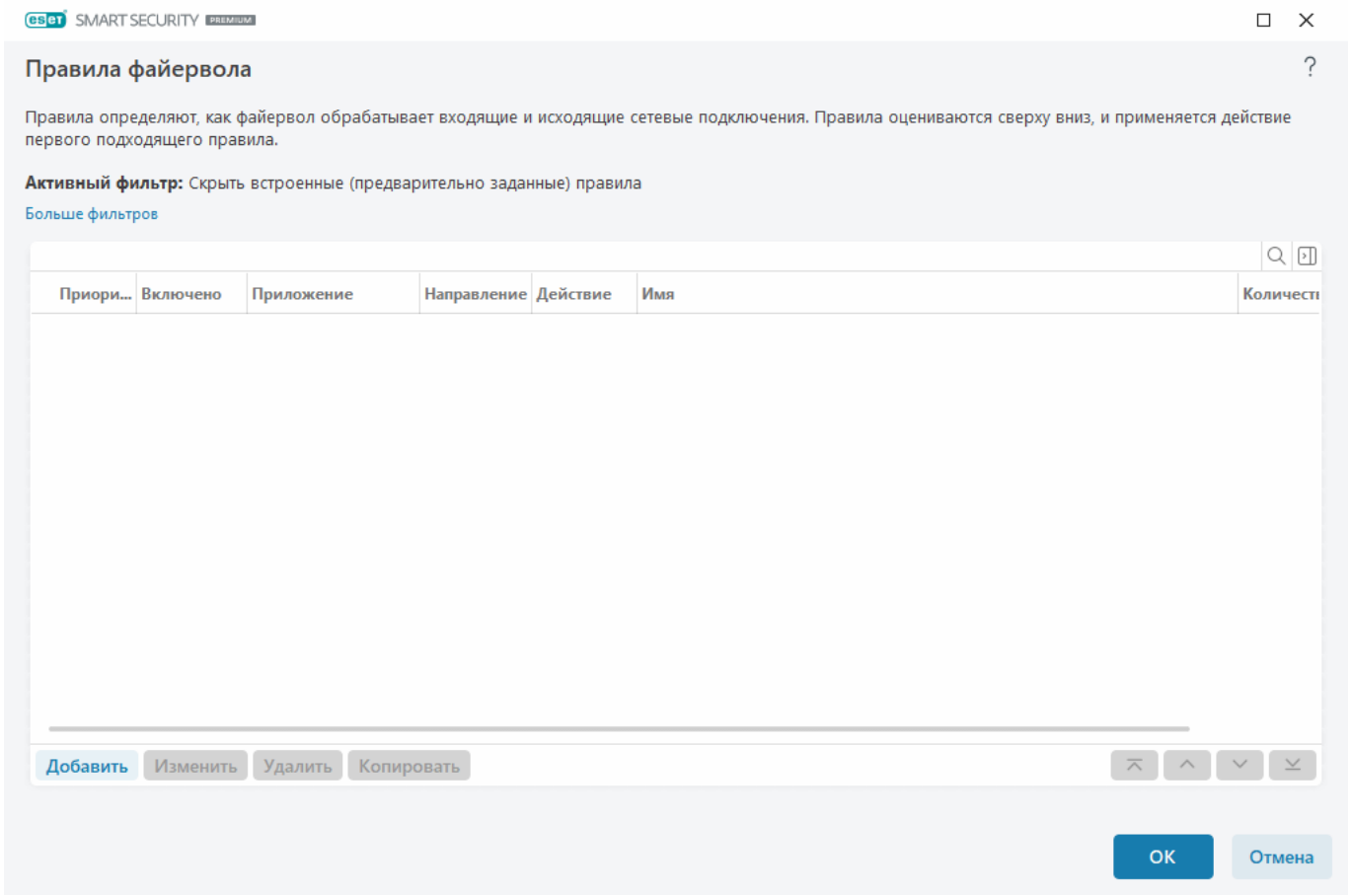
Направление: направление соединения (входящее/исходящее/оба).

Действие: сведения о состоянии подключения (блокировать/разрешать/спрашивать).

Имя: имя правила. Значком ESET обозначаются предварительно заданные правила.

Количество применений: общее количество раз, когда правило было применено.

Щелкните значок расширения, чтобы отобразить сведения о правиле.



Элементы управления

Добавить: создание правила.

Изменить– изменение существующего правила.

Удалить: удаление существующего правила.

Копировать: создание копии выбранного правила.

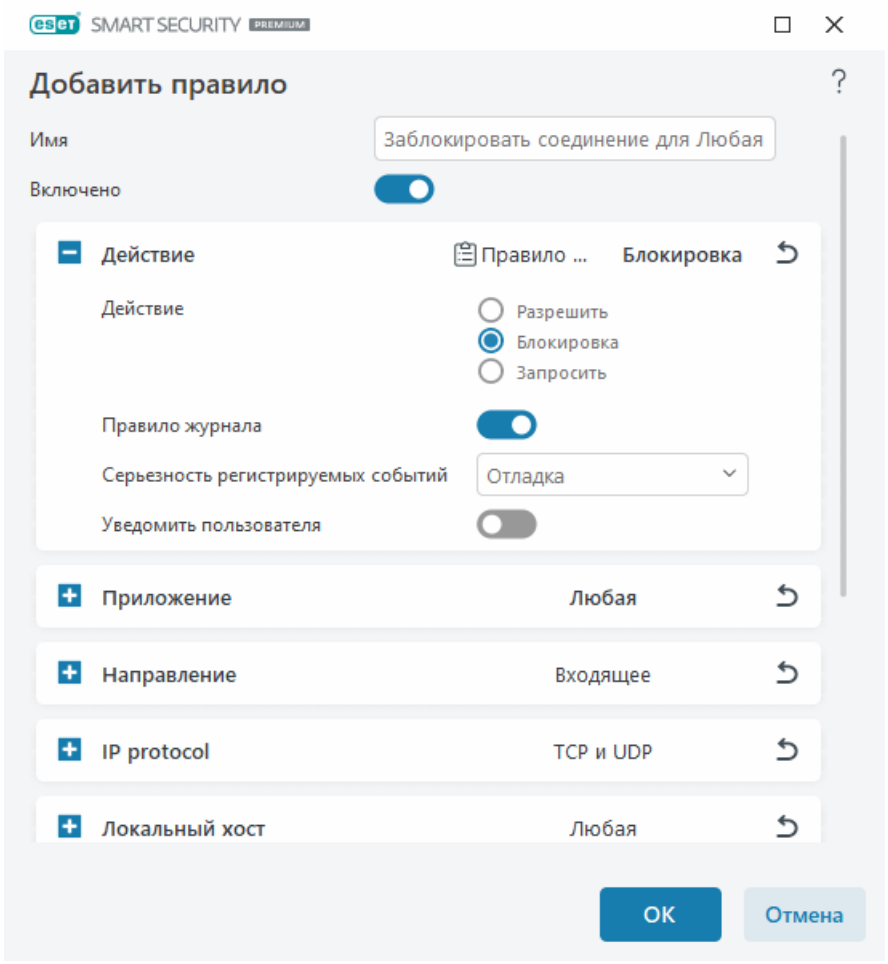

В начало/Вверх/Вниз/В конец: настройка приоритетности правил (правила последовательно выполняются сверху вниз).

Добавление и изменение правил файервола

Правила файервола представляют собой условия, используемые для целенаправленной проверки всех сетевых соединений, и действия, назначаемые для этих условий. При изменении настроек сети (например, при изменении сетевого адреса или номера порта для удаленного компьютера) может потребоваться редактирование или добавление правил файервола, чтобы обеспечить правильную работу приложения, на которое распространяется правило. Создавать пользовательские правила файервола должны опытные пользователи.

> **Иллюстрированные инструкции**
> Следующие статьи из базы знаний ESET могут быть доступны только на английском языке:
> • Открытие или закрытие (разрешение или запрещение) определенного порта с помощью файервола
> • Создание правила файервола на основе файлов журнала в ESET Security Ultimate

Чтобы добавить или изменить правило файервола, откройте раздел Расширенные параметры > **Защита** > **Защита доступа к сети** > **Файервол** > **Правила** > **Изменить**. В окне Правила файервола щелкните **Добавить** или **Изменить**.



Имя: введите имя правила.

Включено: щелкните переключатель, чтобы сделать правило активным.

Добавление действий и условий для правила файервола:

Действие

Действие: выберите вариант **Разрешить** или **Заблокировать** для подключения, которое соответствует условиям, определенным в этом правиле. Или выберите вариант **Запросить**, чтобы программа ESET Security Ultimate выводила запрос при каждом установлении подключения.
Правило журнала: если правило применяется, сведения об этом записываются в файлы журнала.
Серьезность регистрируемых событий: выберите для этого правила серьезность записи журнала.
Уведомить пользователя: отображает уведомление при применении правила.

Приложение

Укажите приложение, в котором будет применяться это правило.
Путь приложения: щелкните **...** и перейдите к приложению или введите полный путь приложения (например, C:\Program Files\Firefox\Firefox.exe). НЕ вводите только лишь имя приложения.
Подпись приложения: правило можно применить к приложениям согласно их подписям (именам издателей). В раскрывающемся меню выберите, следует ли применять правило к приложениям с **любой действительной подписью** или к приложениям, которые **подписаны конкретным лицом**. Если выбраны приложения, которые **подписаны конкретным лицом**, необходимо указать подписывающее лицо в поле **Имя подписавшего**.
Приложение Microsoft Store: в раскрывающемся меню выберите приложение, установленное из магазина Microsoft Store.
Служба: вместо приложения можно выбрать системную службу. Чтобы выбрать службу, откройте раскрывающееся меню.
Применить к дочерним процессам: некоторые приложения могут запускать больше процессов, в то время как вы видите только одно окно приложения. Щелкните переключатель, чтобы включить правило для всех процессов в указанном приложении.

Направление

Выберите **направление** обмена данными для этого правила.
- **Оба**: входящий и исходящий обмен данными.
- **Входящее**: только входящий обмен данными.
- **Исходящее**: только исходящий обмен данными.

Протокол IP

В раскрывающемся меню выберите **протокол**, если это правило должно применяться только к определенному протоколу.

Локальный хост

Локальные адреса, диапазон адресов или подсеть, где применяется это правило. Если адрес не указан, правило будет применяться ко всему обмену данными с локальными хостами. Вы можете добавить IP-адреса, диапазоны адресов или подсети непосредственно в текстовое поле **IP-адрес** или выбрать один из существующих наборов IP-адресов, щелкнув **Изменить** рядом с элементом **Наборы IP-адресов**.

Локальный порт

Порт: номер локального порта (или номера нескольких портов). Если номера не указаны, правило будет применяться к любому порту. Добавьте один порт связи или укажите их диапазон.

Удаленный хост

Удаленный адрес, диапазон адресов или подсеть, где применяется это правило. Если адрес не указан, правило будет применяться ко всему обмену данными с удаленными хостами. Вы можете добавить IP-адреса, диапазоны адресов или подсети непосредственно в текстовое поле **IP-адрес** или выбрать один из существующих наборов IP-адресов, щелкнув **Изменить** рядом с элементом **Наборы IP-адресов**.

Удаленный порт

Порт: номер удаленного порта или номера нескольких портов. Если номера не указаны, правило будет применяться к любому порту. Добавьте один порт связи или укажите их диапазон.

Профиль

Правило файервола может быть применено к определенным профилям сетевых подключений.
Любой: правило будет применяться к любому сетевому подключению независимо от используемого профиля.
Выбрано: правило будет применяться к определенному сетевому подключению согласно выбранному профилю. Установите флажок рядом с профилями, которые нужно выбрать.

Мы создаем новое правило, разрешающее веб-браузеру Firefox доступ к веб-сайтам в сети Интернет и локальной сети.
1.В разделе **Действие** выберите **Действие** > **Разрешить**.
2.В разделе **Приложение** укажите **путь к приложению** веб-браузера (например, C:\Program Files\Firefox\Firefox.exe). НЕ вводите только лишь имя приложения.
3.В разделе **Направление** выберите **Направление** > **Исходящее**.
4.В разделе **Протокол IP** выберите **TCP и UDP** в раскрывающемся меню **Протокол**.
5.В разделе **Удаленный порт** добавьте номера **портов**: *80, 443*, чтобы разрешить стандартное использование браузера.

Обнаружение изменения приложений

Функция обнаружения изменений приложений отображает уведомления, если измененные приложения, для которых существует правило брандмауэра, пытаются установить подключения. Изменение приложений — это механизм временной или постоянной замены исходного приложения другим исполняемым приложением (защита от нарушения правил брандмауэра).

Обратите внимание, что эта функция не предназначена для обнаружения изменений во всех приложениях. Она создана, чтобы не нарушались существующие правила файервола, и отслеживаются только приложения, для которых эти правила предназначены.

Чтобы настроить **обнаружение изменений в приложениях**, откройте раздел Расширенные параметры > **Защита** > **Защита доступа к сети** > **Файервол** > **Обнаружение изменений в приложениях**.

Включить отслеживание изменений приложений: если выбран этот параметр, программа будет отслеживать изменения в приложениях (обновления, заражения и другие изменения). При попытке измененного приложения установить соединение пользователь получит уведомление от файервола.

Разрешить изменения в подписанных (доверенных) приложениях: не уведомлять, если после изменения действительная цифровая подпись приложения остается неизменной.

Список приложений, исключенных из обнаружения: в этом окне можно добавлять и удалять приложения, при изменении которых не выводятся уведомления.

Список приложений, исключенных из обнаружения

Файервол в продукте ESET Security Ultimate выявляет изменения в приложениях, к которым применяются правила (см. раздел Обнаружение изменений приложений).

В определенных случаях приходится отключать эту функцию для некоторых приложений, если нужно исключить их из проверки файерволом.

Добавить: открывает окно, в котором можно выбрать приложение и добавить его в список приложений, исключенных из обнаружения изменений. Вы можете выбрать из списка запущенных приложений с открытой передачей данных по сети, для которых существует правило файервола, или добавить конкретное приложение.

Изменить: открывает окно, в котором можно изменить расположение приложения из списка приложений, исключенных из обнаружения изменений. Вы можете выбрать из списка запущенных приложений с открытой передачей данных по сети, для которых существует правило файервола, или изменить расположение вручную.

Удалить: удаление записей из списка приложений, исключенных из проверки.

Защита от сетевых атак (IDS)

Защита от сетевых атак (IDS) улучшает обнаружение эксплойтов для известных уязвимостей. Дополнительные сведения о защите от сетевых атак см. в глоссарии. Чтобы настроить защиту от сетевых атак, откройте раздел Расширенные параметры > **Защита** > **Защита доступа к сети** > **Защита от сетевых атак**.

Включить защиту от сетевых атак (IDS).Анализ содержимого сетевого трафика и защита от сетевых атак. Любой трафик, который расценивается как опасный, блокируется.

Включить защиту от ботнетов. Обнаружение и блокирование подключений к вредоносным серверам командования и управления. В основе функции лежит распознавание стандартных шаблонов, с помощью которых зараженный ботом компьютер пытается подключаться к опасным серверам.Дополнительные сведения о защите от ботнетов см. в глоссарии.

Правила IDS: Позволяет настраивать расширенные параметры фильтрации для обнаружения различных типов атак, которые могут быть предприняты, чтобы навредить компьютеру.

> **Иллюстрированные инструкции**
> Следующие статьи из базы знаний ESET могут быть доступны только на английском языке:
> - Исключение IP-адреса из IDS в ESET Security Ultimate

Все важные события, обнаруженные защитой сети, сохраняются в файле журнала. Дополнительные сведения см. в журнале защиты сети.

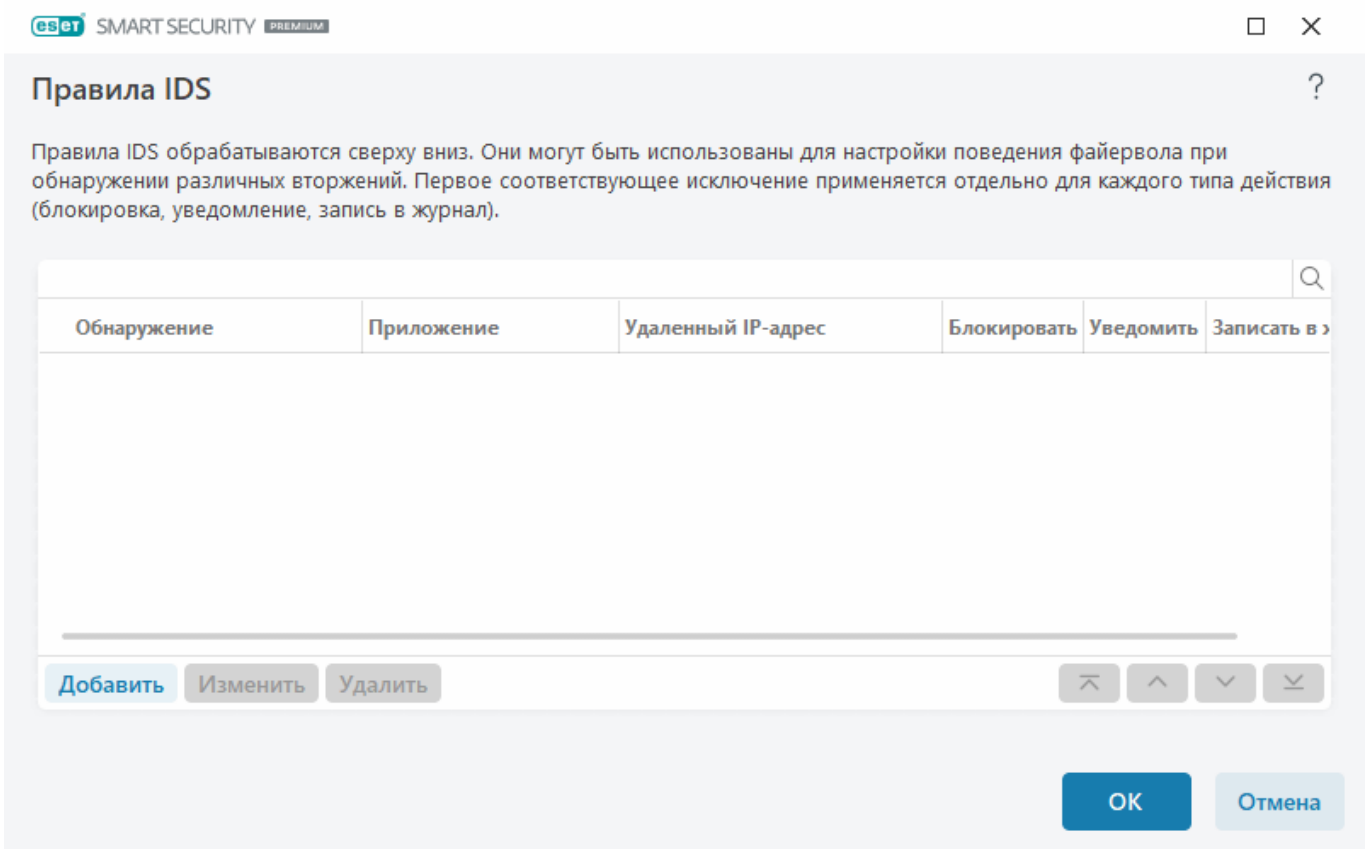
IDS правила

В некоторых случаях система обнаружения вторжения (Intrusion Detection Service, IDS) может расценить передачу информации между маршрутизаторами или другими внутренними сетевыми устройствами как потенциальную атаку. Например, вы можете добавить известный безопасный адрес в адреса, исключенные из системы обнаружения вторжений, чтобы обойти IDS.

> **Иллюстрированные инструкции**
> Следующие статьи из базы знаний ESET могут быть доступны только на английском языке:
> - Исключение IP-адреса из IDS в ESET Security Ultimate

Управление правилами IDS

- **Добавить**: нажмите для создания нового правило IDS.
- **Изменить**: нажмите для изменения существующего правила IDS.
- **Удалить**: выберите и щелкните для удаления правила IDS из списка правил.
-  **В начало/Вверх/Вниз/В конец**: настройка приоритетности правил (исключения обрабатываются сверху вниз).



Редактор правил

Обнаружение: тип обнаружения.

Имя угрозы: можно указать имя угрозы для некоторых доступных обнаружений.

Приложение: выберите путь к файлу исключенного приложения, щелкнув ... (например, *C:\Program Files\Firefox\Firefox.exe*). НЕ вводите имя приложения.

Удаленный IP-адрес. Список удаленных адресов, диапазонов или подсетей (IPv4 или IPv6). Несколько адресов следует разделять запятой.

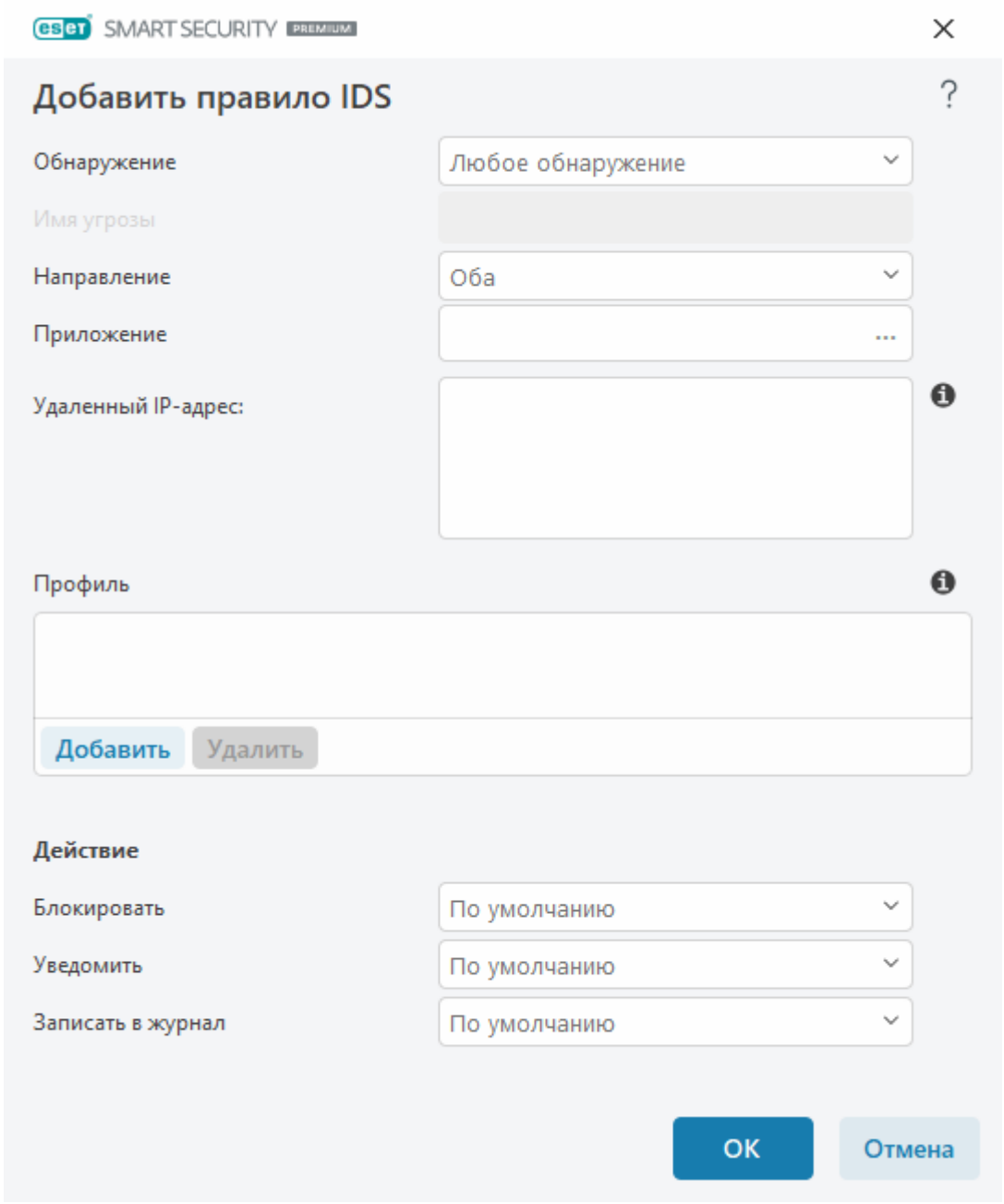
Профиль. Можно выбрать профиль сетевого подключения, к которому применяется это правило.

Действие

Блокировать. Каждый системный процесс имеет свое поведение по умолчанию и назначенное действие (блокировать или разрешить). Для изменения поведения ESET Security Ultimate по умолчанию вы можете разрешить или заблокировать его запуск из раскрывающегося меню.

Уведомить. Выберите Да, чтобы отображать уведомления на рабочем столе на своем компьютере. Выберите Нет, чтобы отключить уведомления. Доступные значения: По умолчанию, Да, Нет.

Записать в журнал. Выберите **Да**, чтобы записывать события в файлы журнала. Выберите **Нет**, чтобы отключить запись. Доступные значения: **По умолчанию**, **Да**, **Нет**.



Если при каждом возникновении события необходимо, чтобы отображалось уведомление и выполнялась запись в журнал:

1.Щелкните**Добавить**, чтобы добавить новое правило IDS.

2.Выберите нужное обнаружение в раскрывающемся меню **Обнаружение**.

3.Выберите путь приложения, щелкнув элемент **...**, для которого необходимо применить это уведомление.

4.Оставьте значение **По умолчанию** в раскрывающемся меню**Блокировать**. Это позволит унаследовать действие по умолчанию, примененное ESET Security Ultimate.

5.Выберите в раскрывающихся меню **Уведомить** и**Записать в журнал** значения **Да**.

6.Щелкните **OK**, чтобы сохранить это уведомление.

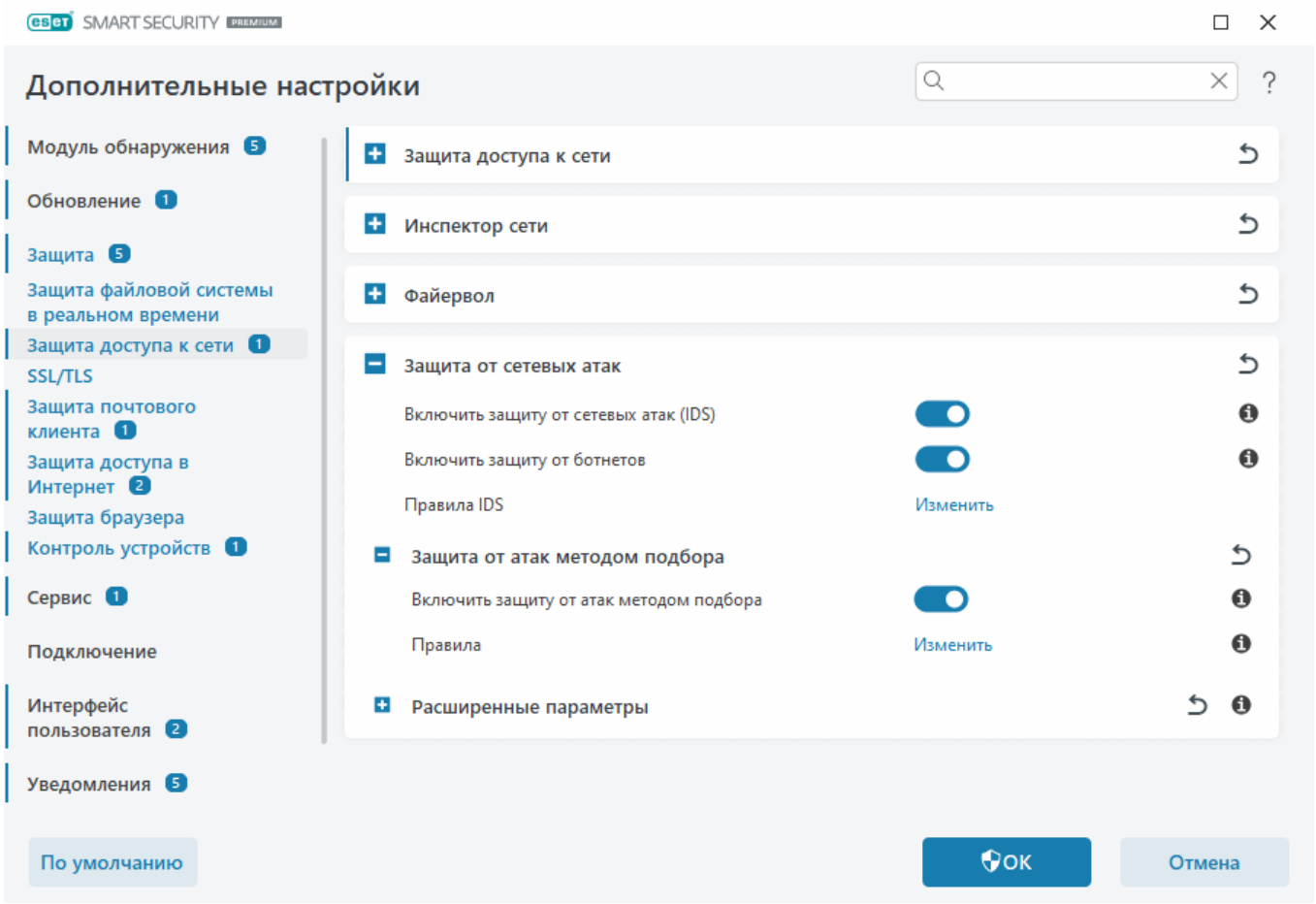
Если вы не хотите отображать повторяющееся уведомление, которое не считаете угрозой определенного типа **обнаружения**:
1.Щелкните**Добавить**, чтобы добавить новое правило IDS.
2.Выберите нужное обнаружение в раскрывающемся меню **Обнаружение**, например **Сеанс SMB без расширений безопасности** или **Атака сканирования портов TCP**.
3.Выберите **В** в раскрывающемся меню с направлениями для входящего подключения.
4.Выберите для раскрывающегося меню **Уведомить** значение **Нет**.
5.Выберите для раскрывающегося меню **Записать в журнал** значение **Да**.
6.Оставьте значение **Приложение** пустым.
7.Если входящий трафик поступает не с определенного IP-адреса, оставьте значение **Удаленные IP-адреса** пустым.
8.Щелкните **OK**, чтобы сохранить это уведомление.

Защита от атак методом подбора

Защита от атак методом подбора блокирует атаки, которые предусматривают угадывание пароля и направлены на службы RDP или SMB. Атака методом подбора — это способ определения пароля, при котором происходит систематический перебор всех комбинаций букв, цифр и символов. Чтобы настроить защиту от атак методом подбора, откройте раздел Расширенные параметры > **Защита** > **Защита доступа к сети** > **Защита от сетевых атак** > **Защита от атак методом подбора**.

Включить защиту от атак методом подбора: ESET Security Ultimate проверяет содержимое сетевого трафика и блокирует попытки атак, которые предусматривают угадывание пароля.

Правила: вы можете создавать, изменять и просматривать правила для входящих и исходящих сетевых подключений. Для получения дополнительных сведений см. главу Правила.



Правила

Правила: вы можете создавать, изменять и просматривать правила для входящих и исходящих сетевых подключений. Предварительно заданные правила нельзя изменить или удалить.

Управление правилами защиты от атак методом подбора

Добавить: создание правила.

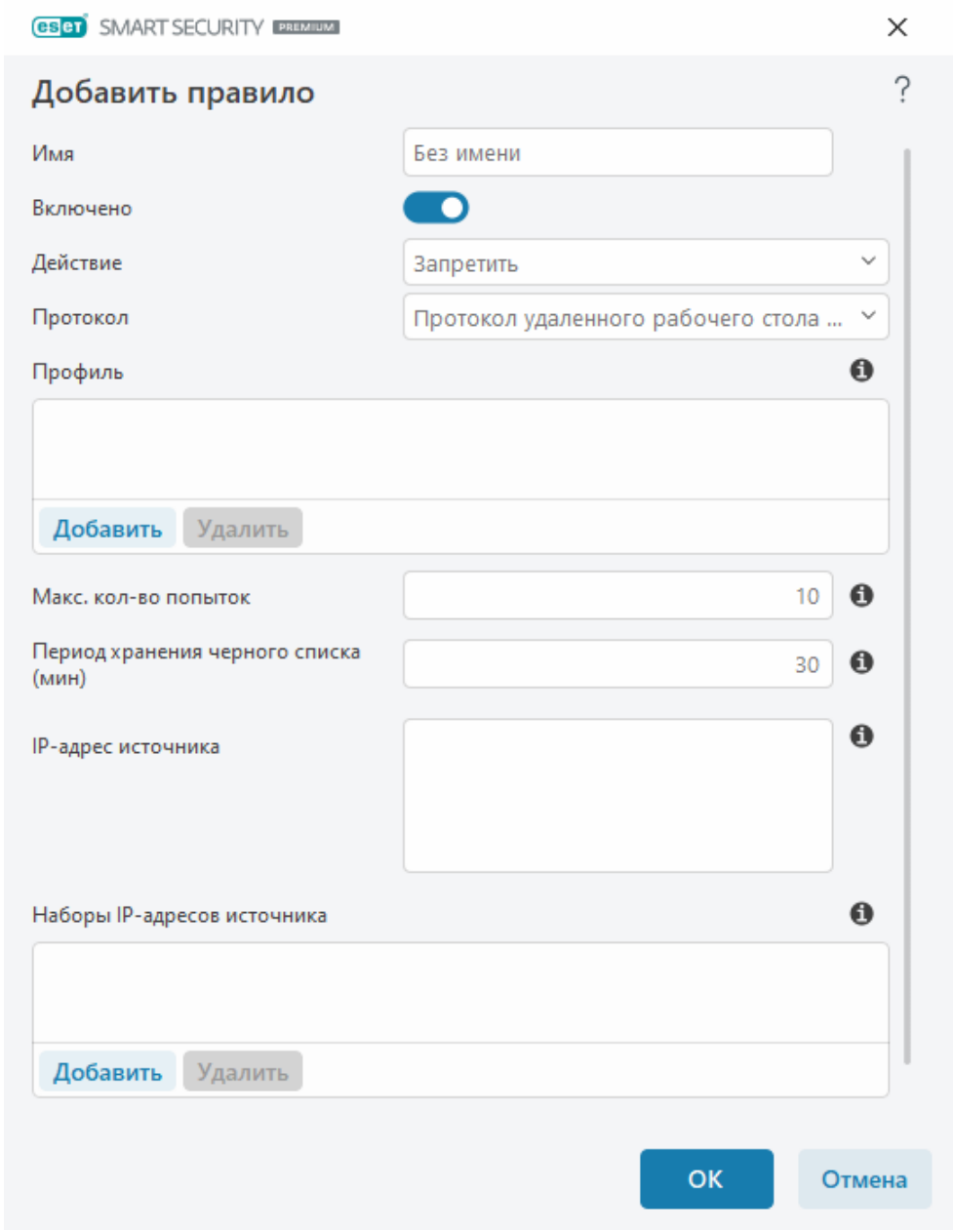
Изменить– изменение существующего правила.

Удалить: удаление существующего правила из списка правил.

 **В начало/Вверх/Вниз/В конец**: настройка приоритетности правил.

> Чтобы обеспечить максимальную защиту, применяется правило блокировки с наименьшим значением параметра **Макс. кол-во попыток**, даже если это правило находится ниже в списке правил, когда условиям обнаружения соответствует несколько правил блокировки.

Редактор правил



Имя: имя правила.

Включено: отключите этот переключатель, если правило нужно оставить в списке, но при этом не применять его.

Действие: выберите, следует ли **запретить** или **разрешить** подключение, если выполняются параметры правила.

Протокол: протокол связи, который будет проверяться этим правилом.

Профиль: для конкретных профилей можно устанавливать и применять пользовательские правила.

Макс. кол-во попыток — Максимальное количество разрешенных попыток повторения атаки, по достижении которого IP-адрес будет заблокирован и добавлен в черный список.

Период хранения черного списка (мин): установка времени, по истечении которого адрес будет исключен из черного списка.

IP-адрес источника: список IP-адресов, диапазонов или подсетей. Несколько адресов следует разделять запятой.

Наборы IP-адресов источника: набор IP-адресов, который вы уже задали в разделе Наборы IP-адресов.

Расширенные параметры

В разделе Расширенные параметры > **Защита** > **Защита доступа к сети** > **Защита от сетевых атак** > **Расширенные параметры** можно включить или отключить обнаружение нескольких типов атак и эксплойтов, которые могут нанести вред компьютеру.

В некоторых случаях уведомление о заблокированном соединении не отображается. См. раздел Ведение журнала и создание правил и исключений на основе журнала, чтобы узнать, как просматривать заблокированные соединения в журнале файервола.

Доступность отдельных параметров в этом окне зависит от типа или версии программы ESET и модуля файервола, а также от версии операционной системы.

Обнаружение вторжения

Функция обнаружения вторжений отслеживает вредоносные действия при обмене данными в сети устройства.

- **Протокол SMB**: обнаруживает и блокирует разные проблемы с безопасностью в протоколе SMB (подробности указаны ниже).
- **Протокол RPC**: обнаруживает и блокирует различные идентификаторы CVE в системе удаленного вызова процедур, разработанной для среды распределенных вычислений (DCE).
- **Протокол RDP**: обнаруживает и блокирует различные идентификаторы CVE в протоколе RDP (см. выше).
- **Обнаружение подделки записей кэша ARP**: обнаружение подделки записей кэша ARP, предпринятой с помощью атаки «злоумышленник в середине», или обнаружение сканирования сетевого коммутатора. Протокол ARP (протокол разрешения адреса) используется сетевым приложением или устройством для определения адреса Ethernet.
- **Обнаружение сканирования портов TCP/UDP**: обнаружение ПО сканирования портов, т. е. приложения, предназначенного для выявления открытых портов на узле путем отправления клиентских запросов на диапазон адресов портов и поиска активных портов для использования уязвимости службы. Дополнительную информацию об этом типе атаки см. в глоссарии.
- **Блокировать небезопасный адрес после обнаружения атаки**: IP-адреса, которые были обнаружены в качестве источников атак, будут добавлены в «черный» список, чтобы на некоторое время предотвратить подключение. Вы можете установить **срок хранения черного списка**, который определяет время, на которое будет заблокирован адрес после обнаружения атаки.
- **Уведомлять об обнаружении атаки**: включение уведомлений в области уведомлений

Windows в правом нижнем углу экрана.

• **Показывать уведомление при обнаружении атаки, использующей бреши в системе безопасности**: показывает уведомления, если обнаруживается атака, использующая бреши в системе безопасности, или если опасный объект пытается войти в систему через брешь.

Проверка пакетов

Тип анализа пакетов, который фильтрует данные, передаваемые по сети.

• **Разрешить входящее подключение к общим ресурсам администратора по протоколу SMB** : общие ресурсы администратора — это общие сетевые ресурсы по умолчанию, которые совместно используют разделы жесткого диска (*C$, D$*, ...) в системе вместе с системной папкой (*ADMIN$*). Отключение соединения с общими ресурсами администратора должны уменьшить возможные последствия угроз безопасности. Например, червь Conficker выполняет атаки перебором по словарю, чтобы подключиться к общим ресурсам администратора.

• **Запретить старые (неподдерживаемые) диалекты SMB**: запрет сеансов SMB, использующих старый диалект SMB, который не поддерживается IDS. Современные операционные системы Windows поддерживают старые диалекты SMB благодаря обратной совместимости со старыми операционными системами, такими как Windows 95. Злоумышленник может использовать старый диалект в сеансе SMB, чтобы избежать контроля трафика. Запретите старые диалекты SMB, если вашему компьютеру не нужно обмениваться файлами (или вообще осуществлять обмен данными SMB) с компьютером под управлением ОС Windows старой версии.

• **Запретить сеансы SMB без расширенной безопасности**: расширенная безопасность может быть использована во время согласования сеанса SMB, чтобы обеспечить более безопасный механизм аутентификации, чем аутентификация LAN Manager Challenge/Response (LM). Схема LM считается слабой и не рекомендуется для использования.

• **Запретить открытие исполняемых файлов на сервере за пределами доверенной зоны в протоколе SMB**: разрывает соединение при попытке запуска исполняемого файла (.exe, .dll и др.) из общей папки на сервере, который не относится к доверенной зоне файервола. Обратите внимание, что копирование исполняемых файлов из надежных источников может быть законным. Обратите внимание, что копирование исполняемых файлов из надежных источников может быть допустимо. С другой стороны, это обнаружение должно уменьшить риски нежелательного открытия файла на вредоносном сервере (например, если пользователь открыл файл, щелкнув гиперссылку на общий вредоносный исполняемый файл).

• **Запретить аутентификацию NTLM в протоколе SMB при подключении к серверу в доверенной зоне или за ее пределами**: протоколы, которые используют схемы аутентификации NTLM (обе версии), могут подвергаться атакам с попыткой пересылки учетных данных (известны как атаки SMB Relay, если речь идет о протоколе SMB). Если запретить аутентификацию NTLM с использованием сервера, который находится за пределами доверенной зоны, это поможет снизить риски пересылки учетных данных вредоносным сервером, который находится за пределами доверенной зоны. Кроме того, можно запретить аутентификацию NTLM с использованием сервера из доверенной зоны.

- **Разрешить подключение к службе диспетчера учетных записей безопасности**: для получения дополнительных сведений об этой службе см. раздел [MS-SAMR].

- **Разрешить подключение к службе локальной системы безопасности**: для получения дополнительных сведений об этой службе см. разделы [MS-LSAD] и [MS-LSAT].

- **Разрешить подключение к службе удаленного управления реестром**: для получения дополнительных сведений об этой службе см. раздел [MS-RRP].

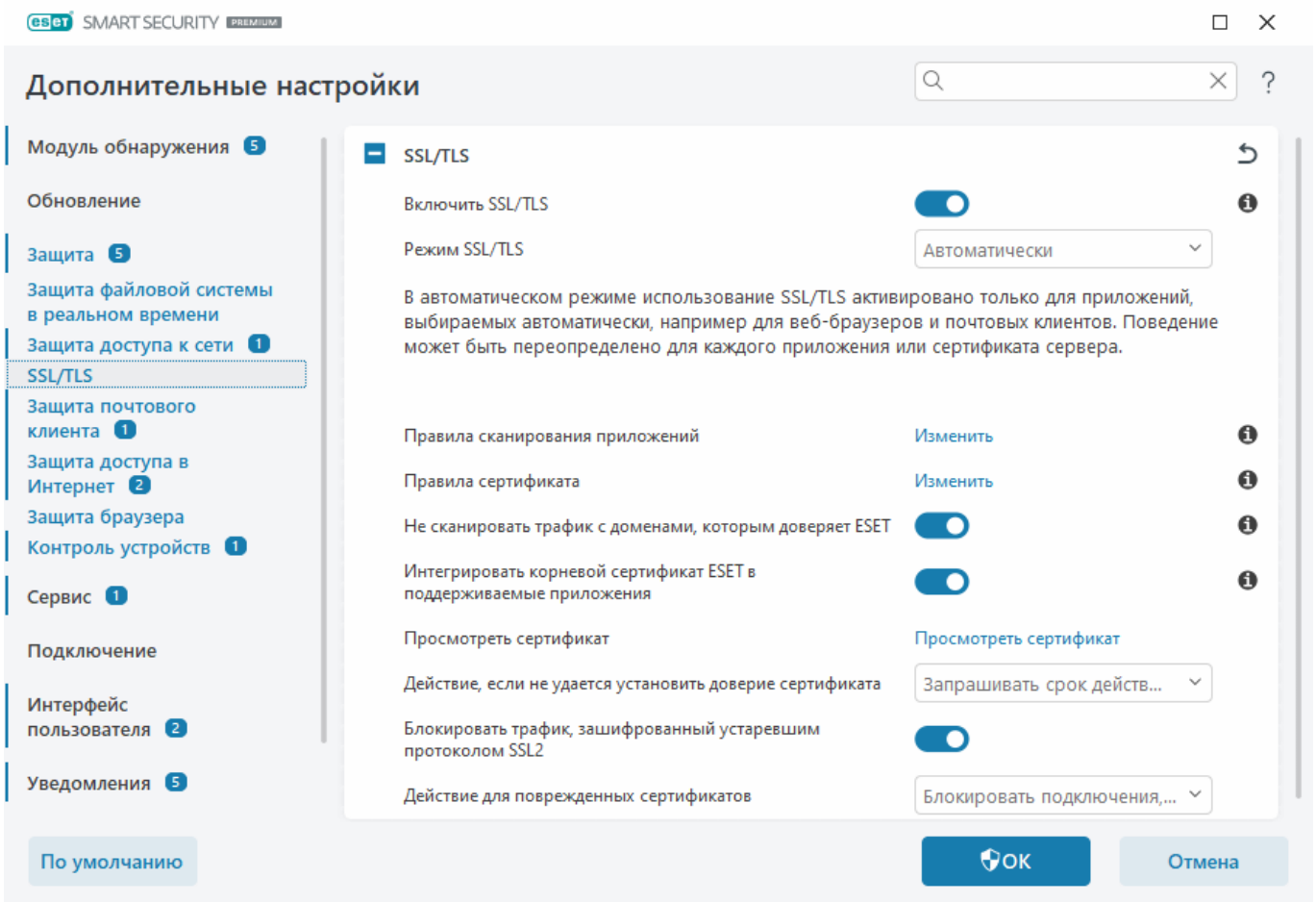
- **Разрешить подключение к службе диспетчера служб**: для получения дополнительных сведений об этой службе см. раздел [MS-SCMR].

- **Разрешить подключение к службе сервера**: для получения дополнительных сведений об этой службе см. раздел [MS-SRVS].

- **Разрешить подключение к другим службам**: другие службы MSRPC. MSRPC — это реализация Microsoft механизма DCE RPC. Кроме того, MSRPC может использовать именованные каналы, перенесенные в протокол SMB (протокол общего доступа к файлам сети) для транспорта (транспорт ncacn_np). Службы MSRPC предоставляют интерфейсы для удаленного доступа к операционной системе Windows и удаленного управления ею. За последние годы обнаружено несколько уязвимостей, которые используются в среде системы Windows MSRPC (червь Conficker, червь Sasser и др.). Отключите обмен данными со службами MSRPC, которые не нужно предоставлять для уменьшения последствий угроз безопасности (например, удаленное выполнение кода или атаки типа «Отказ в обслуживании»).

SSL/TLS

ESET Security Ultimate может выполнять проверку на наличие угроз при обмене данными, которые используют протокол SSL. Можно использовать различные режимы фильтрации для защищенных SSL-соединений, для которых используются доверенные сертификаты, неизвестные сертификаты или сертификаты, исключенные из проверки защищенных SSL-соединений. Чтобы изменить настройки SSL/TLS, откройте раздел Расширенные параметры > **Защита** > **SSL/TLS**.



Включить SSL/TLS: если этот параметр отключен, ESET Security Ultimate не будет сканировать обмен данными по протоколу SSL/TLS.

режим SSL/TLS доступен со следующими параметрами:

Режим фильтрации	Описание
Автоматический	Используемый по умолчанию режим, в котором сканируются только соответствующие приложения, такие как веб-браузеры и почтовые клиенты. Вы можете переопределить его, выбрав приложения, в которых следует сканировать обмен данными.
Интерактивно	При выполнении входа на новый защищенный SSL-сайт (с неизвестным сертификатом) на экран выводится диалоговое окно выбора действия. Этот режим позволяет создавать список сертификатов SSL и приложений, исключаемых из сканирования.
На основе политики	Выберите этот вариант, чтобы сканировать все защищенные SSL-соединения, кроме тех, которые защищены исключенными из проверки сертификатами. Если устанавливается новое соединение, использующее неизвестный заверенный сертификат, пользователь не получит уведомления, а само соединение автоматически будет фильтроваться. При доступе к серверу с ненадежным сертификатом, который помечен пользователем как доверенный (добавлен в список доверенных сертификатов), соединение с этим сервером разрешается, а содержимое канала связи фильтруется.

Правила сканирования приложений: позволяет настроить поведение ESET Security Ultimate для определенных приложений.

Правила сертификата: позволяет настроить поведение ESET Security Ultimate для конкретных сертификатов SSL.

Не сканировать трафик с доменами, которым доверяет ESET: если этот параметр включен, обмен данными с доверенными доменами будет исключен из сканирования. Надежность домена определяется встроенным белым списком, которым управляет компания ESET.

Интегрировать корневой сертификат ESET в поддерживаемые приложения — Для нормальной работы SSL-подключений в браузерах и почтовых клиентах необходимо добавить корневой сертификат ESET в список известных корневых сертификатов (издателей). При включении этого параметра ESET Security Ultimate автоматически добавляет сертификат ESET SSL Filter CA в известные браузеры (например, Opera). Для браузеров, использующих системное хранилище сертификатов, сертификат добавляется автоматически. Например, Firefox автоматически настроен для доверия корневым центрам в хранилище сертификатов системы.

Для установки сертификата в неподдерживаемые браузеры выберите **Просмотреть сертификат** > **Дополнительно** > **Копировать в файл...**, а затем вручную импортируйте его в браузер.

Действие, если не удается установить доверие сертификата: в некоторых случаях сертификат веб-сайта не может быть проверен с помощью хранилища доверенных корневых центров сертификации (TRCA) (например, сертификат с истекшим сроком действия, недоверенный сертификат, сертификат, недействительный для определенного домена, или подпись, которую можно проанализировать, но которая неправильно подписывает сертификат). Законный веб-сайт всегда использует доверенный сертификат. Если он его не предоставляет, это может означать, что злоумышленник расшифровывает ваш обмен данными или веб-сайт испытывает технические трудности.

Если установлен флажок **Запрашивать срок действия сертификата** (он установлен по умолчанию), пользователю будет предложено выбрать действие, которое следует предпринять во время установки зашифрованного соединения. На экране отобразится диалоговое окно для выбора действия, в котором можно принять решение о том, что следует сделать: пометить сертификат как доверенный или как исключенный. Если сертификат отсутствует в списке хранилища доверенных корневых сертификатов сертифицирующих органов, для оформления окна используется красный цвет. Если же сертификат есть в этом списке, окно будет оформлено зеленым цветом.

Можно выбрать вариант **Блокировать подключения, использующие данный сертификат**, чтобы всегда разрывать зашифрованные соединения с сайтом, использующим недоверенный сертификат.

Блокировать трафик, зашифрованный устаревшим протоколом SSL2: обмен данными с использованием более ранней версии протокола SSL будет автоматически блокироваться.

Действие для поврежденных сертификатов: поврежденный сертификат означает, что сертификат использует формат, который не распознается решением ESET Security Ultimate, или сертификат был получен поврежденным (например, перезаписан случайными данными). В этом случае мы рекомендуем оставить выбранным параметр **Блокировать подключения, использующие данный сертификат**. Если выбран параметр **Запрашивать срок действия сертификата**, пользователю будет предложено выбрать действие, которое следует предпринять при установке зашифрованного соединения.

Примеры с иллюстрациями

Следующие статьи из базы знаний ESET могут быть доступны только на английском языке:

- Уведомления касательно сертификатов в продуктах ESET для Windows для домашнего использования
- «Зашифрованный сетевой трафик: ненадежный сертификат» отображается при посещении веб-страниц

Правила сканирования приложений

Параметр **Правила сканирования приложений** может использоваться для настройки поведения ESET Security Ultimate в отношении определенных приложений, а также для запоминания выбранных действий, если для параметра **Режим SSL/TLS** выбран **интерактивный режим**. Список можно просмотреть и изменить в разделе Расширенные параметры > **Защита** > **SSL/TLS** > **Правила сканирования приложений** > **Изменить**.

Окно **Правила сканирования приложений** состоит из следующих элементов.

Столбцы

Приложение: выберите исполняемый файл в дереве каталогов или нажмите кнопку **...**, чтобы вручную ввести путь.

Действие сканирования: выберите **Сканировать** или **Пропустить**, чтобы сканировать или игнорировать обмен данными. Чтобы сканировать в автоматическом режиме и запрашивать действия в интерактивном, выберите элемент **Автоматически**. Выберите **Запрашивать**, чтобы всегда запрашивать действия пользователя.

Элементы управления

Добавить: добавление фильтрованных приложений.

Изменить: выберите приложение, которое нужно настроить, и нажмите кнопку **Изменить**.

Удалить: выберите приложение, которое нужно удалить, и нажмите кнопку **Удалить**.

Импорт/Экспорт: импорт приложений из файла или сохранение текущего списка приложений в файл.

OK/Отмена: нажмите кнопку **OK** для сохранения изменений или **Отмена** для их отмены.

Правила сертификата

Параметр **Правила сертификата** может использоваться для настройки поведения ESET Security Ultimate в отношении определенных сертификатов SSL, а также для запоминания выбранных действий, если для параметра **Режим SSL/TLS** выбран **интерактивный режим**. Список можно просмотреть и изменить в разделе Расширенные параметры > **Защита** > **SSL/TLS** > **Правила сертификата** > **Изменить**.

Окно **Правила сертификата** состоит из следующих элементов.

Столбцы

Имя : имя сертификата.

Издатель сертификата : имя создателя сертификата.

Субъект сертификата : это поле указывает на субъект, которому принадлежит открытый ключ, содержащийся в поле открытого ключа субъекта.

Доступ: в качестве значения параметра **Действие доступа** выберите **Разрешить** или **Заблокировать**, чтобы разрешить или заблокировать обмен данными, защищенный этим сертификатом, независимо от его надежности. Выберите **Автоматически**, чтобы разрешать доверенные сертификаты и предлагать варианты действий для ненадежных. Выберите **Запрашивать**, чтобы всегда запрашивать действия пользователя.

Сканировать: в качестве значения параметра **Действие сканирования** выберите **Сканировать** или **Пропустить**, чтобы сканировать или игнорировать обмен данными, защищенный этим сертификатом. Чтобы сканировать в автоматическом режиме и запрашивать действия в интерактивном, выберите элемент **Автоматически**. Выберите **Запрашивать**, чтобы всегда запрашивать действия пользователя.

Элементы управления

Добавить — выбор нового сертификата и настройка его параметров, связанных с доступом и сканированием.

Изменить: выберите сертификат, который нужно настроить, и нажмите кнопку **Изменить**.

Удалить: выберите сертификат, который нужно удалить, и щелкните **Удалить**.

OK/Отмена : нажмите кнопку **OK** для сохранения изменений или **Отмена** для их отмены.

Зашифрованный сетевой трафик

Если в системе настроено сканирование протокола SSL/TLS, диалоговое окно с запросом на выбор действия будет отображаться в двух случаях.

Во-первых, если веб-сайт использует непроверяемый или недействительный сертификат, а продукт ESET Security Ultimate настроен на выдачу запросов пользователю в таких случаях (по умолчанию запросы отображаются для непроверяемых сертификатов, а для недействительных — нет), появится диалоговое окно с запросом на **разрешение** или **блокирование** подключения. Если сертификата нет в Trusted Root Certification Authorities store (TRCA), то он считается ненадежным.

Во-вторых, если в качестве **SSL/TLS режима** выбран **интерактивный режим**, то при подключении к любому веб-сайту будет отображаться запрос на **сканирование** или **игнорирование**. Некоторые приложения проверяют SSL-трафик на предмет изменений и мониторинга. В таких случаях для сохранения работоспособности приложения программа ESET Security Ultimate должна SSL-трафик **игнорировать**.

Примеры с иллюстрациями

Следующие статьи из базы знаний ESET могут быть доступны только на английском языке:

- Уведомления касательно сертификатов в продуктах ESET для Windows для домашнего использования
- «Зашифрованный сетевой трафик: ненадежный сертификат» отображается при посещении веб-страниц

В каждом их этих случаев пользователь может сохранить в системе выбранное действие. Сохраненные действия хранятся в разделе Правила сертификата.

Защита почтового клиента

Чтобы настроить защиту почтового клиента, откройте раздел Расширенные параметры > **Защита** > **Защита почтового клиента** и сделайте выбор среди следующих опций конфигурации:

- Защита транспортного уровня
- Защита почтового ящика
- Управление списками адресов
- ThreatSense

Защита транспортного уровня

IMAP(S) и POP3(S) — самые распространенные протоколы, используемый для получения электронной почты в почтовых клиентах. Они используются для обмена данными по электронной почте с помощью приложения почтового клиента. Протокол IMAP — это еще один интернет-протокол для получения электронной почты, который имеет определенные преимущества перед POP3. Например, сразу несколько клиентов могут одновременно подключаться к одному и тому же почтовому ящику и передавать сведения о состоянии сообщения, в частности сведения о том, что сообщение было прочитано, удалено или на него был дан ответ. Модуль защиты, обеспечивающий такой контроль, автоматически запускается при запуске системы и остается активным в памяти.

ESET Security Ultimate обеспечивает защиту этих протоколов независимо от используемого почтового клиента и без необходимости перенастраивать почтовый клиент. По умолчанию сканируются все данные, передаваемые по протоколам POP3 и IMAP, независимо от используемых по умолчанию номеров портов POP3/IMAP.
Данные, передаваемые по протоколу MAPI, не сканируются. Но связь с сервером Microsoft Exchange может сканировать модуль интеграции в почтовых клиентах, таких как Microsoft Outlook.

ESET Security Ultimate также поддерживает сканирование протоколов IMAPS (585, 993) и POP3S (995), которые для передачи информации между сервером и клиентом используют зашифрованный канал. ESET Security Ultimate проверяет соединения, использующие методы шифрования SSL и TLS.
Зашифрованные соединения сканируются по умолчанию. Чтобы просмотреть настройки модуля сканирования, откройте раздел Расширенные параметры > **Защита** > SSL/TLS.

Чтобы настроить защиту почтового транспорта, откройте раздел Расширенные параметры > **Защита** > **Защита почтового клиента** > **Защита почтового транспорта**.

Включить защиту почтового транспорта: если этот параметр включен, обмен данными почтового транспорта будет сканироваться решением ESET Security Ultimate.

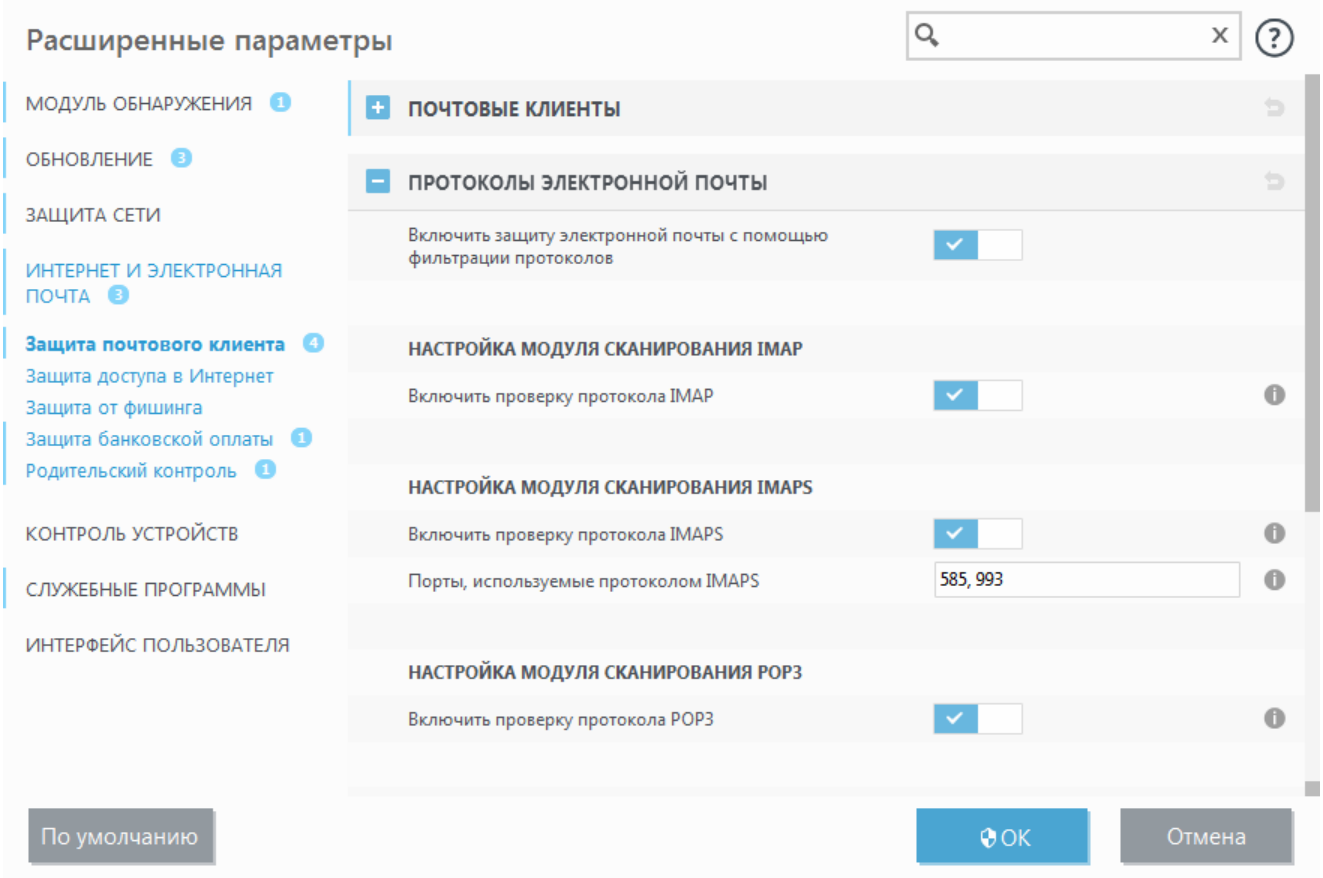
Вы можете выбрать, какие протоколы почтового транспорта будут сканироваться, щелкнув переключатель рядом со следующими опциями (по умолчанию включено сканирование всех протоколов):

- **Сканировать почтовый транспорт IMAP**
- **Сканировать почтовый транспорт IMAPS**
- **Сканировать почтовый транспорт POP3**
- **Сканировать почтовый транспорт POP3S**

По умолчанию ESET Security Ultimate будет сканировать обмен данными по протоколам IMAPS и POP3S на стандартных портах. Чтобы добавить пользовательские порты для протоколов IMAPS и POP3S, добавьте их в текстовое поле рядом с элементом **Порты, используемые протоколом IMAPS** или **Порты, используемые протоколом POP3S**. Номера портов следует разделять запятой.

Исключенные приложения: позволяет исключить определенные приложения из сканирования функцией защиты почтового транспорта. Это полезно, когда защита доступа в Интернет вызывает проблемы совместимости.

Исключенные IP-адреса: позволяет исключить определенные удаленные адреса из сканирования функцией защиты почтового транспорта. Это полезно, когда защита доступа в Интернет вызывает проблемы совместимости.



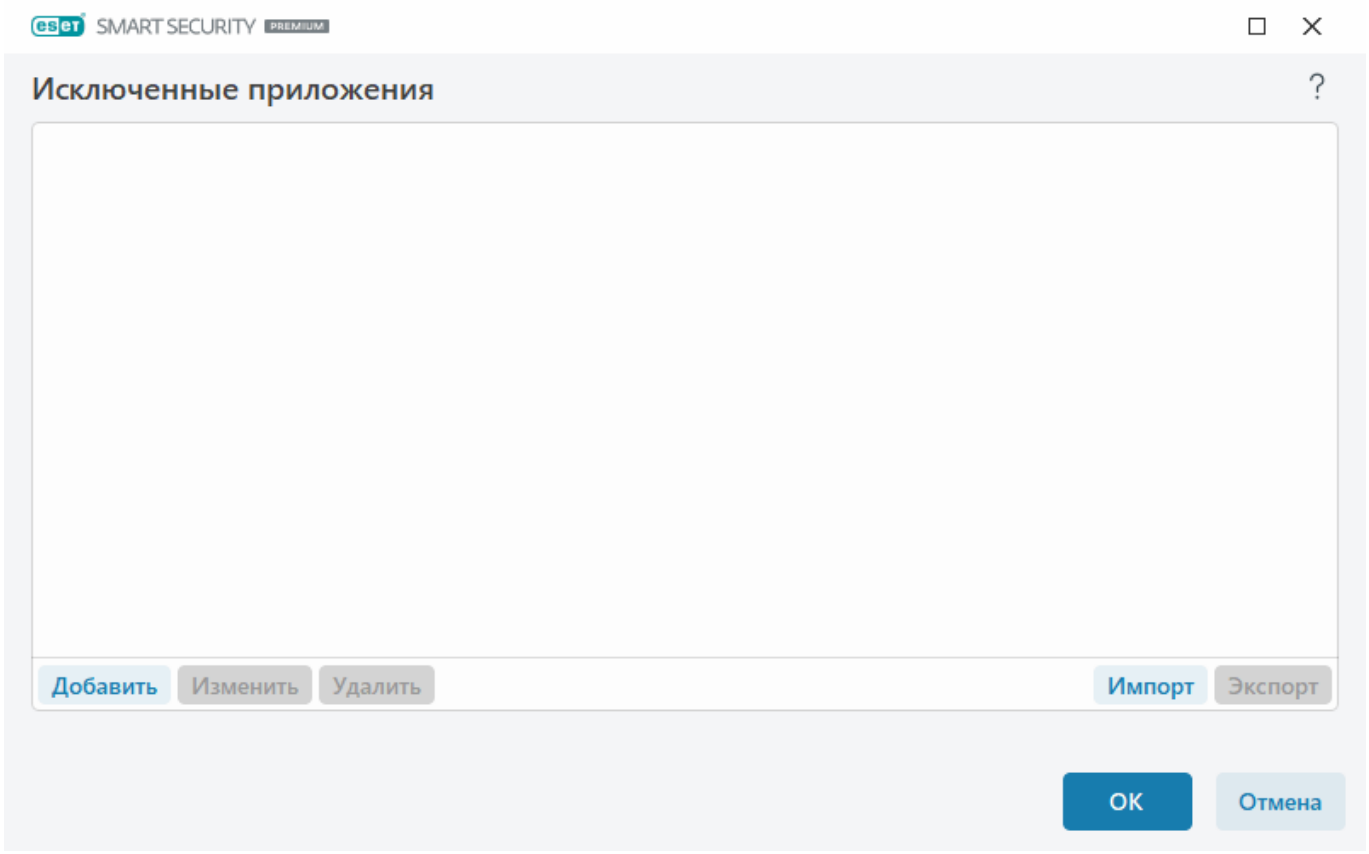
Исключенные приложения

Чтобы исключить сканирование обмена данными для определенных приложений, добавьте их в список. Соединения выделенных приложений по протоколам HTTP(S)/POP3(S)/IMAP(S) не будут проверяться на наличие угроз. Рекомендуется использовать эту возможность только для тех приложений, которые работают некорректно, если их соединения проверяются.

Запущенные приложения и службы будут доступны здесь автоматически, когда вы щелкните **Добавить**. Щелкните **...** и перейдите к приложению, чтобы добавить исключение вручную.

Изменить: изменение выбранных в списке записей.

Удалить: удаление выбранных записей из списка.



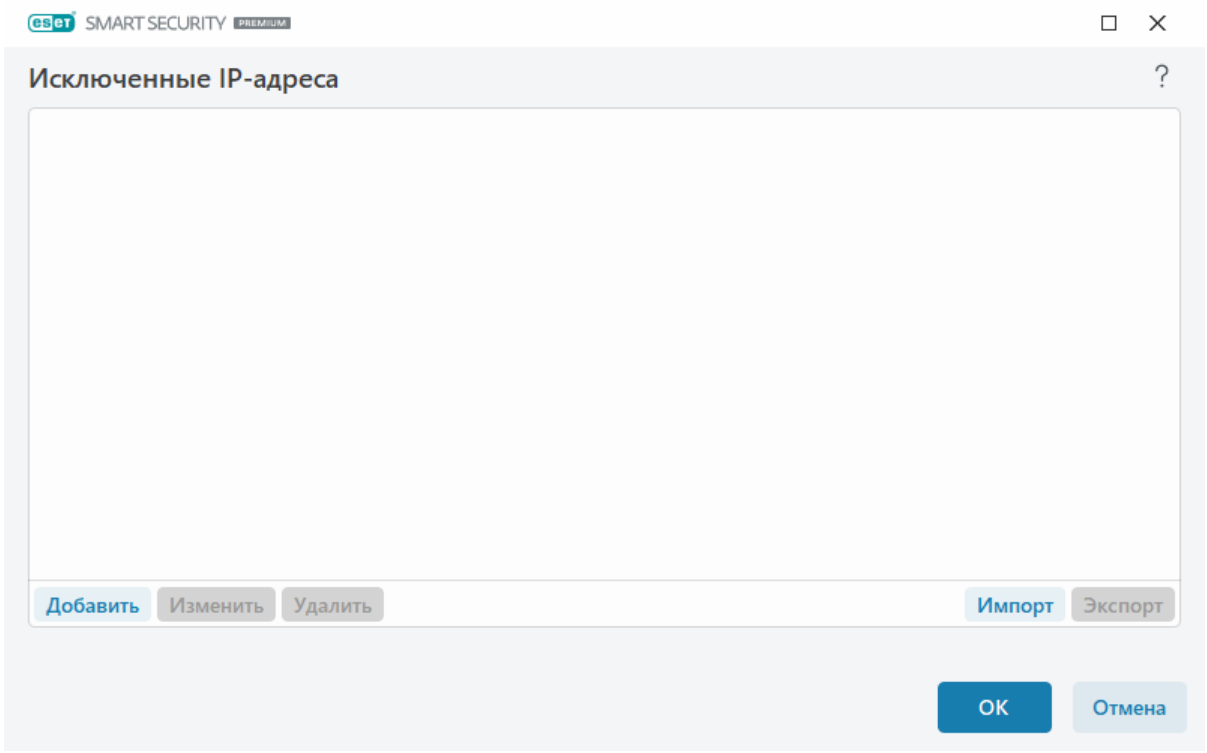
Исключенные IP-адреса

Записи в списке будут исключены из сканирования. Соединения по протоколам HTTP(S)/POP3(S)/IMAP(S), в которых участвуют выбранные адреса, не будут проверяться на наличие угроз. Этот параметр рекомендуется использовать только для заслуживающих доверия адресов.

Щелкните **Добавить**, чтобы исключить IP-адрес, диапазон адресов или подсеть удаленного узла.

Щелкните **Изменить**, чтобы изменить выбранный IP-адрес.

Нажмите кнопку **Удалить**, чтобы удалить выделенные записи из списка.



Примеры IP-адресов

Добавить адрес IPv4:
Один адрес: добавляет IP-адрес отдельного компьютера (например, *192.168.0.10*).
Диапазон адресов: введите начальный и конечный IP-адреса, чтобы задать диапазон IP-адресов нескольких компьютеров (например, *192.168.0.1–192.168.0.99*).
Подсеть: подсеть (группа компьютеров), заданная IP-адресом и маской. Например, 255.255.255.0 — это маска сети для подсети 192.168.1.0. Чтобы исключить всю подсеть, введите *192.168.1.0/24*.
Добавить адрес IPv6:
Один адрес: добавляет IP-адрес отдельного компьютера (например, *2001:718:1c01:16:214:22ff:fec9:ca5*).
Подсеть: подсеть (группа компьютеров), заданная IP-адресом и маской (например, *2002:c0a8:6301:1::1/64*).

Защита почтового ящика

Интеграция ESET Security Ultimate с почтовым клиентом увеличивает уровень активной защиты от вредоносного кода в сообщениях электронной почты.

Чтобы настроить защиту почтового ящика, откройте раздел Расширенные параметры > **Защита** > **Защита почтового клиента** > **Защита почтового ящика**.

Включить защиту электронной почты с помощью подключаемых модулей клиента: если этот параметр отключен, защита электронной почты с помощью подключаемых модулей клиента выключена.

Выберите письма для сканирования:

- **Полученные сообщения**
- **Отправленные сообщения**

- **Прочитанные сообщения**

- **Измененное сообщение электронной почты**

> Рекомендуем оставить параметр **Включить защиту электронной почты с помощью подключаемых модулей клиента** включенным. Даже если интеграция отключена или не работает, передача данных по электронной почте остается защищенной модулем Защита почтового транспорта (IMAP/IMAPS и POP3/POP3S).

Сканирование на наличие спама

Нежелательные сообщения, называемые спамом, входят в число самых серьезных проблем современных телекоммуникационных технологий. Доля спама в общем объеме передаваемых по электронной почте сообщений составляет около 30 %. Защита почтового клиента от спама служит решением этой проблемы. Используя несколько принципов защиты электронной почты, модуль защиты почтового клиента от спама обеспечивает превосходную фильтрацию и не пропускает в папку входящих сообщений нежелательную почту. Одним из важных принципов обнаружения спама является распознавание нежелательных сообщений электронной почты на основе предварительно определенных доверенных адресов (разрешенных) и спам-адресов (заблокированных).

Основным методом обнаружения спама является сканирование свойств сообщения электронной почты. Полученные сообщения сканируются на основные критерии защиты от спама (определения сообщения, статистические эвристики, алгоритмы распознавания и другие уникальные методы). Результатом работы этих методов является значение индекса, по которому можно с высокой степенью достоверности определить, является ли сообщение спамом.

Включить защиту почтового клиента от спама: если этот параметр включен, полученные сообщения будут сканироваться на наличие спама.

Использовать расширенный сканер на наличие спама: периодически будут загружаться дополнительные данные для защиты от спама, что расширяет возможности защиты от спама и улучшает результаты.

Регистрация оценки нежелательности: модуль защиты от спама ESET Security Ultimate присваивает оценку нежелательности каждому просканированному сообщению. Сообщение будет записано в журнал защиты от спама (главное окно программы > **Сервис** > **Файлы журнала** > **Защита почтового клиента от спама**).

- **Нет**: оценка, полученная в результате сканирования на предмет спама, не вносится в журнал.

- **Реклассифицировано и помечено как спам**: если выбран этот параметр, оценки нежелательности всех сообщений, помеченных как SPAM, будут записываться в журнал.

- **Все**: в журнал будут записываться все сообщения вместе с оценкой нежелательности.

Если в папке нежелательной почты выбрать сообщение и выбрать команду **Классифицировать выбранные сообщения как НЕ спам**, выбранное сообщение переместится в папку входящей почты. Если в папке входящих сообщений выбрать сообщение, которые вы считает нежелательным, и выбрать команду **Классифицировать выбранные сообщения как НЕ спам**, выбранное сообщение переместится в папку спама. Вы можете выбрать несколько сообщений и работать со всеми ими одновременно.

Оптимизация работы с вложениями: если оптимизация отключена, все вложения сканируются незамедлительно. Возможно снижение производительности почтового клиента.

Интеграции: позволяет интегрировать защиту почтового ящика в почтовый клиент. Дополнительные сведения см. в разделе Интеграции.

Реагирование: позволяет настроить обработку спам-сообщений. Дополнительные сведения см. в разделе Реагирование.

Интеграции

Интеграция ESET Security Ultimate с почтовым клиентом увеличивает уровень активной защиты от вредоносного кода в сообщениях электронной почты. Если ваш почтовый клиент поддерживается, в ESET Security Ultimate можно включить интеграцию. При этом панель инструментов ESET Security Ultimate вставляется непосредственно в почтовый клиент, обеспечивая более эффективную защиту электронной почты. Чтобы изменить настройки интеграции, откройте раздел Расширенные параметры > **Защита** > **Защита почтового клиента** > **Защита почтового ящика** > **Интеграция**.

Инеграция с Microsoft Outlook: В настоящее время единственным поддерживаемым почтовым клиентом является Microsoft Outlook. Защита электронной почты работает как плагин. Главное преимущество подключаемого модуля заключается в том, что он не зависит от используемого протокола. При получении почтовым клиентом зашифрованного сообщения оно расшифровывается и передается модулю сканирования. Полный список поддерживаемых версий Microsoft Outlook см. в этой статье базы знаний ESET.

Расширенная обработка почтового клиента: обработка дополнительных событий Outlook Messaging API (MAPI) — «Объект изменен» (`fnevObjectModified`) и «Объект создан» (`fnevObjectCreated`). Если при работе с почтовым клиентом наблюдается снижение быстродействия системы, отключите этот параметр.

Панель инструментов Microsoft Outlook

Защита Microsoft Outlook работает в виде плагина. После установки ESET Security Ultimate эта панель инструментов, содержащая опции защиты от вирусов и защиты почтового клиента от спама, добавляется в Microsoft Outlook:

Спам: позволяет пометить выбранные сообщения как спам. «Отпечаток» помеченного сообщения будет отправлен на центральный сервер, на котором хранятся сигнатуры спама. «Отпечаток» помеченного сообщения будет отправлен на центральный сервер, на котором хранятся сигнатуры спама. Если на сервер поступает несколько аналогичных «отпечатков» от

разных пользователей, такое сообщение в дальнейшем будет классифицироваться как спам.

Не спам: позволяет пометить выбранные сообщения как не являющиеся спамом.

Адрес отправителя спама (заблокировано, список рассылающих спам адресов): добавляет новый адрес отправителя в список адресов как заблокированный. Все сообщения, полученные с внесенных в список адресов, будут автоматически классифицироваться как спам.

Остерегайтесь подделки адреса отправителя, направленной на то, чтобы заставить получателя прочесть сообщение и ответить на него.

Доверенные адреса (разрешено, список доверенных адресов): добавляет новый адрес отправителя в список адресов как разрешенный. Все сообщения, полученные с разрешенных адресов, никогда не будут автоматически классифицироваться как спам.

ESET Security Ultimate: дважды щелкните значок, чтобы открыть главное окно ESET Security Ultimate.

Повторное сканирование сообщения: позволяет запустить проверку электронной почты вручную. Можно указать сообщения, которые будут проверяться, и активировать повторное сканирование полученных сообщений. Дополнительные сведения см. в разделе Защита почтового ящика.

Настройки модуля сканирования: отображаются опции для настройки защиты почтового ящика.

Настройка модуля антиспама: отображаются опции для настройки защиты почтового ящика.

Адресные книги: открывается окно Управление списками адресов, содержащее списки исключенных, доверенных адресов и адресов отправителей спама.

Окно подтверждения

Это уведомление предназначено для подтверждения того, что пользователю действительно нужно выполнить выбранное действие, и для предотвращения тем самым возможных ошибок.

Кроме того, в окне также есть возможность отключить подтверждения.

Повторно сканировать сообщения

Панель инструментов ESET Security Ultimate, интегрированная в почтовые клиенты, дает пользователю возможность указать ряд параметров для проверки электронной почты. Параметром **Повторно сканировать сообщения** предлагается два описанных далее режиме сканирования.

Все сообщения в текущей папке: сканируются сообщения в отображаемой сейчас папке.

Только выбранные сообщения: сканируются только помеченные пользователем сообщения.

Флажок **Повторно сканировать уже сканированные сообщения** дает пользователю возможность выполнить еще одно сканирование сообщений, которые уже были

просканированы ранее.

Реагирование

На основании результатов сканирования сообщений решение ESET Security Ultimate может перемещать просканированные сообщения или добавлять пользовательский текст в тему. Эти параметры можно настроить в разделе Расширенные параметры > **Защита** > **Защита почтового клиента** > **Защита почтового ящика** > **Реагирование**.

Защита почтового клиента от спама в ESET Security Ultimate позволяет настроить для сообщений следующие параметры:

Добавить текст к теме сообщения: позволяет добавлять настраиваемую строку префикса в поле темы сообщений, которые классифицированы как спам. **Текст** по умолчанию — [SPAM].

Перемещать в папку для спама: если этот флажок установлен, сообщения со спамом будут перемещаться в стандартную папку для нежелательной почты, а сообщения, повторно классифицированные как не спам, — в папку со входящей почтой. Если щелкнуть сообщение правой кнопкой мыши и выбрать в контекстном меню пункт ESET Security Ultimate, появится возможность выбрать один из нескольких вариантов действий.

Переместить в пользовательскую папку: если этот параметр включен, спам-сообщения будут перемещаться в папку, указанную ниже.

Папка — выбор папки, в которую будут перемещаться обнаруженные зараженные сообщения электронной почты.

Если есть сообщение, содержащее обнаружение, по умолчанию ESET Security Ultimate пытается очистить сообщение. Если сообщение очистить не удается, с помощью параметра **Предпринимаемое действие, если очистка невозможна** можно выбрать нужный вариант:

- **Ничего не предпринимать** — в этом случае программа будет выявлять зараженные вложения, но не будет выполнять никаких действий с сообщениями электронной почты.
- **Удалить сообщение** — программа будет уведомлять пользователя о заражениях и удалять сообщения.
- **Переместить сообщение в папку «Удаленные»** — зараженные сообщения будут автоматически перемещаться в папку «Удаленные».
- **Переместить сообщение в папку** (действие по умолчанию). Зараженные сообщения будут автоматически перемещаться в указанную папку.

Папка — выбор папки, в которую будут перемещаться обнаруженные зараженные сообщения электронной почты.

Отмечать сообщения со спамом как прочитанные: установите этот флажок, чтобы автоматически помечать нежелательные сообщения как прочитанные. Это помогает сосредоточиться на «чистых» сообщениях.

Отмечать повторно классифицированные сообщения как непрочитанные: сообщения, первоначально классифицированные как спам, а затем помеченные как «чистые», будут

отображаться как непрочитанные.

После проверки к сообщению электронной почты может быть прикреплено уведомление с результатами сканирования. Вы можете выбрать **Добавлять уведомление к полученным и прочитанным сообщениям электронной почты** или **Добавлять уведомление к отправленным сообщениям**. Обратите внимание, что в некоторых случаях уведомления могут отсутствовать в проблемных HTML-сообщениях или в сообщениях, поврежденных вредоносными программами. Уведомления могут быть добавлены к входящим и прочитанным сообщениям или к исходящим сообщениям (или и к тем, и к другим). Доступны следующие варианты:

- **Никогда**: уведомления не добавляются.
- **При обнаружении**: будут отмечены только сообщения, содержащие вредоносные программы (по умолчанию).
- **Для всей электронной почты при сканировании**: программа будет добавлять уведомления ко всем сканируемым сообщениям электронной почты.

Изменять тему полученных и прочитанных сообщений электронной почты/Изменять тему отправленных сообщений электронной почты: включите эту опцию, чтобы добавлять в сообщения пользовательский текст, указанный ниже.

Текст для добавления в тему обнаруженных сообщений электронной почты. Этот шаблон можно изменить, если нужно отредактировать формат префикса, добавляемого к зараженному сообщению. Эта функция заменяет тему сообщения Hello на формат [обнаружение %DETECTIONNAME%] Hello. Переменной %DETECTIONNAME% обозначается обнаружение.

Управление списками адресов

Функция защиты почтового клиента от спама в ESET Security Ultimate позволяет настраивать различные параметры для списков адресов. Для настройки списков адресов откройте раздел Расширенные параметры > **Защита** > **Защита почтового клиента** > **Управление списками адресов**.

Включить список адресов пользователя — включите эту опцию, чтобы активировать список адресов пользователя.

Список адресов пользователя — список адресов электронной почты, где можно добавлять, редактировать или удалять адреса для определения правил защиты от спама. Правила в этом списке будут применяться к текущему пользователю.

Включить глобальный список адресов — включите эту опцию, чтобы активировать глобальный список адресов, общий для всех пользователей на этом устройстве.

Глобальный список адресов — список адресов электронной почты, где можно добавлять, редактировать или удалять адреса для определения правил защиты от спама. Правила в этом списке будут применяться ко всем пользователям.

Автоматически разрешать и добавлять в список адресов пользователя

Считать адреса из адресной книги доверенными — Адреса из вашего списка контактов будут расцениваться как доверенные без добавления в список адресов пользователя.

Добавить адреса получателей из исходящих сообщений — добавьте адреса получателей из отправленных сообщений в список адресов пользователя как разрешенные.

Добавить адреса из сообщений, реклассифицированных как НЕ спам, — добавьте адреса отправителей из сообщений, реклассифицированных как НЕ спам, в список адресов пользователя как разрешенные.

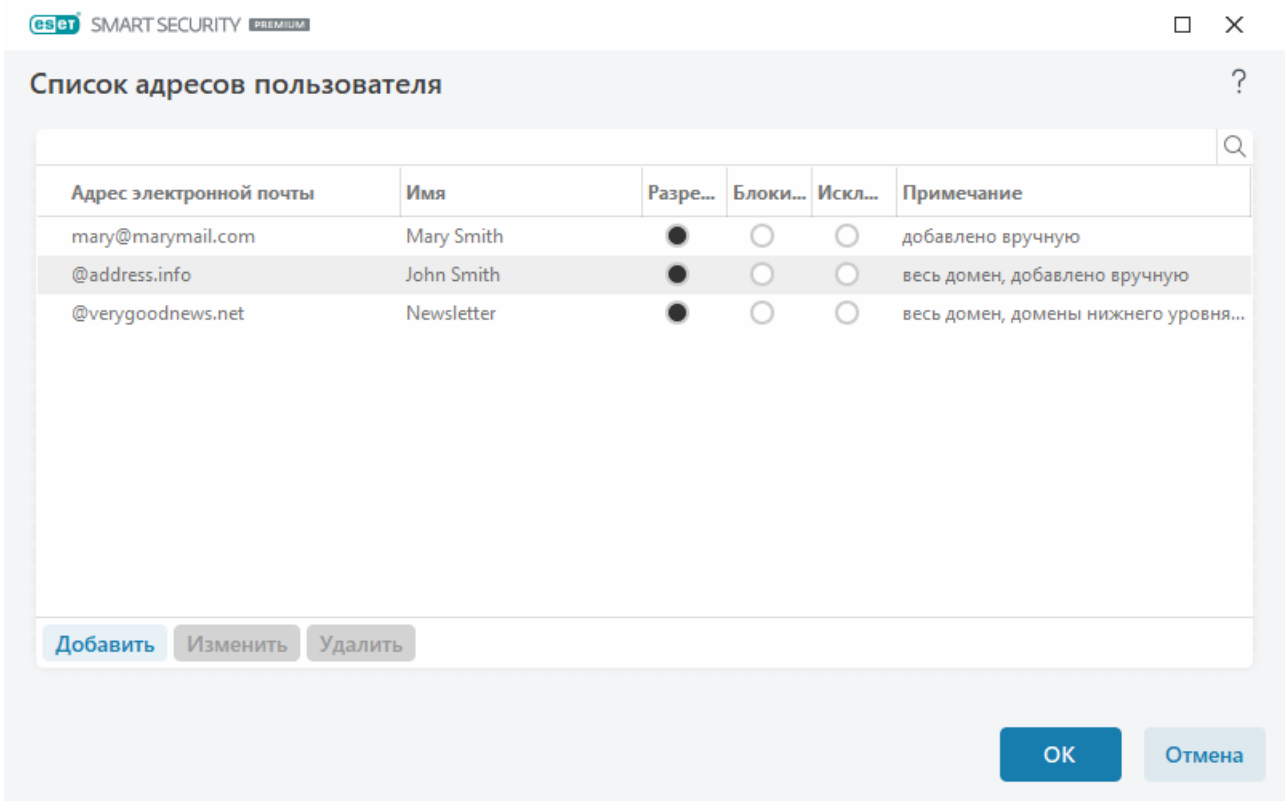
Автоматически добавлять в список адресов пользователя как исключение

Добавить адреса из собственных учетных записей — добавьте свои адреса из существующих учетных записей почтовых клиентов в список адресов пользователя как исключения.

Списоки адресов

Для защиты от нежелательных электронных писем ESET Security Ultimate позволяет классифицировать адреса электронной почты в списках адресов.

Чтобы изменить списки адресов, откройте Расширенные параметры > **Защита** > **Защита почтового клиента** > **Управление списками адресов** и щелкните **Изменить** рядом с элементом **Список адресов пользователя** или **Глобальный список адресов**.



Столбцы

Адрес электронной почты — адрес, к которому будет применяться правило. Подстановочные знаки не поддерживаются.

Имя — имя пользовательского правила.

Разрешить/Заблокировать/Исключение — кнопки-переключатели, используемые для определения действия, которое нужно предпринять для адреса электронной почты (щелкните переключатель в предпочтительном столбце, чтобы быстро изменить действие):

- **Разрешить** — адреса, которые считаются безопасными и с которых необходимо получать сообщения.
- **Заблокировать** — адреса, которые считаются небезопасными/спамом и с которых не нужно получать сообщения.
- **Исключение** — адреса, которые всегда проверяются на наличие спама и которые могут быть подделаны и использованы для отправки спама.

Примечание — информация о том, как было создано правило и применяется ли оно ко всему домену или к доменам более низкого уровня.

Управление адресами

- **Добавить** — щелкните, чтобы добавить правило для нового адреса.
- **Изменить** — выберите и щелкните, чтобы изменить существующее правило.
- **Удалить** — выберите и щелкните, чтобы удалить правило из списка адресов.

Добавление или изменение адреса

В этом окне можно добавить или изменить адрес в Управление списками адресов и конфигурировать предпринимаемые действия:

Адрес электронной почты — адрес, к которому будет применяться правило.

Имя — имя пользовательского правила.

Действие — действие, которое необходимо предпринять, если адрес электронной почты контакта совпадает с адресом, указанным в поле **Адрес электронной почты**:

• **Разрешить** — адреса, которые считаются безопасными и с которых необходимо получать сообщения.

• **Заблокировать** — адреса, которые считаются небезопасными/спамом и с которых не нужно получать сообщения.

• **Исключение** — адреса, которые всегда проверяются на наличие спама и которые могут быть подделаны и использованы для отправки спама.

Весь домен: установите этот флажок, чтобы применить правило ко всему домену контакта (не только к адресу, указанному в поле **Адрес электронной почты**, а ко всем адресам электронной почты в домене *address.info*).

Домены нижнего уровня: установите этот флажок, чтобы правило применялась к доменам нижнего уровня контакта (*address.info* представляет домен, а *my.address.info* — поддомен).

Результат обработки адреса

При добавлении новых адресов или изменении действия, предпринятого для адреса электронной почты, в ESET Security Ultimate отображаются уведомления. Содержимое сообщений варьируется в зависимости от выполняемого действия.

Если нужно, чтобы в дальнейшем конкретное действие выполнялось автоматически без вывода сообщений, установите флажок **Больше не задавать этот вопрос**.

ThreatSense

ThreatSense — это технология, состоящая из множества сложных методов обнаружения угроз. Эта технология является упреждающей, т. е. она защищает от новой угрозы уже в начале ее распространения. При этом используется сочетание анализа и моделирования кода, обобщенных сигнатур и сигнатур вирусов, которые совместно значительно повышают уровень безопасности компьютера. Модуль сканирования может контролировать несколько потоков данных одновременно, что делает эффективность и количество обнаруживаемых угроз максимальными. Технология ThreatSense также успешно уничтожает руткиты.

Для модуля ThreatSense можно настроить несколько параметров сканирования:

- расширения и типы файлов, подлежащих сканированию;
- сочетание различных методов обнаружения;
- уровни очистки и т. д.

Чтобы открыть окно параметров, щелкните **ThreatSense** в окне расширенных параметров любого модуля, использующего технологию ThreatSense (см. ниже). Разные сценарии обеспечения безопасности могут требовать различных настроек. Поэтому технологию ThreatSense можно настроить отдельно для каждого из перечисленных далее модулей защиты.

- Защита в режиме реального времени
- Сканирование в состоянии простоя
- сканирование при запуске
- Защита документов
- Защита почтового клиента
- защита доступа в Интернет;
- Сканирование компьютера

Параметры ThreatSense хорошо оптимизированы для каждого из модулей, а их изменение значительно влияет на поведение системы. Например, изменение параметров сканирования упаковщиков в режиме реального времени или включение расширенной эвристики в модуле защиты файловой системы в режиме реального времени может замедлить работу системы (обычно только новые файлы сканируются с применением этих методов). Рекомендуется не изменять параметры ThreatSense по умолчанию ни для каких модулей, кроме модуля «Сканирование компьютера».

Сканируемые объекты

В этом разделе можно указать компоненты и файлы компьютера, которые будут сканироваться на наличие заражений.

Оперативная память: сканирование на наличие угроз, которые атакуют оперативную память системы.

Загрузочные секторы/UEFI. Загрузочные секторы сканируются на наличие вредоносных программ в основной загрузочной записи. Дополнительные сведения о UEFI см. в глоссарии.

Почтовые файлы. DBX (Outlook Express) и EML

Архивы. Программа поддерживает такие расширения, как ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE, и многие другие.

Самораспаковывающиеся архивы. Тип архивов (SFX), содержимое которых может извлекаться автоматически.

Программы сжатия исполняемых файлов: в отличие от стандартных типов архивов,

программы сжатия исполняемых файлов после запуска распаковываются в памяти. Благодаря эмуляции кода модуль сканирования распознает не только стандартные статические упаковщики (UPX, yoda, ASPack, FSG и т. д.), но и множество других типов упаковщиков.

Параметры сканирования

Выберите способы сканирования системы на предмет заражений. Доступны следующие варианты:

Эвристический анализ: анализ вредоносной активности программ с помощью специального алгоритма. Главным достоинством этого метода является способность идентифицировать вредоносные программы, сведения о которых отсутствуют в существующей версии модуля обновления. Недостатком же является вероятность (очень небольшая) ложных тревог.

Расширенный эвристический анализ/сигнатуры распределенных сетевых атак: для расширенного эвристического анализа используется уникальный эвристический алгоритм компании ESET, который оптимизирован для обнаружения компьютерных червей и троянских программ и написан на высокоуровневых языках программирования. Использование расширенной эвристики значительным образом увеличивает возможности продуктов ESET по обнаружению угроз. С помощью сигнатур осуществляется точное обнаружение и идентификация вирусов. Система автоматического обновления обеспечивает наличие новых сигнатур через несколько часов после обнаружения угрозы. Недостатком же сигнатур является то, что они позволяют обнаруживать только известные вирусы (или их незначительно модифицированные версии).

Очистка

Параметры очистки определяют поведение ESET Security Ultimate при очистке объектов. Предусмотрено четыре уровня очистки.

ThreatSense имеет такие уровни исправления проблем (т. е. очистки):

Исправление в ESET Security Ultimate

Уровень очистки	Описание
Всегда исправлять обнаружения	Пытаться исправлять обнаружения при очистке объектов без вмешательства конечного пользователя. В некоторых случаях (например, с системными файлами), если обнаружение не удается исправить, обнаруженный объект оставляется в исходном расположении.
Исправлять обнаружения, если это безопасно, в другом случае оставить	Пытаться исправлять обнаружения при очистке объектов без вмешательства конечного пользователя. В некоторых случаях (например, системные файлы или архивы, которые содержат и чистые, и зараженные файлы), если обнаружение не удается исправить, обнаруженный объект остается в исходном расположении.

Уровень очистки	Описание
Исправлять обнаружения, если это безопасно, в другом случае спрашивать	Пытаться исправлять обнаружения при очистке объектов. В некоторых случаях, если ни одно из действий выполнить невозможно, конечный пользователь получает интерактивное предупреждение, в котором следует выбрать действие по исправлению (например, удалить или проигнорировать). Этот параметр рекомендуется в большинстве случаев.
Всегда спрашивать у конечного пользователя	Конечному пользователю отображается интерактивное окно при очистке объектов, и он должен выбрать действие по исправлению (например, удалить или пропустить). Этот уровень предназначен для более опытных пользователей, которые знают, какие действия следует предпринять в случае обнаружения.

Исключения

Расширением называется часть имени файла, отделенная от основной части точкой. Оно определяет тип файла и его содержимое. Этот раздел ThreatSense позволяет определить типы файлов, подлежащих сканированию.

Другое

При настройке параметров модуля ThreatSense для сканирования компьютера по требованию также доступны описанные ниже параметры из раздела **Другое**.

Сканировать альтернативные потоки данных (ADS): альтернативные потоки данных, используемые файловой системой NTFS, — это связи файлов и папок, которые не обнаруживаются при использовании обычных методов сканирования. Многие заражения маскируются под альтернативные потоки данных, пытаясь избежать обнаружения.

Запускать фоновое сканирование с низким приоритетом: каждый процесс сканирования потребляет некоторое количество системных ресурсов. Если пользователь работает с ресурсоемкими программами, можно активировать фоновое сканирование с низким приоритетом и высвободить тем самым ресурсы для других приложений.

Журнал всех объектов. Журнал проверки отображает все отсканированные файлы в самораспаковывающихся архивах, даже незараженные (может создавать большое количество данных журнала сканирования и увеличивать размер его файла).

Включить оптимизацию Smart: при включенной оптимизации Smart используются оптимальные параметры для обеспечения самого эффективного уровня сканирования с сохранением максимально высокой скорости. Разные модули защиты выполняют интеллектуальное сканирование, применяя отдельные методы для различных типов файлов. Если оптимизация Smart отключена, при сканировании используются только пользовательские настройки ядра ThreatSense каждого модуля.

Сохранить отметку о времени последнего доступа: установите этот флажок, чтобы сохранить исходное значение времени доступа к сканируемым файлам, а не обновлять их (например, для использования с системами резервного копирования данных).

Ограничения

В разделе «Ограничения» можно указать максимальный размер объектов и уровни вложенности архивов для сканирования.

Параметры объектов

Максимальный размер объекта: определяет максимальный размер объектов, подлежащих сканированию. Данный модуль защиты от вирусов будет сканировать только объекты меньше указанного размера. Этот параметр рекомендуется менять только опытным пользователям, у которых есть веские основания для исключения из сканирования больших объектов. Значение по умолчанию: Не ограничено.

Максимальная продолжительность сканирования объекта (с): определяет максимальное значение времени для сканирования файлов в объекте-контейнере (например, в архиве RAR/ZIP или в электронном письме с несколькими вложениями). Эта настройка не применяется к отдельным файлам. Если пользователь укажет собственное значение и указанное время истечет, сканирование будет остановлено как можно скорее вне зависимости от того, завершено ли сканирование каждого файла в объекте-контейнере.
Если речь идет об архиве с большими файлами, сканирование будет прекращено не раньше, чем произойдет извлечение файла из архива (например, когда пользователь задал значение в 3 секунды, но извлечение файла занимает 5 секунд). По истечении этого времени остальные файлы в архиве сканироваться не будут.
Чтобы ограничить время сканирования, в том числе для архивов большого размера, используйте параметры **Максимальный размер объекта** и **Максимальный размер файла в архиве** (не рекомендуется в связи с возможными проблемами безопасности).
Значение по умолчанию: Не ограничено.

Настройки сканирования архивов

Уровень вложенности архивов: определяет максимальную глубину проверки архивов. Значение по умолчанию: 10.

Максимальный размер файла в архиве: этот параметр позволяет задать максимальный размер файлов в архиве (при их извлечении), которые должны сканироваться. Максимальное значение — **3 ГБ**.

> Не рекомендуется изменять значения по умолчанию, так как обычно для этого нет особой причины.

Защита доступа в Интернет

В разделе «Защита доступа в Интернет» можно настроить расширенные параметры модуля Защита Интернета. В разделе Расширенные параметры > **Защита** > **Защита доступа в Интернет** > **Защита доступа в Интернет** доступны следующие опции:

Включить защиту доступа в Интернет: когда этот параметр отключен, защита доступа в интернет и защита от фишинга не осуществляются.

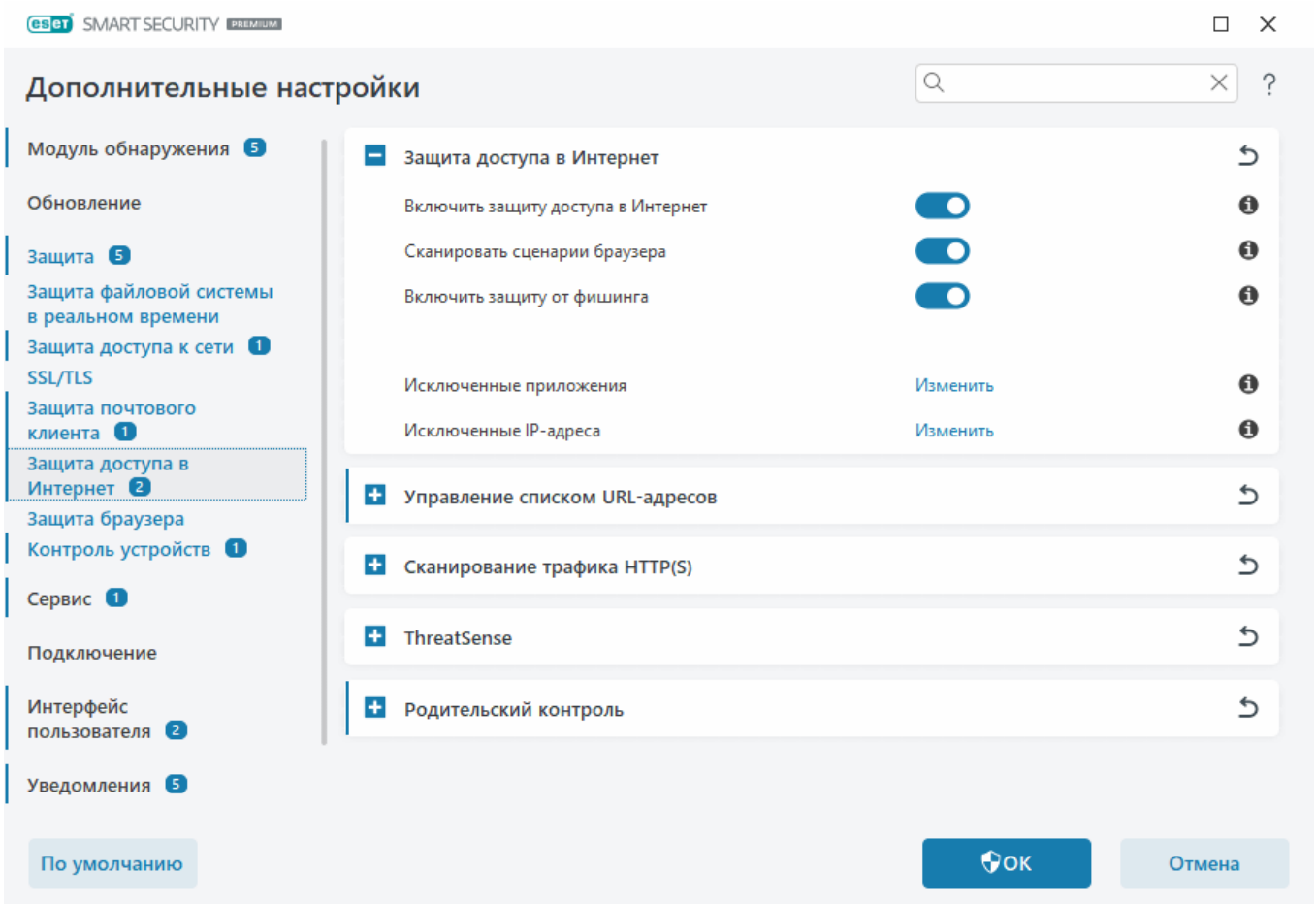
Настоятельно рекомендуем оставить включенной защиту доступа в Интернет и не исключать никакие приложения или IP-адреса по умолчанию.

Сканировать сценарии браузера: если этот параметр включен, модуль обнаружения проверяет все программы JavaScript, выполняемые веб-браузерами.

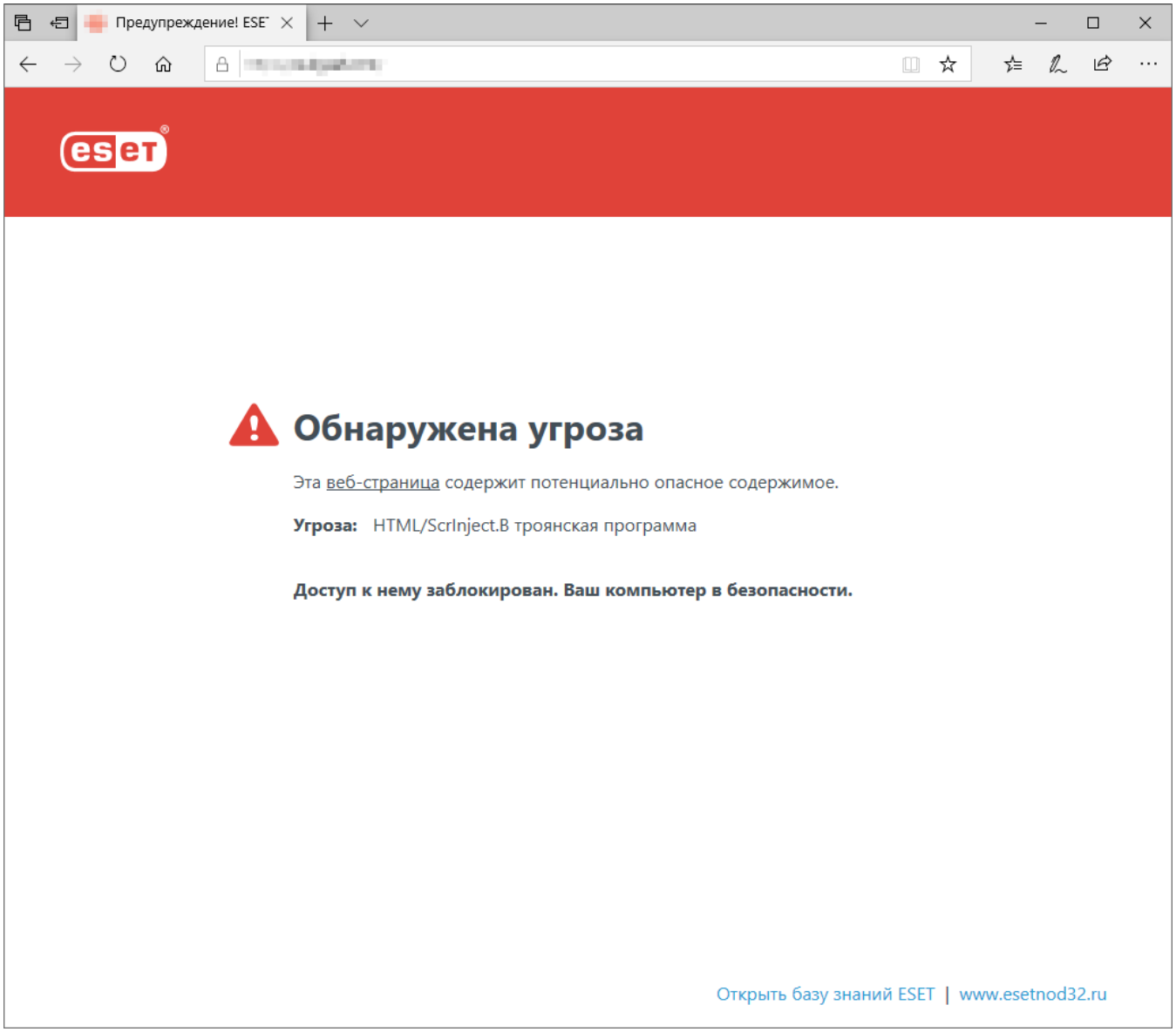
Включить защиту от фишинга: если этот параметр включен, фишинговые веб-страницы блокируются. Для получения дополнительных сведений см. раздел Защита от фишинга.

Исключенные приложения: позволяет исключить определенные приложения из сканирования функцией защиты доступа в Интернет. Это полезно, когда защита доступа в Интернет вызывает проблемы совместимости.

Исключенные IP-адреса: позволяет исключить определенные удаленные адреса из сканирования функцией защиты доступа в Интернет. Это полезно, когда защита доступа в Интернет вызывает проблемы совместимости.



Защита веб-доступа будет отображать следующее сообщение в браузере, когда веб-сайт заблокирован:



Иллюстрированные инструкции

Следующие статьи из базы знаний ESET могут быть доступны только на английском языке:

- Исключение безопасного веб-сайта из блокировки защитой доступа в интернет
- Блокировка веб-сайта с помощью ESET Security Ultimate

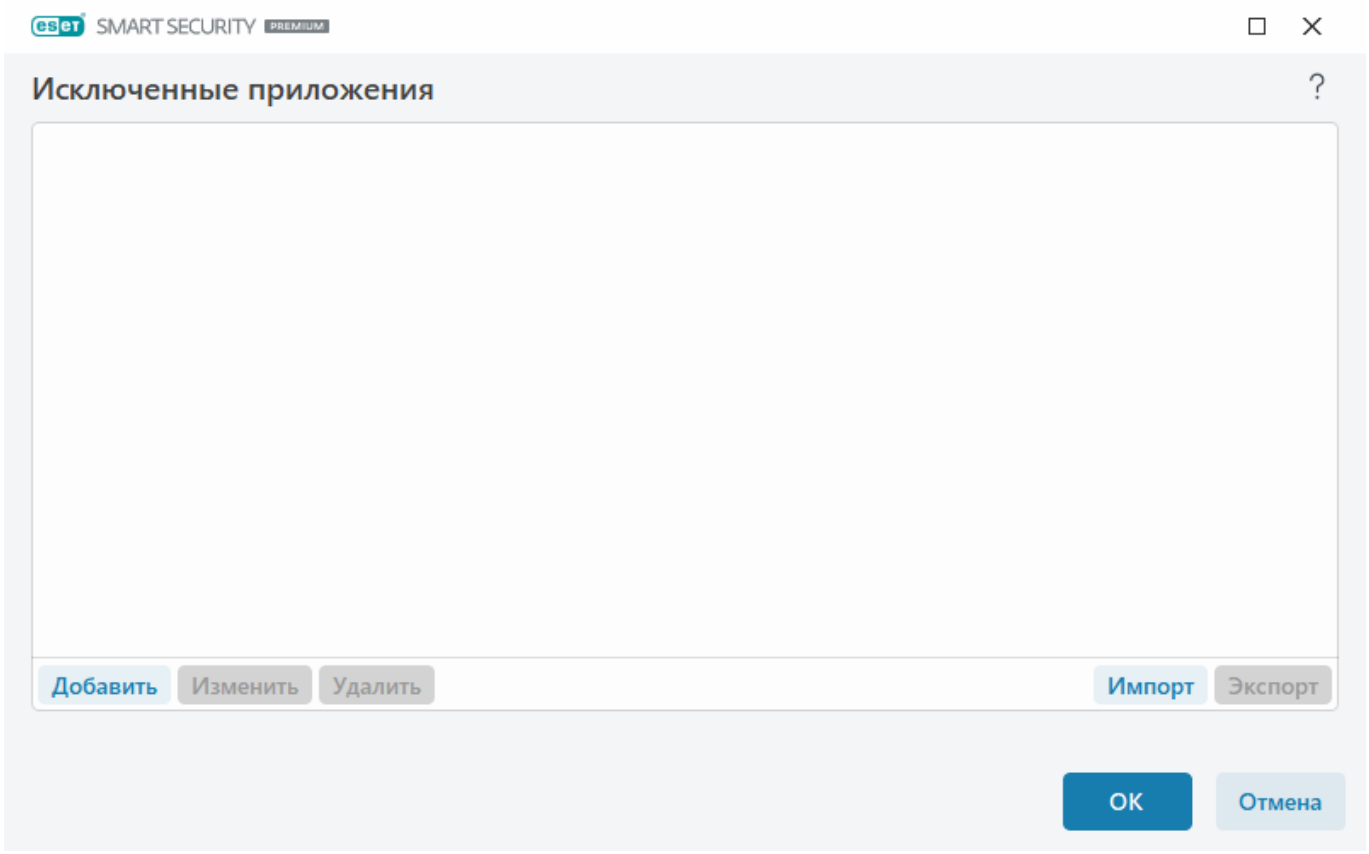
Исключенные приложения

Чтобы исключить сканирование обмена данными для определенных приложений, добавьте их в список. Соединения выделенных приложений по протоколам HTTP(S)/POP3(S)/IMAP(S) не будут проверяться на наличие угроз. Рекомендуется использовать эту возможность только для тех приложений, которые работают некорректно, если их соединения проверяются.

Запущенные приложения и службы будут доступны здесь автоматически, когда вы щелкните **Добавить**. Щелкните **...** и перейдите к приложению, чтобы добавить исключение вручную.

Изменить: изменение выбранных в списке записей.

Удалить: удаление выбранных записей из списка.



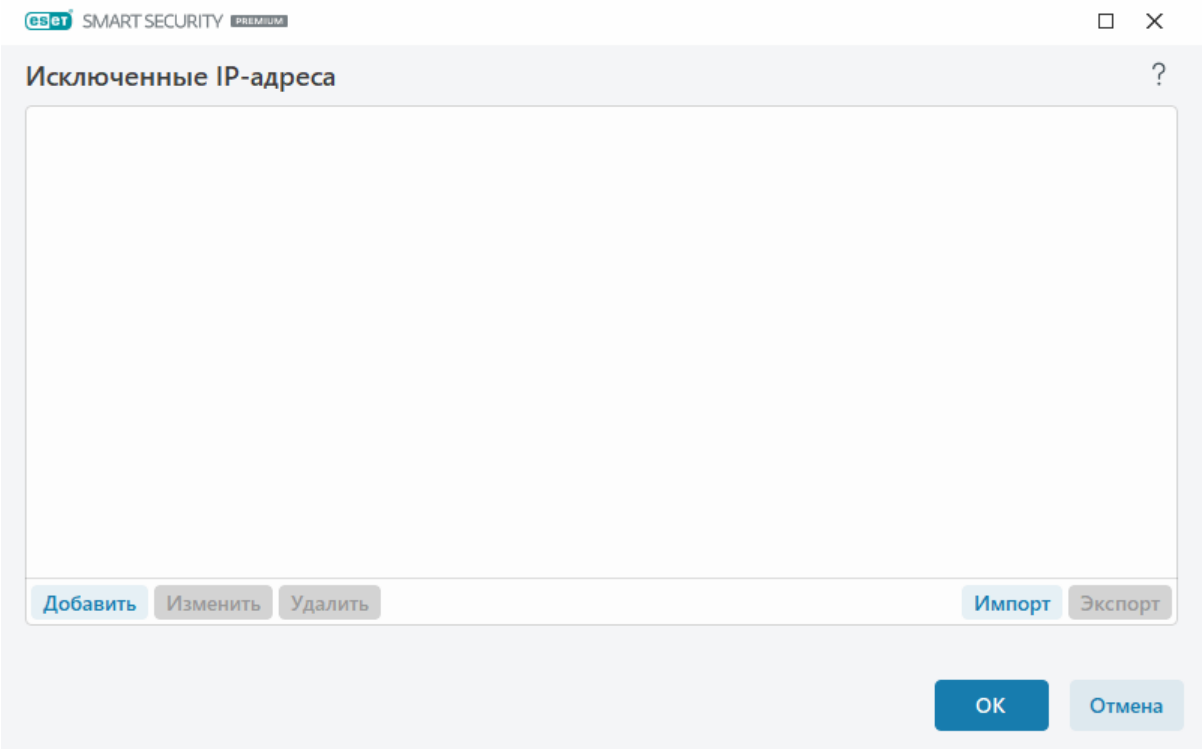
Исключенные IP-адреса

Записи в списке будут исключены из сканирования. Соединения по протоколам HTTP(S)/POP3(S)/IMAP(S), в которых участвуют выбранные адреса, не будут проверяться на наличие угроз. Этот параметр рекомендуется использовать только для заслуживающих доверия адресов.

Щелкните **Добавить**, чтобы исключить IP-адрес, диапазон адресов или подсеть удаленного узла.

Щелкните **Изменить**, чтобы изменить выбранный IP-адрес.

Нажмите кнопку **Удалить**, чтобы удалить выделенные записи из списка.



Примеры IP-адресов

Добавить адрес IPv4:
Один адрес: добавляет IP-адрес отдельного компьютера (например, *192.168.0.10*).
Диапазон адресов: введите начальный и конечный IP-адреса, чтобы задать диапазон IP-адресов нескольких компьютеров (например, *192.168.0.1–192.168.0.99*).
Подсеть: подсеть (группа компьютеров), заданная IP-адресом и маской. Например, 255.255.255.0 — это маска сети для подсети 192.168.1.0. Чтобы исключить всю подсеть, введите *192.168.1.0/24*.
Добавить адрес IPv6:
Один адрес: добавляет IP-адрес отдельного компьютера (например, *2001:718:1c01:16:214:22ff:fec9:ca5*).
Подсеть: подсеть (группа компьютеров), заданная IP-адресом и маской (например, *2002:c0a8:6301:1::1/64*).

Управление списком URL-адресов

С помощью параметра **Управление списком URL-адресов** в разделе Расширенные параметры > **Защита** > **Защита доступа в Интернет** можно указать адреса HTTP, которые следует блокировать, разрешить или исключить из сканирования содержимого.

Протоколы SSL/TLS должны быть включены, если нужно фильтровать адреса HTTPS в дополнение к HTTP. В противном случае в список будут добавлены только посещенные вами домены HTTPS-сайтов, а не полный URL-адрес.

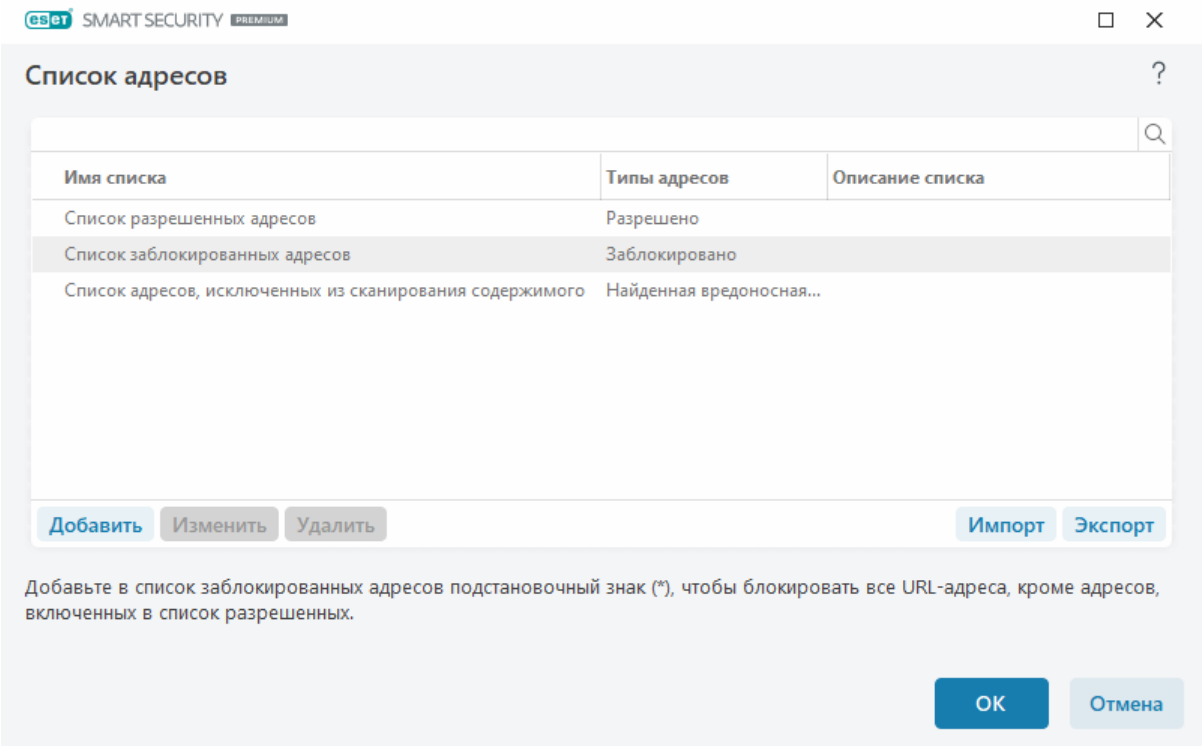
Посещение веб-сайтов, добавленных в **список заблокированных адресов** невозможно, кроме случаев, когда их адреса также добавлены в **список разрешенных адресов**. Веб-сайты из **списка адресов, для которых отключено сканирование содержимого**, загружаются без проверки на вредоносный код.

Если вы хотите заблокировать все HTTP-адреса, кроме адресов, включенных в активный **Список**

разрешенных адресов, добавьте символ «*» в активный **Список заблокированных адресов**.

В списках можно использовать такие специальные символы, как «*» (звездочка) и «?» (вопросительный знак). Символ звездочки заменяет любую последовательность символов, а вопросительный знак — любой символ. Будьте внимательны при указании адресов, исключенных из проверки, поскольку этот список должен включать в себя только доверенные и надежные адреса. Точно так же нужно убедиться в том, что символы шаблона * и ? в этом списке используются правильно. Сведения о том, как можно безопасно обозначить целый домен, включая все поддомены, см. в разделе Добавление HTTP-адреса или маски домена. Чтобы активировать список, установите флажок **Список активен**. Если вы хотите получать уведомления о том, что в адресную строку вводится адрес из текущего списка, установите флажок **Уведомлять о применении**.

> **Адреса, которым доверяет ESET**
> Если параметр **Не сканировать трафик с доменами, которым доверяет ESET** включен в разделе SSL/TLS, на домены в белом списке, которым управляет ESET, не будет распространяться конфигурация управления списком URL-адресов.



Элементы управления

Добавить: создание нового списка в дополнение к предварительно заданным. Это может быть полезно в случае, если вы хотите логически разделить разные группы адресов. Например, один список заблокированных адресов может содержать адреса, полученные из какого-либо внешнего публичного черного списка, а второй — адреса, добавленные вами. Таким образом внешний список можно будет легко обновить, не внося изменений в ваш личный список.

Изменить: редактирование существующих списков. Используйте эту установку для добавления или удаления адресов.

Удалить: удаление существующих списков. Только для списков, созданных посредством

команды **Добавить**. Удаление списков по умолчанию невозможно.

Список адресов

В этом разделе можно указать списки HTTP(S)-адресов, которые будут блокироваться, разрешаться или исключаться из проверки.

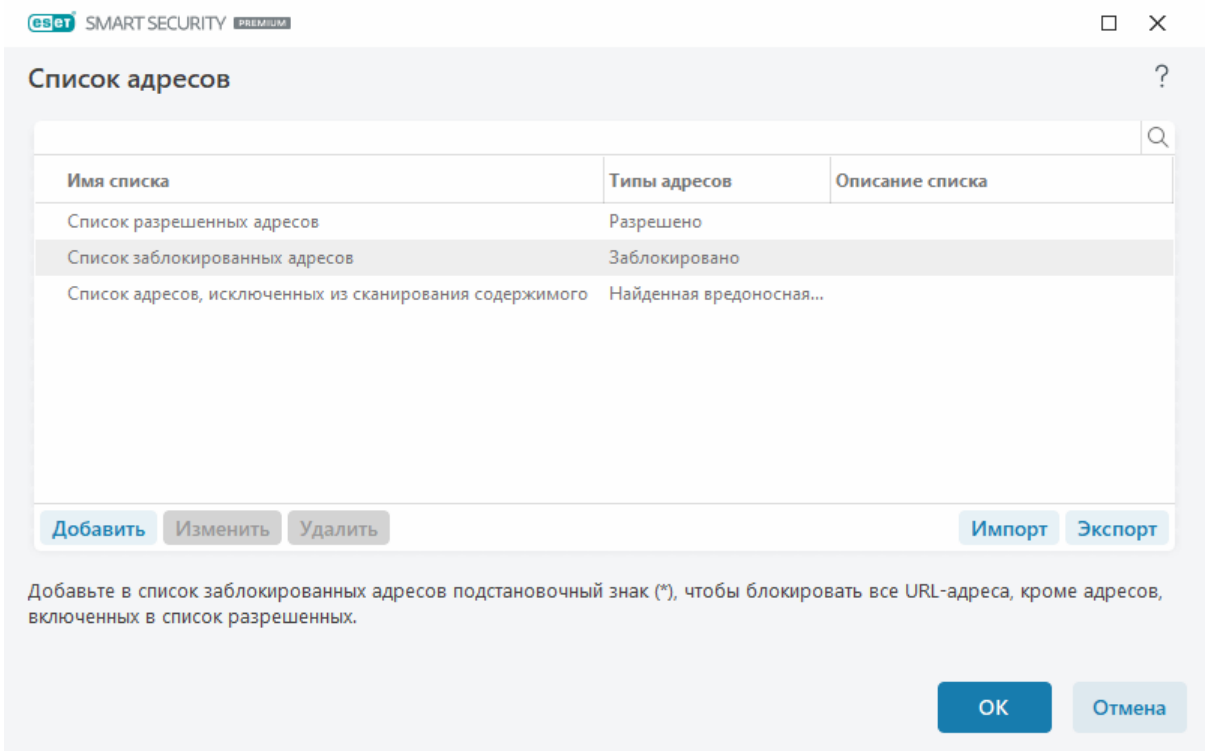
По умолчанию доступны следующие три списка.

- **Список адресов, исключенных из сканирования содержимого**. Для всех добавленных в этот список адресов проверка на наличие вредоносного кода выполняться не будет.

- **Список разрешенных адресов**. Если установлен флажок «Предоставить доступ только к разрешенным HTTP-адресам», а в списке заблокированных адресов указан символ звездочки («*» — блокировать все адреса без исключений), пользователю будет предоставлен доступ только к разрешенным адресам. Адреса в этом списке остаются доступными, даже если они включены в список заблокированных адресов.

- **Список заблокированных адресов**. Пользователь не сможет получить доступ к адресам из этого списка, если они не включены в список разрешенных адресов.

Чтобы создать новый список, нажмите кнопку **Добавить**. Для удаления выделенных списков нажмите кнопку **Удалить**.



Иллюстрированные инструкции

Следующие статьи из базы знаний ESET могут быть доступны только на английском языке:

- Исключение безопасного веб-сайта из блокировки защитой доступа в интернет
- Блокировка веб-сайта с помощью продуктов ESET для Windows для домашнего использования

Дополнительные сведения см. в разделе Управление списком URL-адресов.

Создание списка адресов

В этом диалоговом окне можно настроить новый список URL-адресов и масок, которые будут блокироваться, разрешаться или исключаться из проверки.

Можно конфигурировать следующие опции.

Тип списка адресов. Доступны три типа списков:

- **Найденная вредоносная программа пропущена**. Все добавленные в этот список адреса не будут проверятся на наличие вредоносного кода.
- **Заблокировано**. Доступ к адресам, указанным в этом списке, будет заблокирован.
- **Разрешено**. Доступ к адресам, указанным в этом списке, будет разрешен. Адреса в этом списке разрешены, даже если они включены в список заблокированных адресов.

Имя списка: здесь указывается имя списка. Это поле будет недоступно при редактировании одного из предварительно заданных списков.

Описание списка: здесь указывается краткое описание списка (необязательно). Этот параметр недоступен при редактировании одного из предварительно заданных списков.

Чтобы активировать его, рядом со списком щелкните элемент **Список активен**. Если необходимо получать уведомление, когда при доступе к веб-сайтам используется определенный список, выберите **Уведомлять о применении**. Например, вы получите уведомление, когда доступ к веб-сайту будет заблокирован или разрешен по причине присутствия его адреса в списке заблокированных или разрешенных адресов. На рабочем столе отобразится соответствующее уведомление.

Серьезность регистрируемых событий. Сведения о конкретном списке, используемом при доступе к веб-сайтам, могут быть записаны в файлы журнала.

Элементы управления

Добавить. Добавление нового URL-адреса в список (несколько адресов следует указывать через запятую).

Изменить. Изменение существующего адреса в списке. Доступно только для адресов, созданных с помощью функции **Добавить**.

Удалить: удаление существующих адресов из списка. Доступно только для адресов, созданных с помощью функции **Добавить**.

Импорт. Импорт файла с URL-адресами (в качестве разделителя следует использовать разрыв строки, например текстовый файл с кодировкой UTF-8).

Как добавить маску URL-адреса

Прежде чем вводить нужный адрес или маску домена ознакомьтесь с указаниями в этом диалоговом окне.

ESET Security Ultimate позволяет пользователям блокировать доступ к указанным веб-узлам и предотвращать отображение их содержимого в веб-браузере. Пользователь может указать адреса, которые необходимо исключить из проверки. Если полное имя удаленного сервера неизвестно или пользователь хочет указать группу удаленных серверов, то для идентификации такой группы можно использовать так называемые маски. Эти маски обозначаются символами ? и *.

- Используйте «?», чтобы заменить любой символ.
- Используйте «*», чтобы заменить текстовую строку.

Например, маска *.c?m применяется ко всем адресам, у которых последняя часть начинается с буквы «c», заканчивается буквой «m» и содержит неизвестный символ между ними (.com, .cam и т. д.).

Начальная последовательность «*.» перед именем домена интерпретируется особым образом. Прежде всего, в данном случае подстановочный знак * не соответствует символу косой черты («/»). Смысл этого исключения — избежать обхода маски, например, маска **.domain.com* не будет соответствовать *http://anydomain.com/anypath#.domain.com* (такой суффикс можно присоединить к любому URL-адресу, не влияя на загрузку). Вторая особенность в том, что «*.» в этом особом случае также соответствует пустой строке. Это позволяет обозначить одной маской целый домен, включая возможные поддомены. Например, маска **.domain.com* также соответствует *http://domain.com*. Использовать маску **domain.com* было бы неверно, поскольку она также совпала бы с *http://anotherdomain.com*.

Сканирование трафика HTTP(S)

По умолчанию ESET Security Ultimate сканирует трафик HTTP и HTTPS, который используется интернет-браузерами и другими приложениями. Отключать сканирование трафика следует только в том случае, если у вас возникли проблемы со сторонним программным обеспечением и вам нужно знать, вызвана ли проблема решением ESET Security Ultimate.

Включить сканирование трафика HTTP — HTTP-трафик отслеживается для всех портов и приложений.

Включить сканирование трафика HTTPS — для передачи трафика HTTPS между сервером и клиентом используется зашифрованный канал. ESET Security Ultimate проверяет обмен данными с помощью протоколов SSL и TLS. Программа сканирует трафик только на тех портах, которые указаны в параметре **Порты, используемые протоколом HTTPS**, вне зависимости от версии операционной системы (вы можете добавить порты к предварительно заданным 443 и 0–65535).

ThreatSense

ThreatSense — это технология, состоящая из множества сложных методов обнаружения угроз. Эта технология является упреждающей, т. е. она защищает от новой угрозы уже в начале ее распространения. При этом используется сочетание анализа и моделирования кода, обобщенных сигнатур и сигнатур вирусов, которые совместно значительно повышают уровень безопасности компьютера. Модуль сканирования может контролировать несколько потоков данных одновременно, что делает эффективность и количество обнаруживаемых угроз максимальными. Технология ThreatSense также успешно уничтожает руткиты.

Для модуля ThreatSense можно настроить несколько параметров сканирования:

- расширения и типы файлов, подлежащих сканированию;
- сочетание различных методов обнаружения;
- уровни очистки и т. д.

Чтобы открыть окно параметров, щелкните **ThreatSense** в окне расширенных параметров любого модуля, использующего технологию ThreatSense (см. ниже). Разные сценарии обеспечения безопасности могут требовать различных настроек. Поэтому технологию ThreatSense можно настроить отдельно для каждого из перечисленных далее модулей защиты.

- Защита в режиме реального времени
- Сканирование в состоянии простоя
- сканирование при запуске
- Защита документов
- Защита почтового клиента
- защита доступа в Интернет;
- Сканирование компьютера

Параметры ThreatSense хорошо оптимизированы для каждого из модулей, а их изменение значительно влияет на поведение системы. Например, изменение параметров сканирования упаковщиков в режиме реального времени или включение расширенной эвристики в модуле защиты файловой системы в режиме реального времени может замедлить работу системы (обычно только новые файлы сканируются с применением этих методов). Рекомендуется не изменять параметры ThreatSense по умолчанию ни для каких модулей, кроме модуля «Сканирование компьютера».

Сканируемые объекты

В этом разделе можно указать компоненты и файлы компьютера, которые будут сканироваться на наличие заражений.

Оперативная память: сканирование на наличие угроз, которые атакуют оперативную память системы.

Загрузочные секторы/UEFI. Загрузочные секторы сканируются на наличие вредоносных программ в основной загрузочной записи. Дополнительные сведения о UEFI см. в глоссарии.

Почтовые файлы. DBX (Outlook Express) и EML

Архивы. Программа поддерживает такие расширения, как ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE, и многие другие.

Самораспаковывающиеся архивы. Тип архивов (SFX), содержимое которых может извлекаться автоматически.

Программы сжатия исполняемых файлов: в отличие от стандартных типов архивов, программы сжатия исполняемых файлов после запуска распаковываются в памяти. Благодаря эмуляции кода модуль сканирования распознает не только стандартные статические упаковщики (UPX, yoda, ASPack, FSG и т. д.), но и множество других типов упаковщиков.

Параметры сканирования

Выберите способы сканирования системы на предмет заражений. Доступны следующие варианты:

Эвристический анализ: анализ вредоносной активности программ с помощью специального алгоритма. Главным достоинством этого метода является способность идентифицировать вредоносные программы, сведения о которых отсутствуют в существующей версии модуля обновления. Недостатком же является вероятность (очень небольшая) ложных тревог.

Расширенный эвристический анализ/сигнатуры распределенных сетевых атак: для расширенного эвристического анализа используется уникальный эвристический алгоритм компании ESET, который оптимизирован для обнаружения компьютерных червей и троянских программ и написан на высокоуровневых языках программирования. Использование расширенной эвристики значительным образом увеличивает возможности продуктов ESET по обнаружению угроз. С помощью сигнатур осуществляется точное обнаружение и идентификация вирусов. Система автоматического обновления обеспечивает наличие новых сигнатур через несколько часов после обнаружения угрозы. Недостатком же сигнатур является то, что они позволяют обнаруживать только известные вирусы (или их незначительно модифицированные версии).

Очистка

Параметры очистки определяют поведение ESET Security Ultimate при очистке объектов. Предусмотрено четыре уровня очистки.

ThreatSense имеет такие уровни исправления проблем (т. е. очистки):

Исправление в ESET Security Ultimate

Уровень очистки	Описание
Всегда исправлять обнаружения	Пытаться исправлять обнаружения при очистке объектов без вмешательства конечного пользователя. В некоторых случаях (например, с системными файлами), если обнаружение не удается исправить, обнаруженный объект оставляется в исходном расположении.
Исправлять обнаружения, если это безопасно, в другом случае оставить	Пытаться исправлять обнаружения при очистке объектов без вмешательства конечного пользователя. В некоторых случаях (например, системные файлы или архивы, которые содержат и чистые, и зараженные файлы), если обнаружение не удается исправить, обнаруженный объект остается в исходном расположении.
Исправлять обнаружения, если это безопасно, в другом случае спрашивать	Пытаться исправлять обнаружения при очистке объектов. В некоторых случаях, если ни одно из действий выполнить невозможно, конечный пользователь получает интерактивное предупреждение, в котором следует выбрать действие по исправлению (например, удалить или проигнорировать). Этот параметр рекомендуется в большинстве случаев.
Всегда спрашивать у конечного пользователя	Конечному пользователю отображается интерактивное окно при очистке объектов, и он должен выбрать действие по исправлению (например, удалить или пропустить). Этот уровень предназначен для более опытных пользователей, которые знают, какие действия следует предпринять в случае обнаружения.

Исключения

Расширением называется часть имени файла, отделенная от основной части точкой. Оно определяет тип файла и его содержимое. Этот раздел ThreatSense позволяет определить типы файлов, подлежащих сканированию.

Другое

При настройке параметров модуля ThreatSense для сканирования компьютера по требованию также доступны описанные ниже параметры из раздела **Другое**.

Сканировать альтернативные потоки данных (ADS): альтернативные потоки данных, используемые файловой системой NTFS, — это связи файлов и папок, которые не обнаруживаются при использовании обычных методов сканирования. Многие заражения маскируются под альтернативные потоки данных, пытаясь избежать обнаружения.

Запускать фоновое сканирование с низким приоритетом: каждый процесс сканирования потребляет некоторое количество системных ресурсов. Если пользователь работает с ресурсоемкими программами, можно активировать фоновое сканирование с низким приоритетом и высвободить тем самым ресурсы для других приложений.

Журнал всех объектов. Журнал проверки отображает все отсканированные файлы в самораспаковывающихся архивах, даже незараженные (может создавать большое количество данных журнала сканирования и увеличивать размер его файла).

Включить оптимизацию Smart: при включенной оптимизации Smart используются оптимальные параметры для обеспечения самого эффективного уровня сканирования с

сохранением максимально высокой скорости. Разные модули защиты выполняют интеллектуальное сканирование, применяя отдельные методы для различных типов файлов. Если оптимизация Smart отключена, при сканировании используются только пользовательские настройки ядра ThreatSense каждого модуля.

Сохранить отметку о времени последнего доступа: установите этот флажок, чтобы сохранить исходное значение времени доступа к сканируемым файлам, а не обновлять их (например, для использования с системами резервного копирования данных).

Ограничения

В разделе «Ограничения» можно указать максимальный размер объектов и уровни вложенности архивов для сканирования.

Параметры объектов

Максимальный размер объекта: определяет максимальный размер объектов, подлежащих сканированию. Данный модуль защиты от вирусов будет сканировать только объекты меньше указанного размера. Этот параметр рекомендуется менять только опытным пользователям, у которых есть веские основания для исключения из сканирования больших объектов. Значение по умолчанию: Не ограничено.

Максимальная продолжительность сканирования объекта (с): определяет максимальное значение времени для сканирования файлов в объекте-контейнере (например, в архиве RAR/ZIP или в электронном письме с несколькими вложениями). Эта настройка не применяется к отдельным файлам. Если пользователь укажет собственное значение и указанное время истечет, сканирование будет остановлено как можно скорее вне зависимости от того, завершено ли сканирование каждого файла в объекте-контейнере.
Если речь идет об архиве с большими файлами, сканирование будет прекращено не раньше, чем произойдет извлечение файла из архива (например, когда пользователь задал значение в 3 секунды, но извлечение файла занимает 5 секунд). По истечении этого времени остальные файлы в архиве сканироваться не будут.
Чтобы ограничить время сканирования, в том числе для архивов большого размера, используйте параметры **Максимальный размер объекта** и **Максимальный размер файла в архиве** (не рекомендуется в связи с возможными проблемами безопасности).
Значение по умолчанию: Не ограничено.

Настройки сканирования архивов

Уровень вложенности архивов: определяет максимальную глубину проверки архивов. Значение по умолчанию: 10.

Максимальный размер файла в архиве: этот параметр позволяет задать максимальный размер файлов в архиве (при их извлечении), которые должны сканироваться. Максимальное значение — **3 ГБ**.

> Не рекомендуется изменять значения по умолчанию, так как обычно для этого нет особой причины.

Родительский контроль

Параметр **Включить родительский контроль** позволяет интегрировать функцию родительского контроля в ESET Security Ultimate. Щелкните **Изменить** рядом с элементом Учетные записи пользователей, чтобы связать учетные записи пользователей Windows, используемые функцией родительского контроля, с определенными пользователями для ограничения их доступа к неприемлемому или опасному содержимому в Интернете.

Учетные записи пользователей

В разделе Расширенные параметры > **Защита** > **Защита доступа в Интернет** > **Родительский контроль** > **Учетные записи пользователей** > **Изменить** можно связать учетные записи пользователей Windows, используемые функцией родительского контроля, с определенными пользователями для ограничения их доступа к неприемлемому или опасному содержимому в Интернете.

Столбцы

Учетная запись Windows: имя пользователя.

Включено: когда этот параметр включен, родительский контроль для конкретной учетной записи пользователя активен.

Домен: имя домена, к которому принадлежит пользователь.

День рождения: определяет возраст пользователя, которому принадлежит учетная запись.

Элементы управления

Добавить: отображение диалогового окна Работа с учетной записью пользователя.

Изменить: эта опция дает возможность изменить выбранные учетные записи.

Удалить: удаление выбранной учетной записи.

Обновить: если вы добавили учетную запись пользователя, ESET Security Ultimate может обновить список учетных записей пользователей без необходимости повторного открытия данного окна.

Настройки учетной записи пользователя

В этом окне три вкладки.

Общие

Включите переключатель рядом с элементом **Включено**, чтобы включить родительский контроль для выбранной ниже учетной записи Windows.

Первым делом нужно **Выбрать** учетную запись системы на своем компьютере. Ограничения,

установленные в разделе «Родительский контроль», распространяются только на стандартные учетные записи Windows. Административные учетные записи позволяют обходить ограничения.

Если учетная запись используется одним из родителей, выберите вариант **Родительская учетная запись**.

Укажите **дату рождения ребенка** для учетной записи, чтобы определить ее уровень доступа и задать правила доступа к подходящим по возрасту веб-страницам.

Серьезность регистрируемых событий

Персональный файервол ESET Security Ultimate сохраняет данные обо всех важных событиях в файле журнала, который можно открыть из главного меню. Щелкните **Сервис** > **Файлы журналов** и выберите в раскрывающемся списке **Журнал** элемент **Родительский контроль**.

• **Диагностика**: регистрируется информация, необходимая для тщательной настройки программы.

• **Информация**: записываются информационные сообщения, в том числе разрешенные и заблокированные исключения, а также все перечисленные выше записи.

• **Предупреждение**: записывается информация обо всех критических ошибках и предупреждениях.

• **Ничего** — журналы не создаются.

Исключения

Создание исключения позволяет разрешить или запретить пользователю доступ к веб-сайтам, отсутствующим в списке исключений. Это полезно, если требуется контролировать доступ к определенным веб-сайтам вместо использования категорий. Исключения, созданные для одной учетной записи, можно скопировать и использовать для другой учетной записи. Это может быть полезно, когда требуется создать идентичные правила для детей близкого возраста.

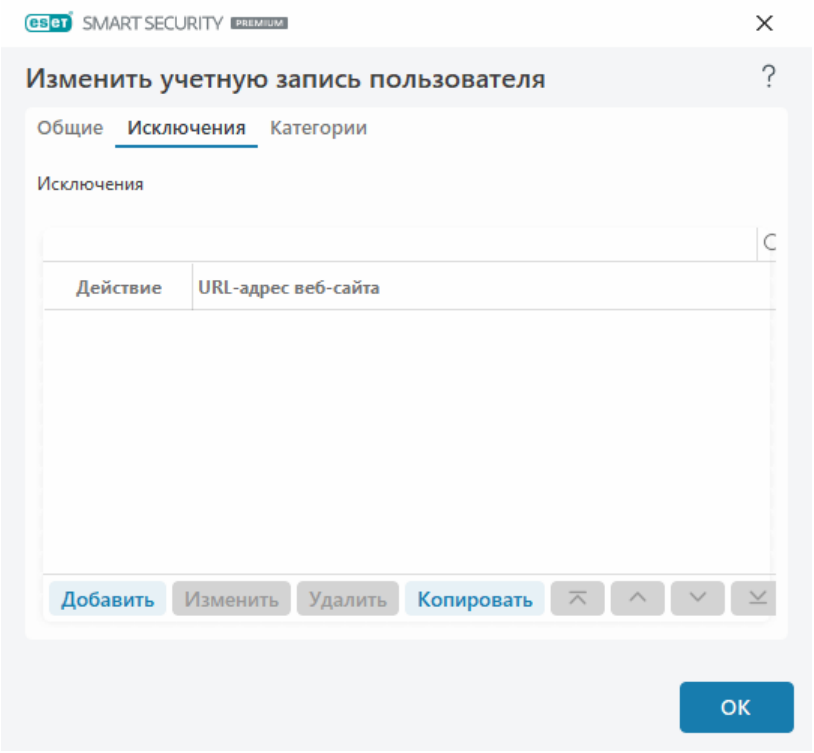
Нажмите кнопку **Добавить**, чтобы создать новое исключение. Задайте **Действие** (например, **Блокировать**), выбрав его в раскрывающемся списке, введите **URL-адрес сайта**, к которому применяется данное исключение, и нажмите кнопку **OK**. Новое исключение будет добавлено в список имеющихся, где будет отображаться также его состояние.

Добавить: создание исключения.

Изменить: команда, позволяющая изменить **URL-адрес веб-сайта** или **Действие** для выбранного исключения.

Удалить: команда, удаляющая выбранное исключение.

Копировать: выберите пользователя в раскрывающемся меню, откуда требуется скопировать созданное исключение.

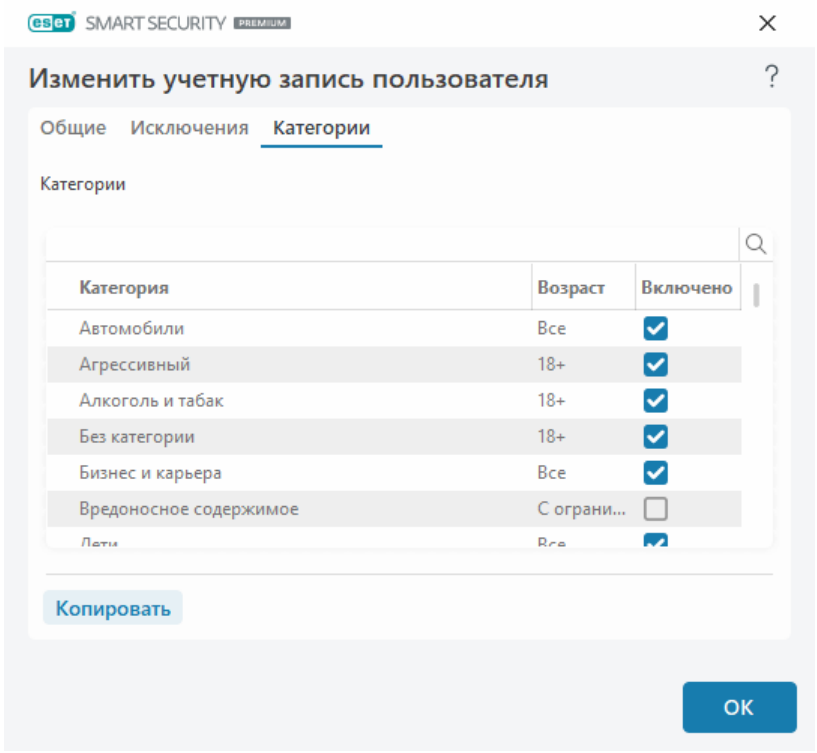


Заданные исключения переопределяют категории, определенные для выбранных учетных записей. Например, если для учетной записи заблокирована категория **Новости**, но при этом в качестве исключения задана разрешенная новостная веб-страница, то данная веб-страница будет доступна для этой учетной записи. Любые сделанные здесь изменения можно просмотреть в разделе Исключения.

Категории

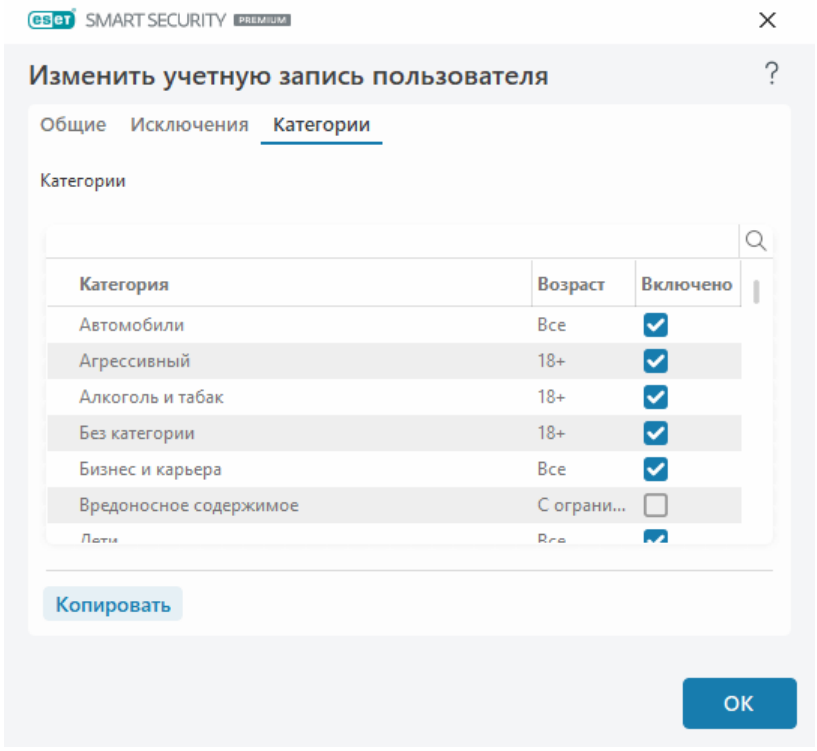
На вкладке **Категории** можно задать общие категории веб-сайтов, которые следует блокировать или разрешать для каждой учетной записи. Чтобы разрешить категорию, установите рядом с ней флажок. Если флажок не установлен, соответствующая категория для данной учетной записи разрешена не будет.

Копировать: позволяет скопировать список заблокированных или разрешенных категорий из существующей измененной учетной записи.



Категории

Установите флажок в столбце **Включено** рядом с категорией, чтобы разрешить ее. Если оставить этот флажок снятым, соответствующая категория для данной учетной записи разрешена не будет.



Ниже приведены некоторые примеры категорий (групп), о которых пользователям может быть неизвестно.

- **Разное**: обычно частные (локальные) IP-адреса, например адреса в интрасети

(127.0.0.0/8, 192.168.0.0/16 и т. д). Веб-сайт, на котором отображается код ошибки 403 или 404, также попадает в эту категорию.

• **Не разрешенная**: данная категория включает веб-страницы, которые не разрешены из-за возникновения ошибки при подключении к модулю базы данных родительского контроля.

• **Без категории**: неизвестные веб-страницы, которых еще нет в базе данных родительского контроля.

• **Динамическая**: веб-страницы, которые переадресовывают на другие страницы других веб-сайтов.

Защита браузера

Защита браузера — это дополнительный уровень защиты для ваших безопасности и конфиденциальности, который ограждает память браузера от проверки другими процессами, улучшает защиту от клавиатурных шпионов и предотвращает вставку из буфера обмена в защищенный браузер любых связанных с онлайн-платежами данных, измененных вредоносными программами. Чтобы настроить защиту браузера, откройте раздел Расширенные параметры > **Защита** > **Защита браузера** и сделайте выбор среди следующих опций конфигурации:

- Защита банковских операций и браузера
- Список разрешенных объектов для защиты браузера
- Рамка браузера

Защита банковских операций и браузера

Функцию Защита банковских операций и браузера можно настроить в разделе Расширенные параметры > **Защита** > **Защита браузера** > **Защита банковских операций и браузера**.

Защита банковских операций и браузера

Включить защиту банковских операций и браузера: когда эта функция включена, все поддерживаемые веб-браузеры по умолчанию будут запускаться в безопасном режиме.

Защита браузера

Включите параметр **Защита всех браузеров**, чтобы все поддерживаемые веб-браузеры запускались в безопасном режиме.

Режим установки расширения: в раскрывающемся меню можно выбрать, какие расширения разрешено устанавливать в браузере, который защищен с помощью ESET:

• **Существенные расширения**: только самые существенные расширения, разработанные конкретным производителем браузера.

- **Все расширения**: все расширения, поддерживаемые конкретным браузером.

> Изменение режима установки расширений не влияет на ранее установленные расширения браузера.

Защищенный браузер

Расширенная защита памяти: если этот параметр включен, память защищенного браузера будет защищена от исследования другими процессами.

Защита клавиатуры — если этот параметр включен, информация, которую вы вводите с клавиатуры в защищенном браузере, будет скрыта от других приложений. Это повышает защиту от клавиатурных шпионов.

Защита буфера обмена: если эта функция включена, ESET Security Ultimate будет предотвращать вставку любых данных, которые связаны с онлайн-платежами и были изменены вредоносными программами, из буфера обмена в защищенный браузер. Это обеспечивает защиту от возможных изменений, вносимых вредоносным программным обеспечением.

Рамка браузера — Персонализируйте настройки отображения рамки в защищенных браузерах.

Список разрешенных объектов для защиты браузера — Здесь можно управлять файлами, добавленными в список разрешенных объектов для защиты браузера.

Конфиденциальность и безопасность браузера

Включить функцию «Конфиденциальность и безопасность браузера»: если этот параметр отключен, расширение «Конфиденциальность и безопасность браузера» будет удалено из всех поддерживаемых браузеров во всех учетных записях Windows.

Отображать уведомления функции «Конфиденциальность и безопасность браузера»: если этот параметр включен, ESET Security Ultimate будет отображать уведомления функции «Конфиденциальность и безопасность браузера».

Сканер сценариев браузера

Включить расширенное сканирование сценариев браузера: если этот параметр включен, сканер защиты от вирусов будет проверять все программы JavaScript, выполняемые интернет-браузерами.

00

Контроль устройств

ESET Security Ultimate обеспечивает автоматический контроль устройств (компакт-дисков, DVD-дисков, устройств USB и т. д.). Данный модуль позволяет блокировать или изменять расширенные фильтры и разрешения, а также указывать, может ли пользователь получать доступ к конкретному устройству и работать с ним. Это может быть удобно, если

администратор компьютера хочет предотвратить использование устройств с нежелательным содержимым.

Поддерживаемые внешние устройства:

- Дисковый накопитель (жесткий диск, съемный USB-диск)
- Компакт-/DVD-диск
- Принтер USB
- FireWire Хранилище
- Bluetooth Устройство
- Устройство чтения смарт-карт
- Устройство обработки изображений
- Модемы
- LPT/COM порт
- Портативное устройство (устройства от аккумулятора, такие как мультимедийный проигрыватель, смартфоны, самонастраивающиеся устройства и т. д.)
- Все типы устройств

Параметры контроля устройств можно изменить в разделе Дополнительные настройки > **Защиты** > **Контроль устройств**.

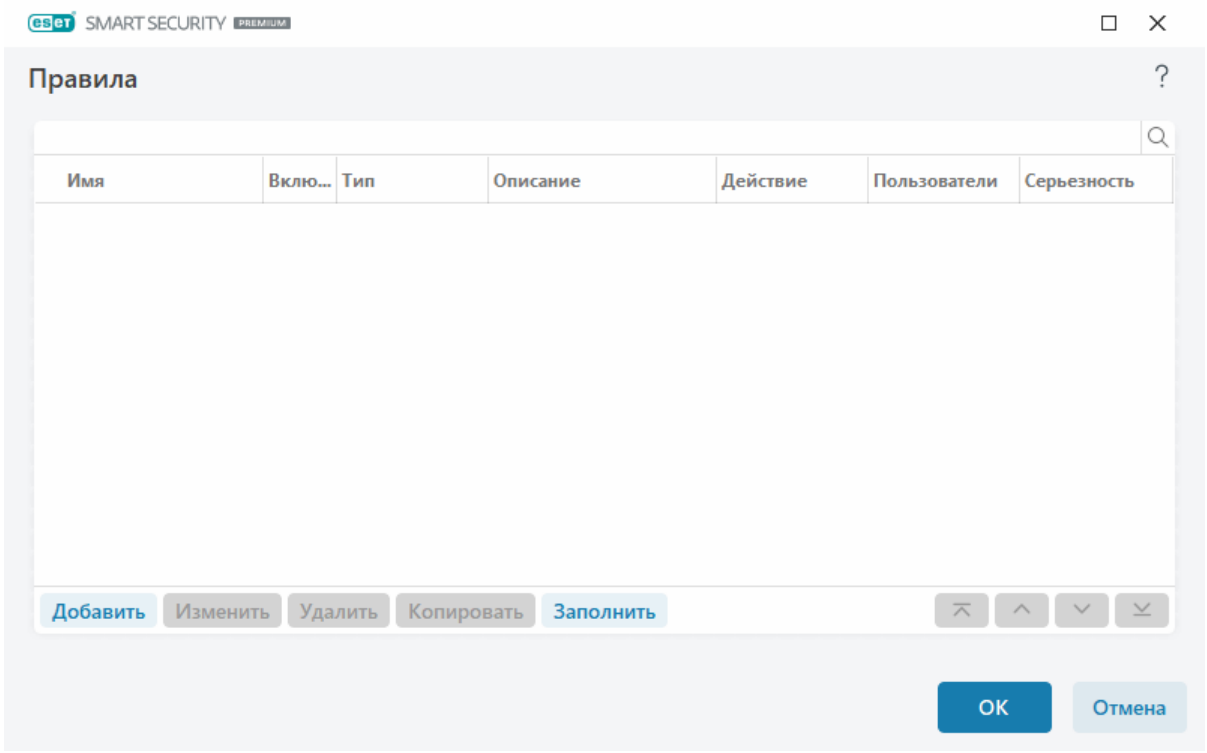
Щелкните переключатель **Включить контроль устройств**, чтобы включить функцию контроля устройств в ESET Security Ultimate. Чтобы это изменение вступило в силу, необходимо перезапустить компьютер. После включения контроля устройств можно настроить **правила** в окне Редактор правил.

> Вы можете создать разные группы устройств, к которым будут применяться разные правила. Можно создать только одну группу устройств, к которой применяется правило с действием **Разрешить** или **Блокировка записи**. Благодаря этому, когда к компьютеру подключаются нераспознанные устройства, функция контроля устройств их блокирует.

При подключении устройства, заблокированного существующим правилом, отобразится окно оповещения, и доступ к устройству будет заблокирован.

Редактор правил для контроля устройств

В окне **Редактор правил для контроля устройств** отображаются существующие правила. С его помощью можно контролировать внешние устройства, которые пользователи подключают к компьютеру.



Вы можете разрешить или заблокировать определенные устройства для конкретных пользователей или их групп, а также в соответствии с дополнительными параметрами, которые задаются в конфигурации правил. В списке правил для каждого правила отображается описание, включающее название и тип внешнего устройства, действие, выполняемое после его подключения к компьютеру, а также серьезность для журнала. См. также статью Добавление правил контроля устройств.

Для управления правилом используйте кнопки **Добавить** или **Изменить**. Чтобы создать правило с использованием заранее заданных параметров из другого правила, нажмите кнопку **Копировать**. XML-строки, которые отображаются, если щелкнуть правило, можно скопировать в буфер обмена. Кроме того, они могут помочь системным администраторам экспортировать или импортировать эти данные, а также использовать их.

Чтобы выделить несколько правил, щелкните их, удерживая нажатой клавишу **CTRL**. Затем их можно будет одновременно удалить либо переместить к началу или концу списка. С помощью флажка **Включено** можно отключать и включать правило. Эта функция может понадобиться, если вы хотите оставить правило.

Щелкните **Заполнить**, чтобы выполнить автоматическое заполнение параметров для съемных носителей, подключенных к компьютеру.

Правила приведены в порядке их приоритета: имеющие более высокий приоритет правила располагаются ближе к началу списка. Для перемещения отдельных правил или групп правил используйте кнопки **В начало/Вверх/Вниз/В конец**.

Записи журнала можно просмотреть в главном окне программы в разделе **Инструменты** > Файлы журнала.

В журнал контроля устройств записываются все случаи, когда срабатывает функция контроля устройств.

Обнаруженные устройства

С помощью кнопки **Заполнить** можно ознакомиться со следующей информацией о подключенных на данный момент устройствах: тип устройства, производитель, модель и серийный номер (если есть). Если вы хотите просмотреть все скрытые устройства, выберите **Показывать скрытые устройства**.

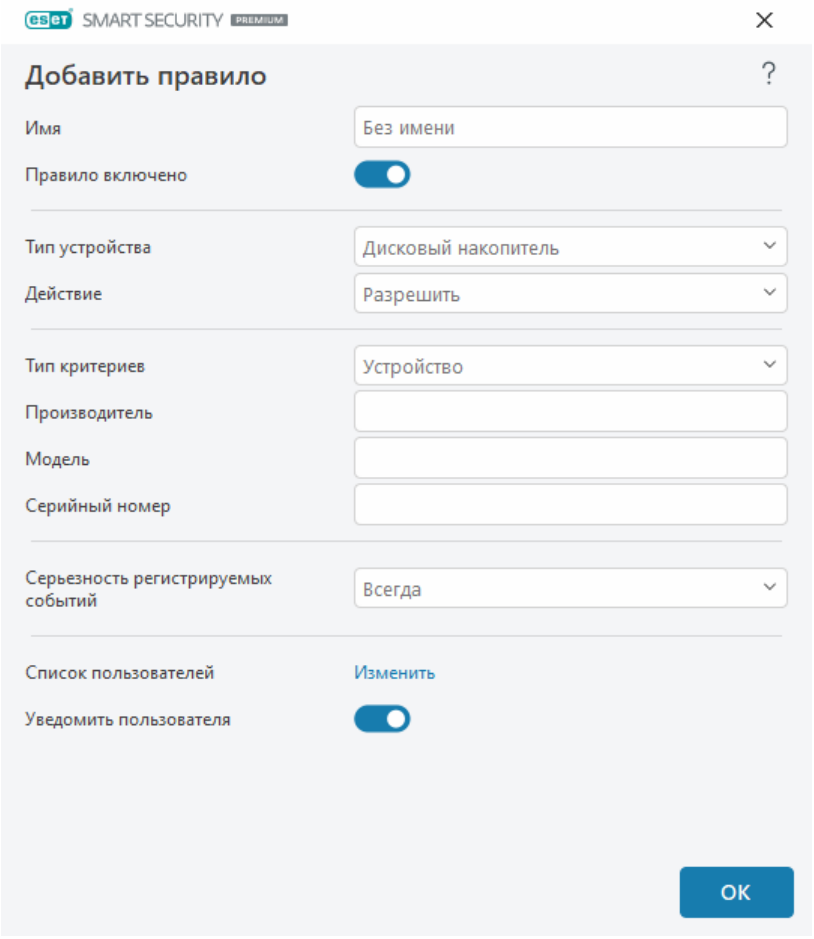
Выберите устройство в списке обнаруженных устройств и нажмите кнопку **OK**, чтобы добавить правило контроля устройств с предварительно заданной информацией (все параметры можно настраивать).

Устройства в режиме низкого энергопотребления (спящем режиме) отмечены значком предупреждения . Чтобы активировать кнопку **OK** и добавить правило для этого устройства, сделайте следующее:

- Повторное подключение устройства
- Использование устройства (например, запуск приложения «Камера» в Windows для активации веб-камеры)

Добавление правил контроля устройств

Правилом контроля устройств определяется действие, выполняемое при подключении к компьютеру устройств, которые соответствуют заданным критериям.



Чтобы упростить идентификацию правила, введите его описание в поле **Имя**. Чтобы включить или отключить это правило, щелкните ползунок рядом с элементом **Правило включено**. Это может быть полезно, если полностью удалять правило не нужно.

Тип устройства

В раскрывающемся меню выберите тип внешнего устройства (дисковый накопитель, портативное устройство, Bluetooth, FireWire и т. д.). Сведения о типе устройства поступают от операционной системы. Их можно просмотреть с помощью диспетчера устройств, если устройство подключено к компьютеру. К накопителям относятся внешние диски и традиционные устройства чтения карт памяти, подключенные по протоколу USB или FireWire. Устройства чтения смарт-карт позволяют читать карты со встроенными микросхемами, такие как SIM-карты или идентификационные карточки. Примерами устройств для обработки изображений служат сканеры и камеры. Так как эти устройства предоставляют сведения только о своих действиях, а не о пользователях, заблокировать их можно только глобально.

Действие

Доступ к устройствам, не предназначенным для хранения данных, можно только разрешить или заблокировать. Напротив, правила для устройств хранения данных позволяют выбрать одно из указанных ниже прав.

- **Разрешить** — будет разрешен полный доступ к устройству.
- **Блокировать** — доступ к устройству будет заблокирован.
- **Блокировка записи** — будет разрешено только чтение данных с устройства.
- **Предупредить** — при каждом подключении устройства пользователь получает уведомление, разрешено ли это устройство или заблокировано, и при этом создается запись журнала. Устройства не запоминаются. Уведомления отображаются при каждом повторном подключении одного и того же устройства.

Обратите внимание, что полный список действий (разрешений) доступен не для всех типов устройств. Если устройство относится к типу хранилищ, будут доступны все четыре действия. Если устройство не предназначено для хранения данных, доступны будут только три действия. Например, право **Блокировка записи** неприменимо к Bluetooth-устройствам, поэтому доступ к ним можно только разрешить, заблокировать или разрешить с предупреждением.

Тип критериев

Выберите элемент **Группа устройств** или **Устройство**.

С помощью указанных ниже дополнительных параметров можно точно настраивать правила для разных устройств. Во всех параметрах учитывается регистр и поддерживаются подстановочные знаки (*, ?):

- **Производитель** — фильтрация по имени или идентификатору производителя.

- **Модель** — имя устройства.

- **Серийный номер** — у внешних устройств обычно есть серийные номера. Когда речь идет о CD- или DVD-диске, то это серийный номер конкретного носителя, а не дисковода CD-дисков.

Если для этих параметров не заданы значения, во время сопоставления правило игнорирует эти поля. Параметры фильтрации во всех текстовых полях учитывают регистр и поддерживают подстановочные знаки (вопросительный знак (?) обозначает один символ, а звездочка (*) — строку длиной ноль символов и более).

Для просмотра сведений об этом устройстве создайте правило для соответствующего типа устройств, подключите устройство к компьютеру и ознакомьтесь со сведениями об устройстве в журнале контроля устройств.

Серьезность регистрируемых событий

Персональный файервол ESET Security Ultimate сохраняет данные обо всех важных событиях в файле журнала, который можно открыть из главного меню. Щелкните **Служебные программы** > **Файлы журналов** и выберите в раскрывающемся списке **Журнал** элемент **Контроль устройств**.

- **Всегда** — записываются все события.
- **Диагностика**: регистрируется информация, необходимая для тщательной настройки программы.
- **Информация** — в журнал вносятся информационные сообщения, в том числе сообщения об успешном выполнении обновления, а также все перечисленные выше записи.
- **Предупреждение**: записывается информация обо всех критических ошибках и предупреждениях.
- **Ничего** — журналы не создаются.

Список пользователей

Правила можно назначать только для некоторых пользователей или их групп, добавленных в список пользователей, щелкнув пункт **Изменить** рядом с элементом **Список пользователей**.

- **Добавить** — открывается диалоговое окно **Типы объектов: Пользователи и группы**, в котором можно выбрать нужных пользователей.
- **Удалить**: выбранный пользователь удаляется из фильтра.

Ограничения для списка пользователей

Список пользователей нельзя определить для правил с указанными типами устройств:

- USB-принтер
- Устройство Bluetooth
- Устройство чтения смарт-карт
- Устройство обработки изображений
- Модемы
- LPT/COM-порты

Уведомить пользователя — при подключении устройства, заблокированного существующим правилом, отобразится окно оповещения.

Группы устройств

⚠ Устройство, подключенное к компьютеру, может представлять угрозу безопасности.

Окно групп устройств разделено на две части. В правой части окна отображается список устройств, входящих в выбранную группу, а в левой части — созданные группы. Выберите группу для отображения устройств на правой панели.

Открыв окно групп устройств и выбрав группу, вы можете добавлять устройства в список или удалять их из него. Добавлять устройства в группу также можно посредством импорта данных об устройствах из файла. Или же можно нажать кнопку **Заполнить**. В этом случае все устройства, подключенные к компьютеру, отобразятся в окне **Обнаруженные устройства**. Выберите устройства из этого списка и нажмите кнопку **OK**, чтобы добавить их в группу.

Элементы управления

Добавить. Позволяет добавить группу, введя ее имя, или устройство в существующую группу (в зависимости от того, в какой части окна нажата кнопка).

Изменить. Позволяет изменить имя выбранной группы или параметров устройства (производитель, модель, серийный номер).

Удалить: удаление выбранной группы или устройства (в зависимости от того, в какой части окна нажата кнопка).

Импорт. Импортирует список устройств из текстового файла. Для импорта устройств из текстового файла требуется правильное форматирование:

- каждое устройство должно быть указано с новой строки;
- для каждого устройства должны быть указаны через запятую сведения о **производителе**, **модели** и **серийном номере**.

✓ Вот пример содержимого такого текстового файла:

```
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101
```

Экспорт. Экспортирует список устройств в файл.

С помощью кнопки **Заполнить** можно ознакомиться со следующей информацией о подключенных на данный момент устройствах: тип устройства, производитель, модель и серийный номер (если есть).

Добавить устройство

Щелкните **Добавить** в правом окне, чтобы добавить устройство в существующую группу. С помощью указанных ниже дополнительных параметров можно точно настраивать правила для разных устройств. Во всех параметрах учитывается регистр и поддерживаются подстановочные знаки (*, ?):

- **Производитель**: фильтрация по имени или ID производителя.

• **Модель** — имя устройства.

• **Серийный номер** — у внешних устройств обычно есть серийные номера. Когда речь идет о CD- или DVD-диске, то это серийный номер конкретного носителя, а не дисковода CD-дисков.

• **Описание** — ваше описание устройства.

> Если для этих параметров не заданы значения, во время сопоставления правило игнорирует эти поля. Параметры фильтрации во всех текстовых полях учитывают регистр и поддерживают подстановочные знаки (вопросительный знак [?] обозначает один символ, а звездочка [*] — строку длиной ноль символов и более).

Для сохранения изменений нажмите кнопку **OK**. Чтобы закрыть окно **Группы устройств** без сохранения изменений, щелкните **Отмена**.

> После создания группы устройств необходимо для созданной группы устройств добавить новое правило контроля устройств и выбрать выполняемое действие.

Обратите внимание, что полный список действий (разрешений) доступен не для всех типов устройств. Если устройство относится к типу хранилищ, будут доступны все четыре действия. Если устройство не предназначено для хранения данных, доступны только три действия. Например, действие **Блокировка записи** недоступно для Bluetooth-устройств, поэтому доступ к ним можно только разрешить, заблокировать или разрешить с предупреждением.

Защита веб-камеры

Защита веб-камеры: оповещает о том, какие процессы и приложения осуществляют доступ к подключенной к компьютеру веб-камере. Когда приложение попытается осуществить доступ к вашей камере, вы получите уведомление. В нем можно **разрешить** либо **заблокировать** доступ. Цвет окна уведомления зависит от репутации приложения.

Параметры защиты веб-камеры можно изменить в разделе Расширенные параметры > **Защита** > **Контроль устройств** > **Защита веб-камеры**.

Чтобы активировать функцию защиты веб-камеры в ESET Security Ultimate, включите ползунок рядом с элементом **Включить защиту веб-камеры**.

Если защита веб-камеры включена, элемент **Правила** становится активным, и вы можете открыть окно Редактор правил.

Чтобы отключить оповещения для приложений с правилом, которые были изменены, но все еще имеют действительную цифровую подпись (например, обновление приложения), включите ползунок рядом с элементом **Отключить оповещения о доступе к веб-камере для измененных приложений**.

Редактор правил защиты веб-камеры

В этом окне отображаются имеющиеся правила и предоставляется возможность управлять приложениями и процессами, которые осуществляют доступ к веб-камере вашего компьютера,

основываясь на совершенном вами действии.

Доступны перечисленные далее действия.

- **Разрешить доступ**
- **Заблокировать доступ**

- **Запросить**: спрашивать пользователя каждый раз, когда приложение пытается получить доступ к веб-камере.

Чтобы перестать получать уведомления, когда приложения получают доступ к веб-камере, снимите флажок в столбце **«Уведомить»**.

> **Иллюстрированные инструкции**
> Создание и изменение правил веб-камеры в ESET Security Ultimate.

ThreatSense

ThreatSense — это технология, состоящая из множества сложных методов обнаружения угроз. Эта технология является упреждающей, т. е. она защищает от новой угрозы уже в начале ее распространения. При этом используется сочетание анализа и моделирования кода, обобщенных сигнатур и сигнатур вирусов, которые совместно значительно повышают уровень безопасности компьютера. Модуль сканирования может контролировать несколько потоков данных одновременно, что делает эффективность и количество обнаруживаемых угроз максимальными. Технология ThreatSense также успешно уничтожает руткиты.

Для модуля ThreatSense можно настроить несколько параметров сканирования:

- расширения и типы файлов, подлежащих сканированию;
- сочетание различных методов обнаружения;
- уровни очистки и т. д.

Чтобы открыть окно параметров, щелкните **ThreatSense** в окне расширенных параметров любого модуля, использующего технологию ThreatSense (см. ниже). Разные сценарии обеспечения безопасности могут требовать различных настроек. Поэтому технологию ThreatSense можно настроить отдельно для каждого из перечисленных далее модулей защиты.

- Защита в режиме реального времени
- Сканирование в состоянии простоя
- сканирование при запуске
- Защита документов
- Защита почтового клиента
- защита доступа в Интернет;
- Сканирование компьютера

Параметры ThreatSense хорошо оптимизированы для каждого из модулей, а их изменение значительно влияет на поведение системы. Например, изменение параметров сканирования упаковщиков в режиме реального времени или включение расширенной эвристики в модуле защиты файловой системы в режиме реального времени может замедлить работу системы (обычно только новые файлы сканируются с применением этих методов). Рекомендуется не изменять параметры ThreatSense по умолчанию ни для каких модулей, кроме модуля «Сканирование компьютера».

Сканируемые объекты

В этом разделе можно указать компоненты и файлы компьютера, которые будут сканироваться на наличие заражений.

Оперативная память: сканирование на наличие угроз, которые атакуют оперативную память системы.

Загрузочные секторы/UEFI. Загрузочные секторы сканируются на наличие вредоносных программ в основной загрузочной записи. Дополнительные сведения о UEFI см. в глоссарии.

Почтовые файлы. DBX (Outlook Express) и EML

Архивы. Программа поддерживает такие расширения, как ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE, и многие другие.

Самораспаковывающиеся архивы. Тип архивов (SFX), содержимое которых может извлекаться автоматически.

Программы сжатия исполняемых файлов: в отличие от стандартных типов архивов, программы сжатия исполняемых файлов после запуска распаковываются в памяти. Благодаря эмуляции кода модуль сканирования распознает не только стандартные статические упаковщики (UPX, yoda, ASPack, FSG и т. д.), но и множество других типов упаковщиков.

Параметры сканирования

Выберите способы сканирования системы на предмет заражений. Доступны следующие варианты:

Эвристический анализ: анализ вредоносной активности программ с помощью специального алгоритма. Главным достоинством этого метода является способность идентифицировать вредоносные программы, сведения о которых отсутствуют в существующей версии модуля обновления. Недостатком же является вероятность (очень небольшая) ложных тревог.

Расширенный эвристический анализ/сигнатуры распределенных сетевых атак: для расширенного эвристического анализа используется уникальный эвристический алгоритм компании ESET, который оптимизирован для обнаружения компьютерных червей и троянских программ и написан на высокоуровневых языках программирования. Использование расширенной эвристики значительным образом увеличивает возможности продуктов ESET по обнаружению угроз. С помощью сигнатур осуществляется точное обнаружение и идентификация вирусов. Система автоматического обновления обеспечивает наличие новых сигнатур через несколько часов после обнаружения угрозы. Недостатком же сигнатур является то, что они позволяют обнаруживать только известные вирусы (или их незначительно модифицированные версии).

Очистка

Параметры очистки определяют поведение ESET Security Ultimate при очистке объектов. Предусмотрено четыре уровня очистки.

ThreatSense имеет такие уровни исправления проблем (т. е. очистки):

Исправление в ESET Security Ultimate

Уровень очистки	Описание
Всегда исправлять обнаружения	Пытаться исправлять обнаружения при очистке объектов без вмешательства конечного пользователя. В некоторых случаях (например, с системными файлами), если обнаружение не удается исправить, обнаруженный объект оставляется в исходном расположении.
Исправлять обнаружения, если это безопасно, в другом случае оставить	Пытаться исправлять обнаружения при очистке объектов без вмешательства конечного пользователя. В некоторых случаях (например, системные файлы или архивы, которые содержат и чистые, и зараженные файлы), если обнаружение не удается исправить, обнаруженный объект остается в исходном расположении.
Исправлять обнаружения, если это безопасно, в другом случае спрашивать	Пытаться исправлять обнаружения при очистке объектов. В некоторых случаях, если ни одно из действий выполнить невозможно, конечный пользователь получает интерактивное предупреждение, в котором следует выбрать действие по исправлению (например, удалить или проигнорировать). Этот параметр рекомендуется в большинстве случаев.
Всегда спрашивать у конечного пользователя	Конечному пользователю отображается интерактивное окно при очистке объектов, и он должен выбрать действие по исправлению (например, удалить или пропустить). Этот уровень предназначен для более опытных пользователей, которые знают, какие действия следует предпринять в случае обнаружения.

Исключения

Расширением называется часть имени файла, отделенная от основной части точкой. Оно определяет тип файла и его содержимое. Этот раздел ThreatSense позволяет определить типы файлов, подлежащих сканированию.

Другое

При настройке параметров модуля ThreatSense для сканирования компьютера по требованию также доступны описанные ниже параметры из раздела **Другое**.

Сканировать альтернативные потоки данных (ADS): альтернативные потоки данных, используемые файловой системой NTFS, — это связи файлов и папок, которые не обнаруживаются при использовании обычных методов сканирования. Многие заражения маскируются под альтернативные потоки данных, пытаясь избежать обнаружения.

Запускать фоновое сканирование с низким приоритетом: каждый процесс сканирования потребляет некоторое количество системных ресурсов. Если пользователь работает с

ресурсоемкими программами, можно активировать фоновое сканирование с низким приоритетом и высвободить тем самым ресурсы для других приложений.

Журнал всех объектов. Журнал проверки отображает все отсканированные файлы в самораспаковывающихся архивах, даже незараженные (может создавать большое количество данных журнала сканирования и увеличивать размер его файла).

Включить оптимизацию Smart: при включенной оптимизации Smart используются оптимальные параметры для обеспечения самого эффективного уровня сканирования с сохранением максимально высокой скорости. Разные модули защиты выполняют интеллектуальное сканирование, применяя отдельные методы для различных типов файлов. Если оптимизация Smart отключена, при сканировании используются только пользовательские настройки ядра ThreatSense каждого модуля.

Сохранить отметку о времени последнего доступа: установите этот флажок, чтобы сохранить исходное значение времени доступа к сканируемым файлам, а не обновлять их (например, для использования с системами резервного копирования данных).

Ограничения

В разделе «Ограничения» можно указать максимальный размер объектов и уровни вложенности архивов для сканирования.

Параметры объектов

Максимальный размер объекта: определяет максимальный размер объектов, подлежащих сканированию. Данный модуль защиты от вирусов будет сканировать только объекты меньше указанного размера. Этот параметр рекомендуется менять только опытным пользователям, у которых есть веские основания для исключения из сканирования больших объектов. Значение по умолчанию: Не ограничено.

Максимальная продолжительность сканирования объекта (с): определяет максимальное значение времени для сканирования файлов в объекте-контейнере (например, в архиве RAR/ZIP или в электронном письме с несколькими вложениями). Эта настройка не применяется к отдельным файлам. Если пользователь укажет собственное значение и указанное время истечет, сканирование будет остановлено как можно скорее вне зависимости от того, завершено ли сканирование каждого файла в объекте-контейнере.
Если речь идет об архиве с большими файлами, сканирование будет прекращено не раньше, чем произойдет извлечение файла из архива (например, когда пользователь задал значение в 3 секунды, но извлечение файла занимает 5 секунд). По истечении этого времени остальные файлы в архиве сканироваться не будут.
Чтобы ограничить время сканирования, в том числе для архивов большого размера, используйте параметры **Максимальный размер объекта** и **Максимальный размер файла в архиве** (не рекомендуется в связи с возможными проблемами безопасности).
Значение по умолчанию: Не ограничено.

Настройки сканирования архивов

Уровень вложенности архивов: определяет максимальную глубину проверки архивов. Значение по умолчанию: 10.

Максимальный размер файла в архиве: этот параметр позволяет задать максимальный размер файлов в архиве (при их извлечении), которые должны сканироваться. Максимальное значение — **3 ГБ**.

> Не рекомендуется изменять значения по умолчанию, так как обычно для этого нет особой причины.

Уровни очистки

Чтобы изменить настройки уровня очистки для нужного модуля защиты, разверните элемент **ThreatSense** (например, **Защита файловой системы в реальном времени**), а затем выберите в раскрывающемся меню пункт **Уровень очистки**.

ThreatSense имеет такие уровни исправления проблем (т. е. очистки):

Исправление в ESET Security Ultimate

Уровень очистки	Описание
Всегда исправлять обнаружения	Пытаться исправлять обнаружения при очистке объектов без вмешательства конечного пользователя. В некоторых случаях (например, с системными файлами), если обнаружение не удается исправить, обнаруженный объект оставляется в исходном расположении.
Исправлять обнаружения, если это безопасно, в другом случае оставить	Пытаться исправлять обнаружения при очистке объектов без вмешательства конечного пользователя. В некоторых случаях (например, системные файлы или архивы, которые содержат и чистые, и зараженные файлы), если обнаружение не удается исправить, обнаруженный объект остается в исходном расположении.
Исправлять обнаружения, если это безопасно, в другом случае спрашивать	Пытаться исправлять обнаружения при очистке объектов. В некоторых случаях, если ни одно из действий выполнить невозможно, конечный пользователь получает интерактивное предупреждение, в котором следует выбрать действие по исправлению (например, удалить или проигнорировать). Этот параметр рекомендуется в большинстве случаев.
Всегда спрашивать у конечного пользователя	Конечному пользователю отображается интерактивное окно при очистке объектов, и он должен выбрать действие по исправлению (например, удалить или пропустить). Этот уровень предназначен для более опытных пользователей, которые знают, какие действия следует предпринять в случае обнаружения.

Исключенные из сканирования расширения файлов

Исключенные расширения файлов относятся к ThreatSense. Чтобы настроить исключенные расширения файлов, щелкните **ThreatSense** в окне «Расширенные параметры» для любого модуля, который использует технологию ThreatSense.

Расширением называется часть имени файла, отделенная от основной части точкой. Оно определяет тип файла и его содержимое. Этот раздел ThreatSense позволяет определить типы файлов, подлежащих сканированию.

Не следует путать эту функцию с другими возможностями исключения — Исключения для процессов, Исключения системы HIPS или Исключения файлов/папок.

По умолчанию сканируются все файлы. Любое расширение можно добавить в список файлов, исключенных из сканирования.

Иногда может быть необходимо исключить файлы, если сканирование определенных типов файлов препятствует нормальной работе программы, которая использует эти расширения. Например, может быть полезно исключить расширения `.edb`, `.eml` и `.tmp` при использовании серверов Microsoft Exchange.

Для добавления в список нового расширения нажмите **Добавить**. Введите расширение в пустое поле (например, tmp) и нажмите кнопку **OK**. Выбрав вариант **Добавить несколько значений**, можно добавить несколько расширений имен файлов, разделив их символом перевода строки, запятой или точкой с запятой (например, выберите **Точка с запятой** из раскрывающегося меню в качестве разделителя и введите `edb;eml;tmp`).
Можно использовать специальный символ «?» (вопросительный знак). Вопросительный знак представляет любой символ (например, `?db`).

Чтобы увидеть расширение файла (при наличии расширения) в операционной системе Windows, необходимо установить флажок **Расширения имен файлов** в **проводнике Windows** на вкладке **Вид**.

Дополнительные параметры ThreatSense

Чтобы изменить эти настройки, откройте раздел Расширенные параметры > **Защита** > **Защита файловой системы в реальном времени** > **Дополнительные параметры ThreatSense**.

Дополнительные параметры ThreatSense для только что созданных и измененных файлов

Вероятность заражения только что созданных или измененных файлов выше по сравнению с аналогичным показателем для существующих файлов. Именно поэтому программа проверяет эти файлы с использованием дополнительных параметров сканирования. ESET Security Ultimate вместе с обычными методами сканирования, основанными на сигнатурах, применяет расширенный эвристический анализ, что делает возможным обнаружение новых угроз еще до выпуска обновлений модуля обнаружения.

В дополнение к только что созданным файлам выполняется также сканирование **самораспаковывающихся архивов** (.sfx) и **программ-упаковщиков среды выполнения** (исполняемых файлов с внутренним сжатием). По умолчанию архивы сканируются до 10-го уровня вложенности независимо от их фактического размера. Для изменения параметров проверки архивов снимите флажок **Параметры сканирования архивов по умолчанию**.

Дополнительные параметры ThreatSense для исполняемых файлов

Расширенный эвристический анализ при запуске файлов: по умолчанию при запуске файлов применяется расширенная эвристика. Если этот параметр включен, настоятельно рекомендуется включить оптимизацию Smart и ESET LiveGrid®, чтобы уменьшить воздействие на производительность системы.

Расширенный эвристический анализ при запуске файлов со съемных носителей: прежде чем разрешить запуск кода со съемного носителя, система расширенного эвристического анализа эмулирует код в виртуальной среде и оценивает его поведение.

Служебные программы

Вы можете настроить дополнительные параметры для функций, которые обеспечивают дополнительную безопасность и упрощают администрирование ESET Security Ultimate, в разделе Расширенные параметры > **Сервис**.

- Центр обновления Microsoft Windows®
- ESET CMD
- Файлы журнала
- Игровой режим
- Диагностика

Центр обновления Microsoft Windows®

Функция обновления Windows является важной составляющей защиты пользователей от вредоносных программ. По этой причине обновления Microsoft Windows следует устанавливать сразу после их появления. Программное обеспечение ESET Security Ultimate уведомляет пользователя об отсутствующих обновлениях в соответствии с выбранным уровнем в Расширенные параметры > **Сервис**. Доступны следующие уровни:

- **Без обновлений**: запросы на загрузку обновлений системы не отображаются.
- **Необязательные обновления**: отображаются запросы на загрузку обновлений с низким и более высоким уровнем приоритета.
- **Рекомендуемые обновления**: отображаются запросы на загрузку обновлений с обычным и более высоким уровнем приоритета.
- **Важные обновления**: отображаются запросы на загрузку обновлений, помеченных как важные и с более высоким уровнем приоритета.
- **Критические обновления**: пользователю предлагается загрузить только критические обновления.

Диалоговое окно — обновления системы

При наличии обновлений для вашей операционной системы программа ESET Security Ultimate покажет уведомление в главном окне программы > **Обзор**. Щелкните **Дополнительные сведения**, чтобы открыть окно обновлений системы.

В окне «Обновления системы» представлен список доступных обновлений, готовых для загрузки и установки. Тип обновления отображается рядом с его названием.

Дважды щелкните любую строку обновления, чтобы отобразить окно Информация об обновлениях, содержащее дополнительную информацию.

Щелкните **Запустить обновление системы**, чтобы загрузить и установить все перечисленные обновления операционной системы.

Информация об обновлениях

В окне «Обновления системы» представлен список доступных обновлений, готовых для загрузки и установки. Уровень приоритета обновления отображается справа от его названия.

Нажмите **Запустить обновление системы**, чтобы начать загрузку и установку обновлений операционной системы.

Щелкните правой кнопкой мыши любую строку обновления и нажмите **Показать информацию**, чтобы вывести на экран новое окно с дополнительными сведениями.

ESET CMD

Эта функция включает расширенные команды ecmd. Она позволяет экспортировать и импортировать параметры с помощью командной строки (ecmd.exe). До недавнего времени экспортировать параметры можно было только через графический интерфейс пользователя. Конфигурацию ESET Security Ultimate можно экспортировать в файл с расширением *.xml*.

При включенной функции ESET CMD доступны два метода авторизации:

- **Нет** — без авторизации. Этот метод не рекомендуется, так как он разрешает импорт любой неподписанной конфигурации, что представляет собой потенциальный риск.

- **Пароль для расширенной настройки** — пароль требуется для импорта конфигурации из файла с расширением .xml. Этот файл должен быть подписан (сведения о подписании файла конфигурации с расширением .xml представлены далее). Новую конфигурацию можно импортировать только после того, как будет указан пароль, заданный в разделе Настройка доступа. Если настройка доступа не включена, пароль не совпадает или файл конфигурации в формате .xml не подписан, конфигурация не будет импортирована.

После включения ESET CMD можно использовать командную строку для импорта и экспорта конфигураций программы ESET Security Ultimate. Это можно сделать вручную или создать сценарий с целью автоматизации.

Для использования расширенных команд ECMD необходимо запустить их с правами администратора или открыть командную строку Windows (cmd) командой **Запуск от имени администратора**. В противном случае появится сообщение **Error executing command**. Кроме того, при экспорте конфигурации должна существовать папка назначения. Команда экспорта работает даже при отключенном параметре ESET CMD.

Команда экспорта параметров:
`ecmd /getcfg c:\config\settings.xml`

Команда импорта параметров:
`ecmd /setcfg c:\config\settings.xml`

Расширенные команды ecmd можно выполнить только локально.

Для подписания файла конфигурации в формате XML (*.xml*) выполните следующие действия.

1. Загрузите исполняемый файл XmlSignTool.

2. Откройте командную строку Windows (cmd) с помощью команды **Запуск от имени администратора**.

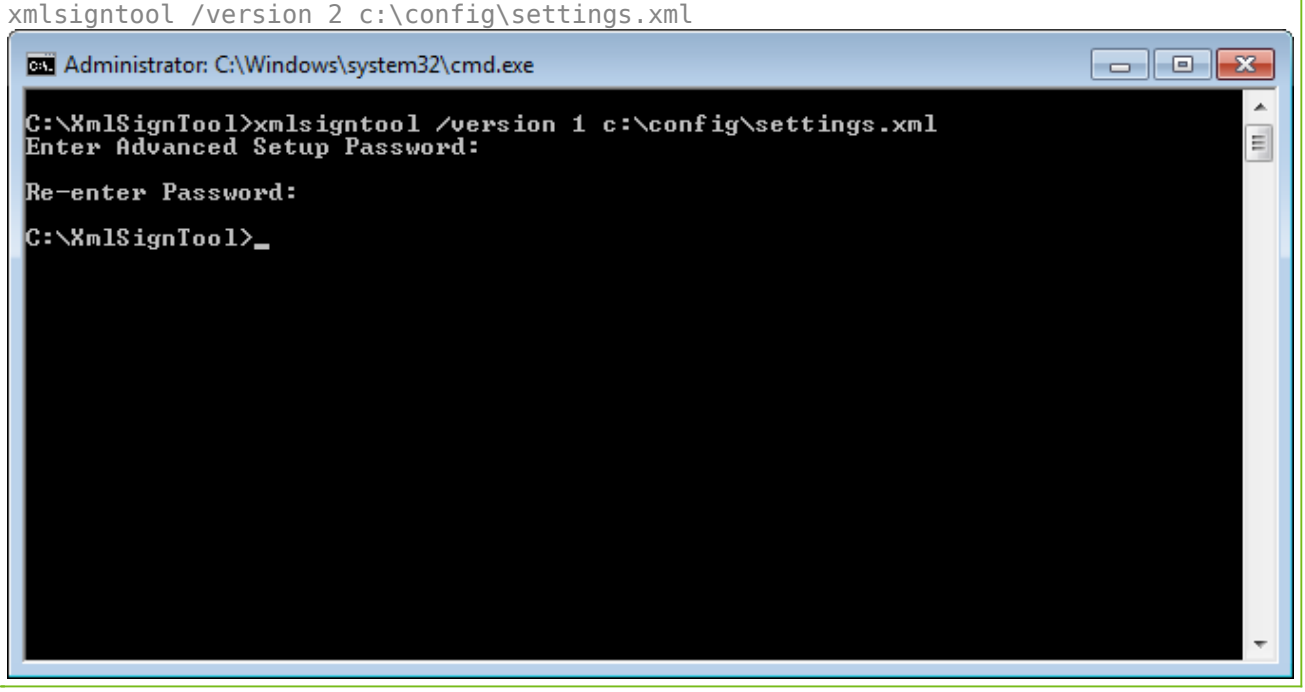
3. Перейдите в расположение файла `xmlsigntool.exe`.

4. Выполните команду для подписания файла конфигурации в формате XML (*.xml*).
Использование: `xmlsigntool /version 1|2 <xml_file_path>`

Значение параметра `/version` зависит от установленной версии ESET Security Ultimate. Используйте `/version 1`, если установлена более старая версия, чем ESET Security Ultimate 11.1. Используйте `/version 2` для актуальной версии ESET Security Ultimate.

5. Введите и повторно введите пароль для расширенных параметров, когда появится запрос средства XmlSignTool. Теперь файл конфигурации в формате *XML* подписан и может использоваться для импорта в другом экземпляре ESET Security Ultimate с функцией ESET CMD с помощью метода парольной авторизации.

Команда подписания экспортированного файла конфигурации:
`xmlsigntool /version 2 c:\config\settings.xml`



Если пароль в разделе Настройка доступа изменится и потребуется импортировать конфигурацию, подписанную ранее с помощью старого пароля, необходимо подписать файл конфигурации в формате *.xml* заново с помощью текущего пароля. Это позволит использовать старый файл конфигурации без необходимости экспортировать его на другой компьютер с работающей программой ESET Security Ultimate перед импортом.

Включать ESET CMD без авторизации не рекомендуется, поскольку это даст возможность импортировать любую неподписанную конфигурацию. Установите пароль в разделе Дополнительные настройки > **Интерфейс пользователя** > **Настройка доступа**, чтобы пользователи не вносили неавторизованные изменения.

Файлы журнала

Конфигурацию ведения журнала ESET Security Ultimate можно найти в разделе Расширенные параметры > **Сервис** > **Файлы журнала**. Этот раздел используется для настройки управления журналами. Программа автоматически удаляет старые файлы журналов, чтобы сэкономить дисковое пространство. Для файлов журнала можно задать параметры, указанные ниже.

Минимальная степень детализации журнала: настройка минимального уровня детализации записей о событиях.

- **Диагностика**: в журнал вносится информация, необходимая для тщательной настройки программы, и все перечисленные выше записи.
- **Информация**: в журнал вносятся информационные сообщения, в том числе сообщения об успешном выполнении обновления, а также все перечисленные выше записи.
- **Предупреждения**: в журнал вносится информация обо всех критических ошибках и предупреждениях.
- **Ошибки**: в журнал вносится информация об ошибках загрузки файлов и критических ошибках.
- **Критические ошибки**: регистрируются только критические ошибки (ошибки запуска защиты от вирусов,, файервола, итд).

Если выбрать уровень детализации «Диагностика», в журнал будут записываться сведения обо всех заблокированных подключениях.

Записи в журнале, созданные раньше, чем указано в поле **Автоматически удалять записи старше, чем X дн.**, будут автоматически удаляться.

Автоматически оптимизировать файлы журналов: если этот флажок установлен, файлы журналов будут автоматически дефрагментироваться в тех случаях, когда процент фрагментации превышает значение, указанное в параметре **Если количество неиспользуемых записей превышает (%)**.

Щелкните **Оптимизировать**, чтобы начать дефрагментацию файлов журналов. При этом удаляются все пустые записи журналов, что улучшает производительность и скорость обработки журналов. Такое улучшение особенно заметно, если в журналах содержится большое количество записей.

Выберите **Включить текстовый протокол**, чтобы разрешить хранение журналов в другом формате отдельно от файлов журналов.

• **Целевой каталог**: каталог, в котором будут храниться файлы журналов (только для текстового формата и формата CSV). Каждый раздел журнала сохраняется в отдельный файл с предварительно заданным именем (например, в файл virlog.txt записывается раздел **Обнаружения** файла журнала, если для хранения файлов журнала вами выбран формат обычного текста).

• **Тип**: если выбрать формат **Текст**, журналы будут сохраняться в текстовый файл, данные в котором будут разделены табуляцией. То же касается формата **CSV**. Если выбрать **Событие**, журналы будут сохраняться не в файл, а в журнал событий Windows (его можно просмотреть на панели управления в средстве просмотра событий).

• **Удалить все файлы журнала**: удаляет все сохраненные журналы, выбранные в раскрывающемся меню **Тип**. После удаления журналов появится уведомление о завершении процесса удаления.

Для более быстрого решения проблем специалисты ESET иногда могут запрашивать у пользователей журналы с их компьютеров. ESET Log Collector облегчает сбор необходимой информации. Дополнительные сведения о ESET Log Collector см. в этой статье базы знаний ESET.

Игровой режим

Игровой режим — это функция для пользователей, которым нужно избежать перерывов при использовании своих программ и появления отвлекающих уведомлений или предупреждений, а также свести к минимуму нагрузку на процессор (CPU). Его также можно использовать во время презентаций, которые нельзя прерывать деятельностью модуля защиты от вирусов. При включении этой функции отключаются все всплывающие окна, а работа планировщика полностью останавливается. Защита системы по-прежнему работает в фоновом режиме, но не требует какого-либо вмешательства со стороны пользователя.

Включение и отключение игрового режима осуществляется в главном окне программы в разделе **Настройка** > **Защита компьютера**, где необходимо щелкнуть  или  рядом с элементом **Игровой режим**. Включая игровой режим, вы подвергаете систему угрозе, поэтому значок состояния защиты на панели задач станет оранжевым и будет отображать предупреждение. Кроме того, данное предупреждение будет отображаться в главном окне программы, где оранжевым цветом будет написано **Игровой режим активен**.

Активируйте параметр **Автоматически включать игровой режим при выполнении приложений в полноэкранном режиме** в разделе Расширенные параметры > **Сервис** > **Игровой режим**, чтобы игровой режим включался при запуске любого приложения в полноэкранном режиме и выключался при выходе из приложения.

Выберите параметр **Автоматически отключать игровой режим через**, чтобы задать время, спустя которое игровой режим будет автоматически отключаться.

Если файервол работает в интерактивном режиме и включен игровой режим, возможны проблемы при подключении к Интернету. Это может представлять сложности, если запускается игра, в которой используется подключение к Интернету. Обычно пользователю предлагается подтвердить нужное действие (если не задано никаких правил или исключений для подключения), но в игровом режиме взаимодействие с пользователем невозможно. Чтобы разрешить сетевое взаимодействие, определите правило подключения для каждого приложения, которое может его осуществлять, или используйте другой Режим фильтрации в файерволе. Также следует помнить о том, что при включенном игровом режиме может быть заблокирован переход на веб-страницу или использование приложения, которые способны представлять угрозу для безопасности, но при этом на экран не будет выведено никакого пояснения или предупреждения, поскольку взаимодействие с пользователем отключено.

Диагностика

Средство диагностики собирает аварийные дампы процессов ESET (например, ekrn). Если происходит аварийное завершение работы приложения, создается соответствующий дамп. С помощью таких дампов разработчики могут отлаживать и исправлять различные проблемы программы ESET Security Ultimate.

Откройте раскрывающееся меню рядом с элементом **Тип дампа** и выберите один из трех доступных вариантов:

• Выберите **Отключить**, чтобы отключить эту функцию.

• **Мини** (по умолчанию) — регистрируется самый малый объем полезной информации, которая может помочь определить причину неожиданного сбоя приложения. Подобный файл дампа может пригодиться, если на диске мало места. Однако ограниченный объем включенной в него информации может при анализе не позволить обнаружить ошибки, которые не были вызваны непосредственно потоком, выполнявшимся в момент возникновения проблемы.

• **Полный**: когда неожиданно прекращается работа приложения, регистрируется все содержимое системной памяти. Полный дамп памяти может содержать данные процессов, которые выполнялись в момент создания дампа.

Целевой каталог — каталог, в котором будет создаваться дамп при сбое.

Открыть папку диагностики: нажмите кнопку **Показать**, чтобы открыть этот каталог в новом окне проводника *Windows*.

Создать дамп диагностики: нажмите кнопку **Создать**, чтобы создать в **целевом каталоге** файлы дампа диагностики.

Расширенное ведение журналов

Включить расширенное ведение журналов в рекламных сообщениях: запись всех событий, связанных с рекламными сообщениями в продукте.

Включить расширенное ведение журнала для модуля защиты от спама: запись всех

событий, которые происходят в процессе сканирования на наличие спама. Это помогает разработчикам выявлять и исправлять проблемы, связанные с модулем защиты от спама ESET.

Включить расширенное ведение журнала для модуля Антивор: запись всех событий, которые происходят в модуле Антивор, для диагностики и устранения проблем.

Включить расширенное ведение журналов для защиты браузера: запись всех событий, происходящих в функции «Защита банковских операций и браузера».

Включить расширенное ведение журналов для модуля сканирования компьютера: запись всех событий, возникающих в процессе сканирования файлов и папок функцией «Сканирование компьютера».

Включение расширенного ведения журнала контроля устройств: запись всех событий, которые происходят в модуле контроля устройств. Это помогает разработчикам выявлять и исправлять проблемы, связанные с модулем контроля устройств.

Включить расширенное ведение журнала Direct Cloud: запись всех событий, которые происходят в ESET LiveGrid®. Это помогает разработчикам выявлять и исправлять проблемы, связанные с модулем ESET LiveGrid®.

Включить расширенное ведение журнала защиты документов: запись всех событий, которые происходят в модуле защиты документов, для диагностики и устранения проблем.

Включить расширенное ведение журналов защиты почтового клиента — запись всех событий, происходящих в защите почтового клиента и плагине почтового клиента, для диагностики и решения проблем.

Включить расширенное ведение журнала ESET LiveGuard: запись всех событий, которые происходят в модуле ESET LiveGuard, для диагностики и устранения проблем.

Включить расширенное ведение журнала ядра: запись всех событий, которые происходят в ядре ESET (ekrn).

Включить расширенное ведение журнала для лицензирования: запись всего обмена данными между серверами ESET License Manager или решением для активации ESET.

Включить трассировку памяти: запись всех событий, которые помогут разработчикам выявлять утечки памяти.

Включить расширенное ведение журнала защиты сети: запись всех сетевых данных, проходящих через файервол в формате PCAP. Это помогает разработчикам выявлять и устранять проблемы, связанные с файерволом.

Включить расширенное ведение журнала для сканера сетевого трафика: запись всех данных, проходящих через сканер сетевого трафика в формате PCAP. Это помогает разработчикам выявлять и устранять проблемы, связанные со сканером сетевого трафика.

Включить расширенное ведение журнала операционной системы: запись дополнительных сведений об операционной системе, например о запущенных процессах, активности ЦП и работе дисков. Это помогает разработчикам диагностировать и исправлять проблемы, связанные с продуктом ESET в вашей операционной системе.

Включить расширенное ведение журнала родительского контроля: запись всех событий, которые происходят в модуле родительского контроля. Это помогает разработчикам выявлять и исправлять проблемы, связанные с модулем родительского контроля.

Включить расширенное ведение журналов для обмена push-сообщениями: запись всех событий, происходящих во время обмена push-сообщениями.

Включение расширенного ведения журналов для защиты файловой системы в реальном времени: запись всех событий, происходящих в процессе сканирования файлов и папок функцией «Защита файловой системы в реальном времени».

Включить расширенное ведение журнала для модуля обновления: запись всех событий, которые происходят во время обновления. Это помогает разработчикам выявлять и исправлять проблемы, связанные с модулем обновления.

Файлы журнала находятся в папке *C:\ProgramData\ESET\ESET Security\Diagnostics*.

Служба технической поддержки

При обращении в службу технической поддержки ESET из программы ESET Security Ultimate можно отправить данные о конфигурации системы. Выберите **Отправлять всегда** в раскрывающемся меню **Отправка данных о конфигурации системы** для автоматической отправки данных или выберите **Запрашивать подтверждение перед отправкой**, чтобы получать запрос перед отправкой данных.

Подключение

В определенных сетях подключение компьютеров к Интернету может осуществляться через прокси-сервер. Если вы используете прокси-сервер, вам необходимо задать следующие настройки. В противном случае решение ESET Security Ultimate и его модули не смогут обновляться автоматически. В ESET Security Ultimate настройка прокси-сервера доступна в двух разных разделах расширенных параметров.

Глобальные настройки прокси-сервера можно конфигурировать в разделе Расширенные параметры > **Подключение** > **Прокси-сервер**. Настройка прокси-сервера на этом уровне позволяет задать его параметры для программы ESET Security Ultimate в целом. Они используются всеми модулями программы, которым требуется подключение к Интернету.

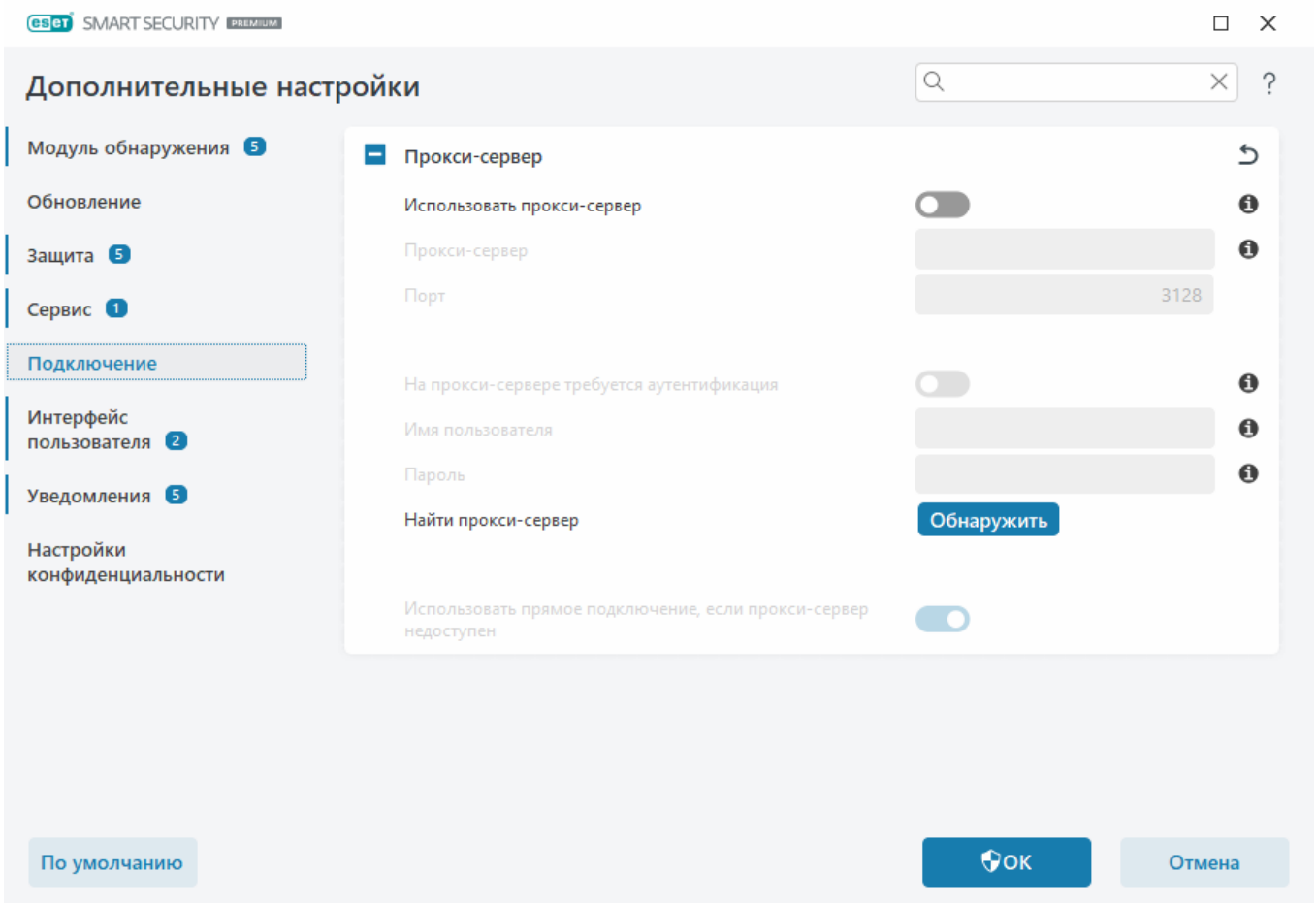
Чтобы задать глобальные настройки прокси-сервера, включите параметр **Использовать прокси-сервер** и введите адрес **прокси-сервера**, а также его номер **порта**.

Если для обмена данными с прокси-сервером требуется аутентификация, установите флажок **Прокси-сервер требует аутентификации**, а затем заполните поля **Имя пользователя** и **Пароль**. Щелкните **Обнаружить прокси-сервер**, чтобы обнаружить и автоматически заполнить настройки прокси-сервера. ESET Security Ultimate скопирует параметры, указанные в свойствах обозревателя для Internet Explorer или Google Chrome.

> В настройках **прокси-сервера** имя пользователя и пароль нужно вводить вручную.

Использовать прямое подключение, если прокси-сервер недоступен: если в ESET Security Ultimate настроено подключение через прокси-сервер, а он недоступен, ESET Security Ultimate будет обходить прокси-сервер и подключаться к серверам ESET напрямую.

Параметры прокси-сервера также можно настроить в области Дополнительные настройки > **Обновление** > **Профили** > **Обновления** > **Параметры подключения** и в раскрывающемся списке **Режим прокси-сервера** выберите элемент **Подключение через прокси-сервер**). Эта конфигурация применяется только для обновлений и рекомендуется для ноутбуков, получающих обновления модулей из удаленных расположений. Дополнительные сведения см. в разделе Дополнительные настройки обновления.



Интерфейс пользователя

Чтобы настроить поведение графического интерфейса программы, откройте раздел Расширенные параметры > **Интерфейс**.

В окне Элементы интерфейса расширенных параметров можно настроить внешний вид программы и используемые эффекты.

Чтобы обеспечить максимальную защиту для программы безопасности, можно запретить удаление программы или внесение несанкционированных изменений, защитив параметры паролем с помощью служебной программы Настройка доступа.

> Сведения о том, как настроить системные уведомления, предупреждения об обнаружении и состояния приложения, см. в разделе Уведомления.

Элементы интерфейса пользователя

Рабочую среду ESET Security Ultimate (графический интерфейс пользователя) можно настроить в соответствии со своими предпочтениями в разделе Расширенные параметры > **Интерфейс** > **Элементы интерфейса**.

Режим цвета: выберите в раскрывающемся меню цветовую схему интерфейса ESET Security Ultimate.

- **Соответствовать цвету системы**: цветовая схема ESET Security Ultimate задается согласно настройкам операционной системы.
- **Темная**: выбор темной цветовой схемы для ESET Security Ultimate (темный режим).
- **Светлая**: выбор стандартной (светлой) цветовой схемы для ESET Security Ultimate.

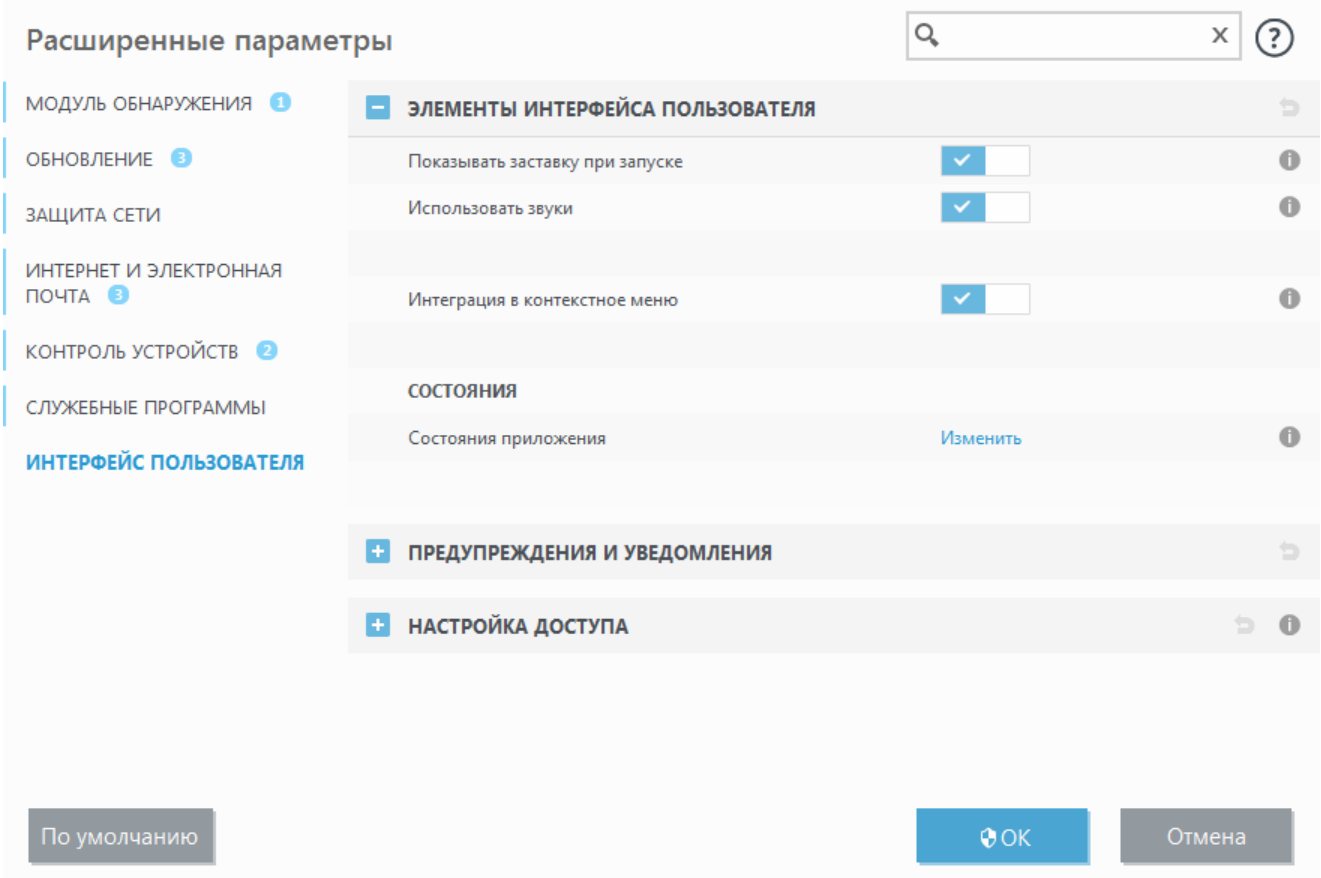
> Кроме того, цветовую схему графического интерфейса ESET Security Ultimate можно выбрать в правом верхнем углу главного окна программы.

Показывать заставку при запуске: во время запуска будет отображаться заставка ESET Security Ultimate.

Использовать звуки: программа воспроизводит звуковой сигнал, если во время сканирования происходит важное событие, например при обнаружении угрозы или завершении сканирования.

Прозрачный фон: включение эффекта прозрачного фона для главного окна программы. Прозрачный фон доступен только для последних версий Windows (RS4 и более поздних).

Интегрировать с контекстным меню: возможность интеграции элементов управления ESET Security Ultimate в контекстное меню.



Настройка доступа

Настройки ESET Security Ultimate являются важной составной частью вашей политики безопасности. Несанкционированное изменение параметров может нарушить стабильность работы системы и ослабить ее защиту. Для предотвращения несанкционированного изменения параметры настройки и возможность удаления приложения ESET Security Ultimate можно защитить паролем. Доступ можно настроить в разделе Расширенные параметры > **Интерфейс** > **Настройка доступа**.

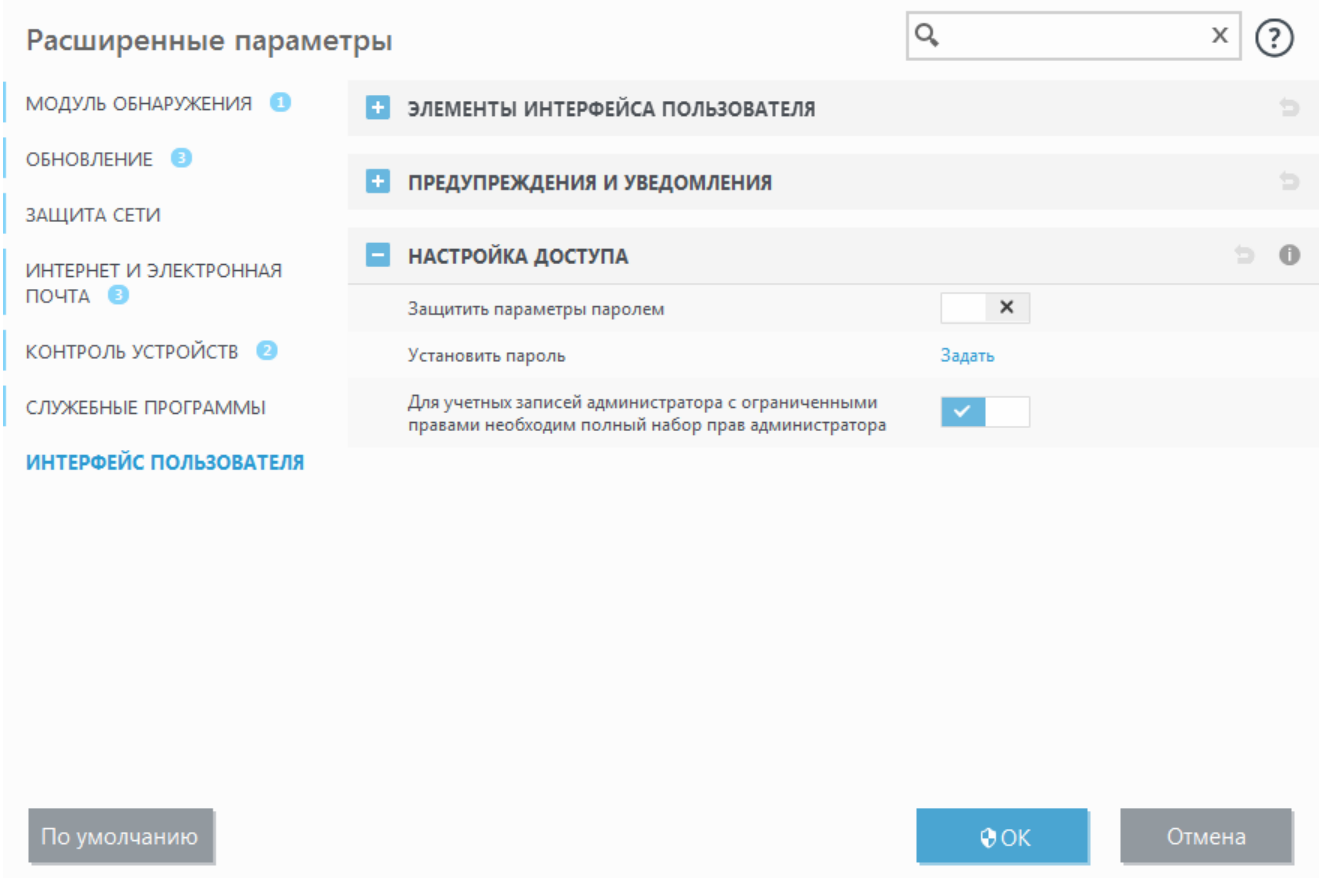
Чтобы установить пароль для защиты параметров настройки и функции удаления приложения ESET Security Ultimate, щелкните **Задать** рядом с полем **Защитить параметры паролем**.

Когда вы хотите получить доступ к защищенным дополнительным настройкам, открывается окно для ввода пароля. Если вы забудете или потеряете свой пароль, щелкните опцию **Восстановить пароль** ниже и введите адрес электронной почты, указанный при регистрации подписки. ESET отправит вам сообщение электронной почты с кодом проверки и инструкциями по сбросу пароля.

- Разблокировка дополнительных настроек

Чтобы изменить пароль, щелкните **Изменить пароль** рядом с полем **Защитить параметры паролем**.

Чтобы удалить пароль, щелкните **Удалить** рядом с полем **Защитить параметры паролем**.



Пароль для доступа к расширенным параметрам

Чтобы защитить расширенные параметры ESET Security Ultimate и избежать их несанкционированного изменения, введите новый пароль в поля **Новый пароль** и **Подтвердите пароль**. Нажмите кнопку **OK**.

Если нужно изменить существующий пароль, выполните следующие действия.

1. Введите старый пароль в поле **Старый пароль**.
2. Введите новый пароль в поля **Новый пароль** и **Подтвердите пароль**.
3. Нажмите кнопку **OK**.

Этот пароль будет необходим для доступа к расширенным параметрам.

Если вы забудете пароль, см. раздел Разблокировка пароля для настроек в продуктах ESET для домашнего использования.

Сведения о восстановлении утерянного ключа активации ESET, дате истечения срока действия подписки и прочие сведения о подписке ESET Security Ultimate см. в разделе Действия в случае потери ключа активации.

Поддержка средств чтения с экрана

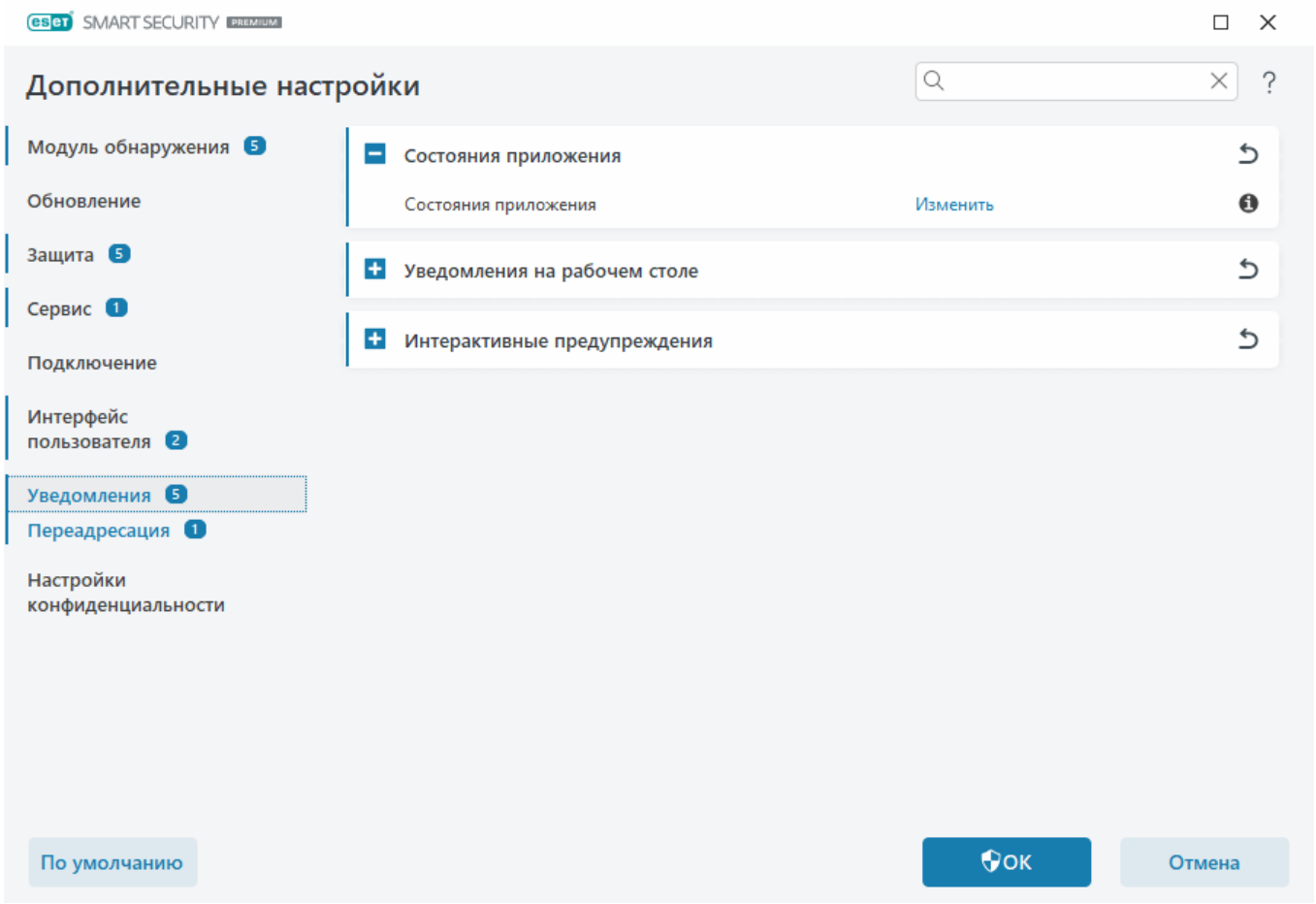
ESET Security Ultimate можно использовать со средствами чтения с экрана, чтобы пользователи ESET с проблемами зрения могли использовать меню продукта и настраивать параметры. Поддерживаются следующие средства чтения с экрана: (JAWS, NVDA, Narrator).

Чтобы обеспечить правильную работу средства чтения с графическим интерфейсом ESET Security Ultimate, следуйте инструкциям в статье нашей базы знаний.

Уведомления

Чтобы управлять уведомлениями ESET Security Ultimate, откройте раздел Расширенные параметры > **Уведомления**. Можно настроить следующие типы уведомлений.

- Состояния приложения: уведомления, отображаемые в главном окне программы в разделе **Обзор**.
- Уведомления на рабочем столе: небольшие окна уведомления рядом с системной панелью задач.
- Интерактивные предупреждения: окна и сообщения с предупреждениями, которые требуют вмешательства пользователя.
- Переадресация (уведомления по электронной почте): уведомления отправляются на указанный адрес электронной почты.



Состояния приложения

Состояния приложения: щелкните **Изменить**, чтобы выбрать, какие состояния приложения будут отображаться на домашней странице главного окна программы > **Обзор**.

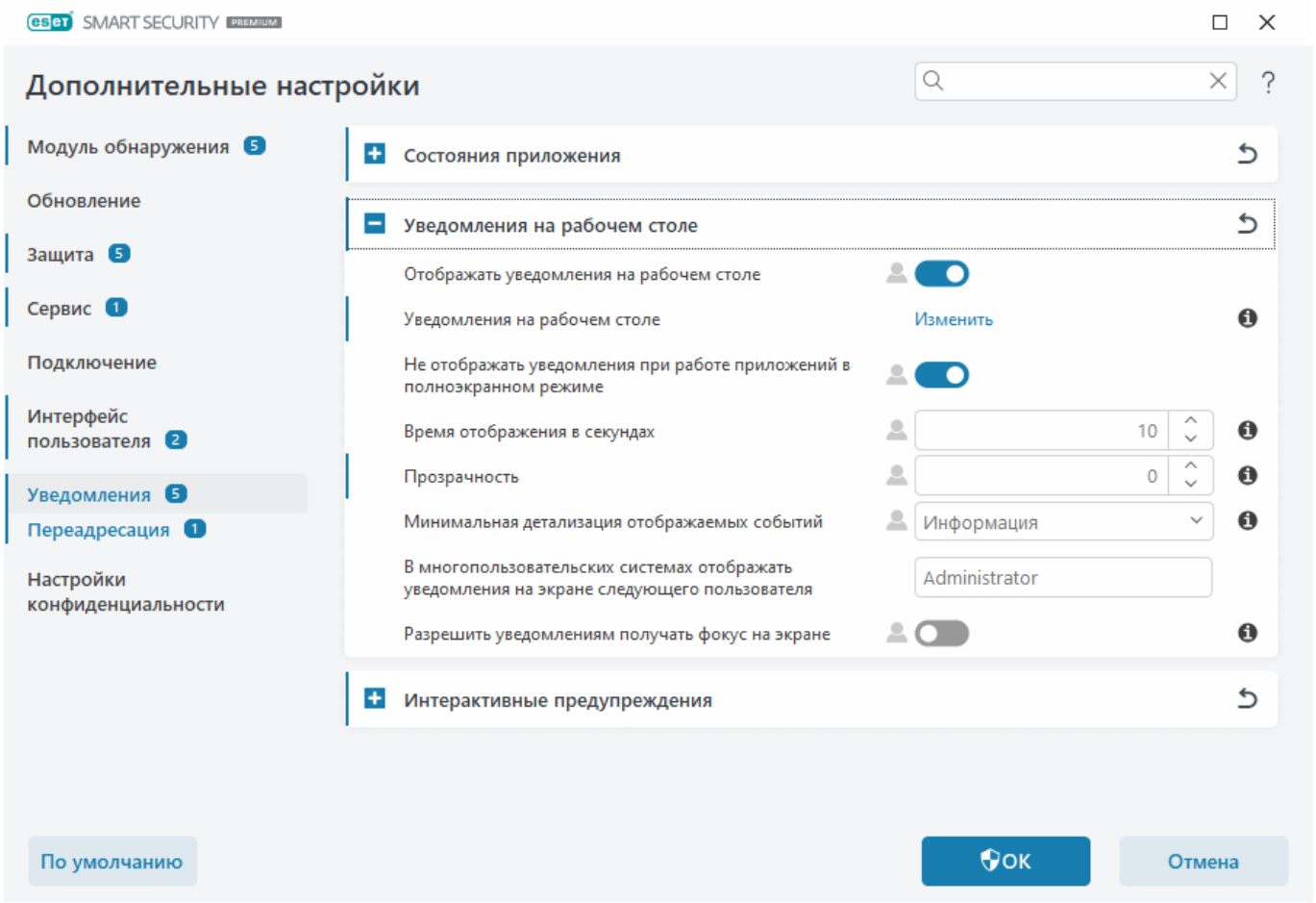
Диалоговое окно «Состояния приложения»

В этом диалоговом окне можно выбрать, какие состояния приложения будут отображаться. Например, при приостановке защиты от вирусов и шпионских программ или при включенном игровом режиме.

Кроме того, состояние приложения будет отображаться, если продукт не активирован или истек срок действия подписки.

Уведомления на рабочем столе

Уведомления на рабочем столе отображаются в виде небольшого окна уведомления рядом с панелью задач системы. По умолчанию оно отображается в течение 10 секунд, затем медленно исчезает. Уведомления сообщают об обновлении программы, подключении новых устройств, завершении задач сканирования на наличие вирусов и об обнаружении новых угроз.



Отображать уведомления на рабочем столе: рекомендуем не выключать этот параметр, чтобы продукт мог сообщать вам о новых событиях.

Уведомления на рабочем столе: щелкните **Изменить**, чтобы включить или отключить определенные уведомления на рабочем столе.

Не отображать уведомления при работе приложений в полноэкранном режиме: скрытие всех неинтерактивных уведомлений, когда запущены приложения в полноэкранном режиме.

Время отображения в секундах: настройка продолжительности отображения уведомлений. Значение должно быть от 3 до 30 секунд.

Прозрачность: настройка процента прозрачности уведомлений. Поддерживаются значения от 0 (без прозрачности) до 80 (очень высокая прозрачность).

Минимальная детализация отображаемых событий: настройка начального уровня серьезности уведомлений, которые следует отображать. В раскрывающемся меню можно выбрать следующие параметры.

- **Диагностика**: отображение информации, необходимой для тщательной настройки программы, и все перечисленные выше записи.
- **Информация**: отображение информационных сообщений, например о нестандартных сетевых событиях, включая сообщения об успешном обновлении, а также все перечисленные выше записи.

- **Предупреждения**: отображение предупреждений, сообщений об ошибках и критических ошибках (например, о невыполненном обновлении).

- **Ошибки**: отображение сообщений об ошибках (например, о том, что не удалось запустить защиту документов) и критических ошибках.

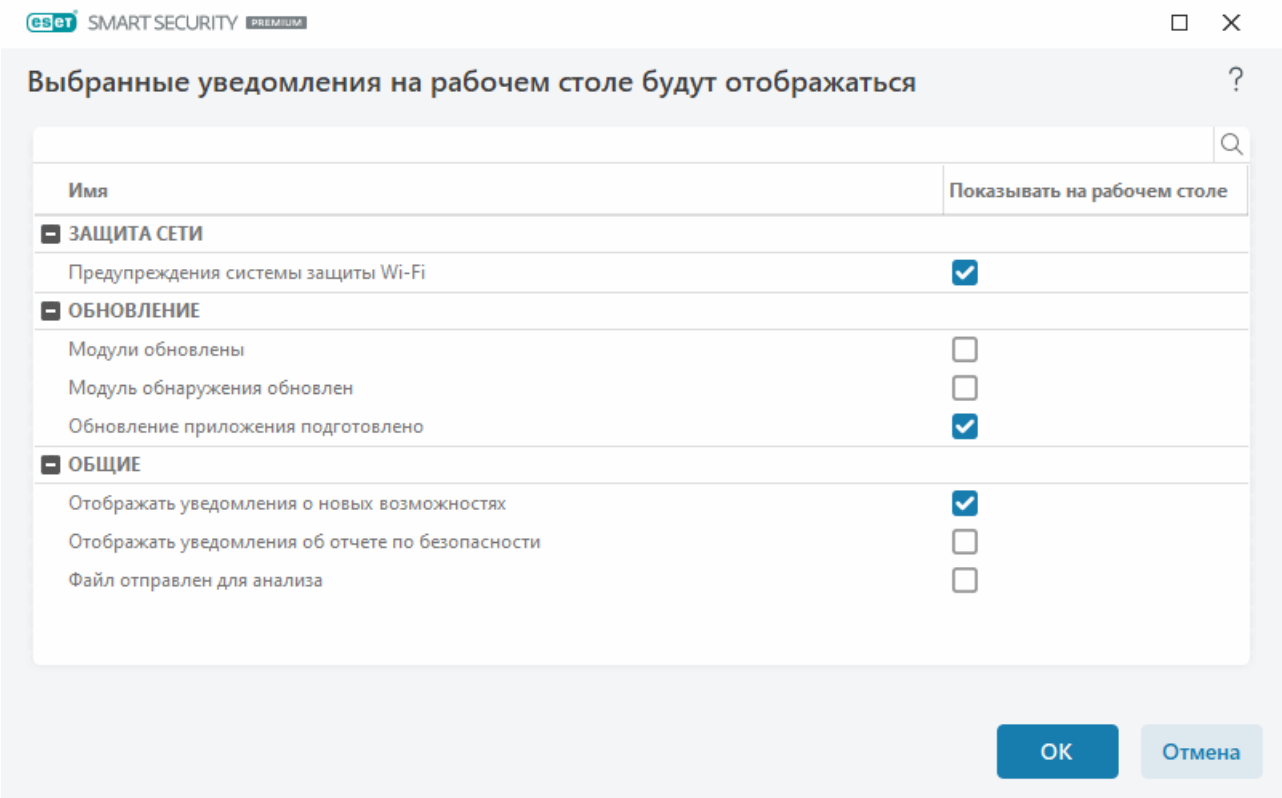
- **Критические ошибки**: отображение сообщений только о критических ошибках (ошибка запуска защиты от вирусов или сообщение о заражении системы и т. п.).

В многопользовательских системах отображать уведомления на экране следующего пользователя: можно разрешить выбранным учетным записям получать уведомления на рабочем столе. Например, если учетная запись администратора не используется, введите полное имя учетной записи, и уведомления на рабочем столе будут отображаться для указанной учетной записи. Получать уведомления на рабочем столе может только одна учетная запись пользователя.

Разрешить уведомлениям получать фокус на экране: можно разрешить уведомлениям получать фокус на экране и быть доступными в меню **ALT + Tab**.

Список уведомлений на рабочем столе

Чтобы изменить видимость уведомлений на рабочем столе (отображаются в правом нижнем углу экрана), откройте раздел Расширенные параметры > **Уведомления** > **Уведомления на рабочем столе**. Щелкните **Изменить** рядом с элементом **Уведомления на рабочем столе** и установите соответствующий флажок **Показать**.



Общие

Отображать уведомления об отчете по безопасности: получение уведомления при создании нового отчета по безопасности.

Отображать уведомления о новых возможностях: уведомления обо всех новых и усовершенствованных функциях в последней версии продукта.

Файл отправлен для анализа: получение уведомления каждый раз, когда ESET Security Ultimate отправляет файл на анализ.

Инспектор сети

Уведомлять о новых сетевых устройствах: получение уведомления при подключении нового устройства к сети.

Защита сети

Профиль сети изменен: получение уведомления об изменении профиля сети.

Предупреждения системы защиты Wi-Fi: получение уведомления при попытке подключения к сети Wi-Fi со слабым паролем или без него.

Обновление

Обновление приложения подготовлено: получение уведомления, когда подготовлено обновление до новой версии ESET Security Ultimate.

Модуль обнаружения обновлен: получение уведомления, когда продукт обновляет модуль обнаружения.

Модули обновлены: получение уведомления, когда продукт обновляет компоненты программы.

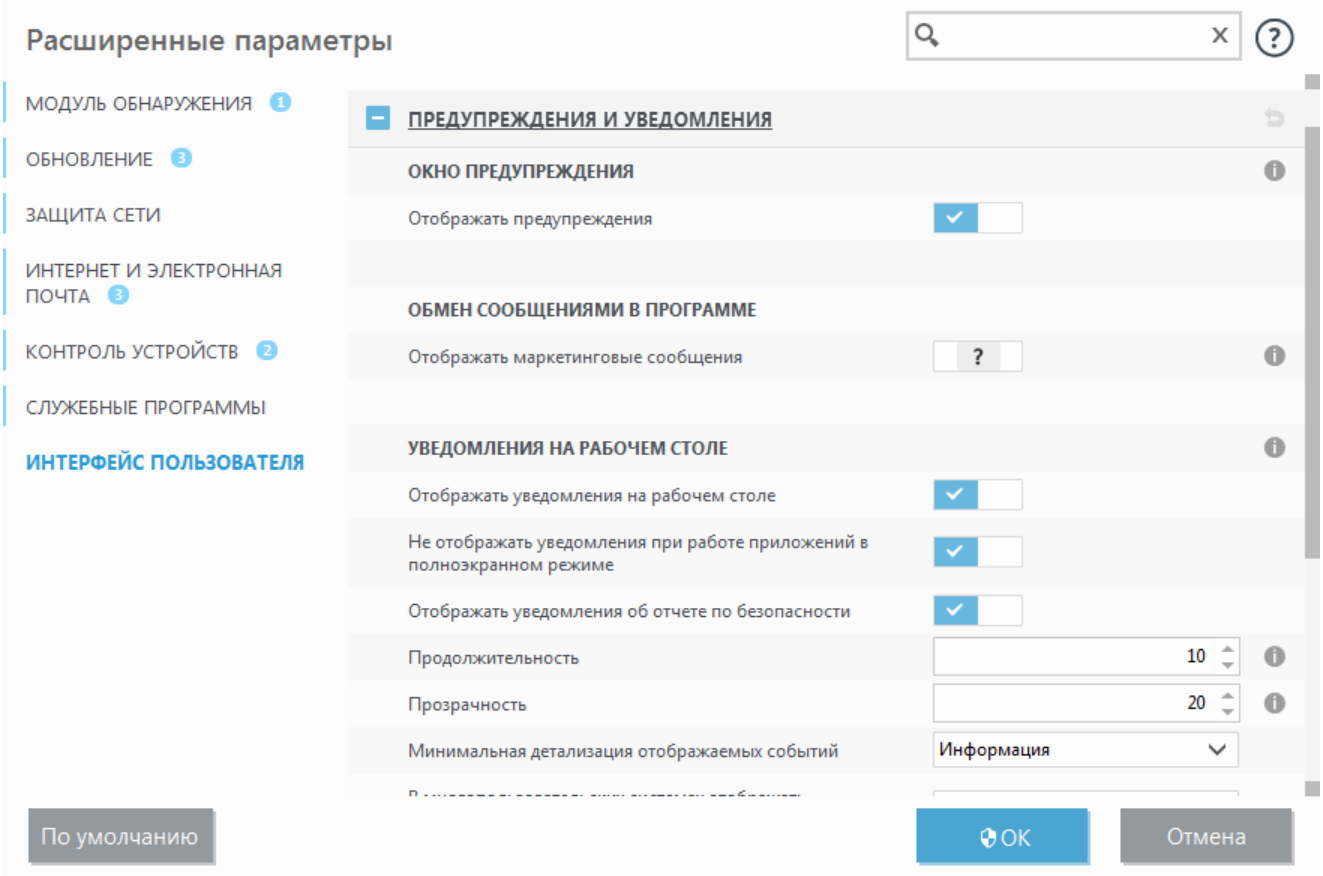
Чтобы задать общие параметры для уведомлений на рабочем столе (например, время отображения сообщения или минимальную детализацию отображаемых событий), выберите Уведомления на рабочем столе в разделе Расширенные параметры > **Уведомления**.

Интерактивные предупреждения

Нужны сведения о распространенных предупреждениях и уведомлениях?

- Угроза найдена
- Адрес заблокирован
- Программа не активирована
- Переход к использованию продукта с большим количеством функций
- Переход к использованию продукта с меньшим количеством функций
- Доступно обновление
- Данные обновления не согласованы
- Устранение ошибки «Обновление модулей не выполнено»
- Устранение ошибок обновления модулей
- Сетевая угроза заблокирована
- Сертификат веб-сайта отозван

Раздел **Интерактивные предупреждения**, который можно открыть, выбрав Расширенные параметры> **Уведомления**, позволяет конфигурировать способ обработки в программе ESET Security Ultimate окон с сообщениями и интерактивных предупреждений об обнаружениях, в которых требуется принятие решения пользователем (например, о потенциальных фишинговых веб-сайтах).



Интерактивные предупреждения

Если отключить параметр **Отображать интерактивные предупреждения**, окна предупреждений и диалоговые окна браузера выводиться на экран не будут. Такой подход следует использовать только для ограниченного количества особых ситуаций. Рекомендуем оставить этот параметр включенным.

Обмен сообщениями в программе

Функция внутрипрограммного обмена сообщениями предназначена для информирования пользователей о новостях ESET и для других сообщений. Для отправки маркетинговых сообщений требуется согласие пользователя. Маркетинговые сообщения по умолчанию не отправляются пользователю (отображается как вопрос). Включение этого параметра означает ваше согласие на получение маркетинговых сообщений ESET. Если вы не хотите получать маркетинговые материалы ESET, отключите параметр **Отображать маркетинговые сообщения**.

Окно сообщения

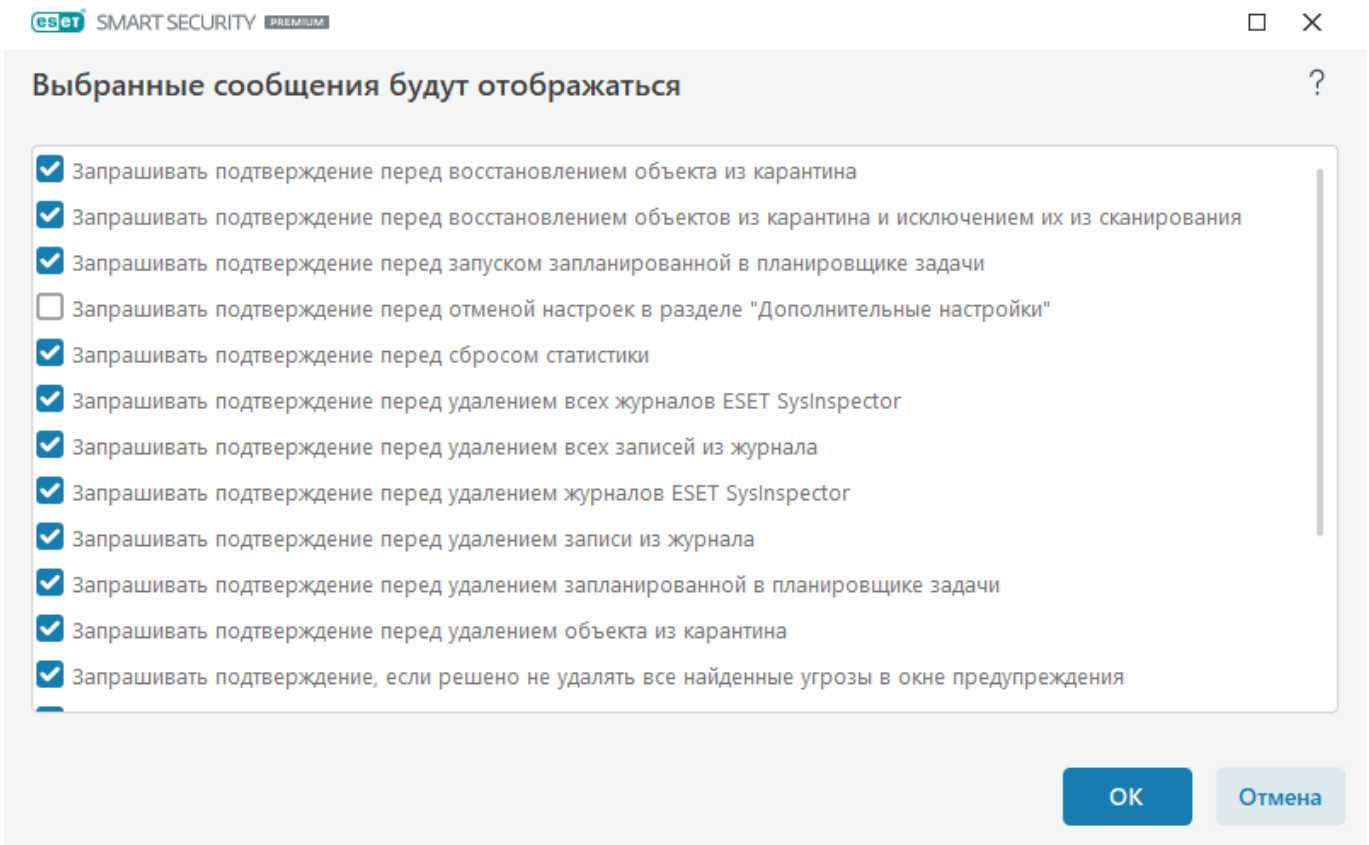
Чтобы окна сообщений закрывались автоматически по истечении определенного времени, установите флажок **Автоматически закрывать окна сообщений**. Если окно предупреждения не будет закрыто пользователем, оно закрывается автоматически через указанный промежуток времени.

Время отображения в секундах: настройка продолжительности отображения предупреждения. Значение должно быть от 10 до 999 секунд.

Подтверждения: щелкните **Изменить**, чтобы открыть список подтверждений, для которых можно включить или отключить отображение.

Подтверждения

Чтобы настроить подтверждения, откройте раздел Расширенные параметры > **Уведомления** > **Интерактивные предупреждения**, а затем щелкните **Изменить** рядом с элементом **Подтверждения**.



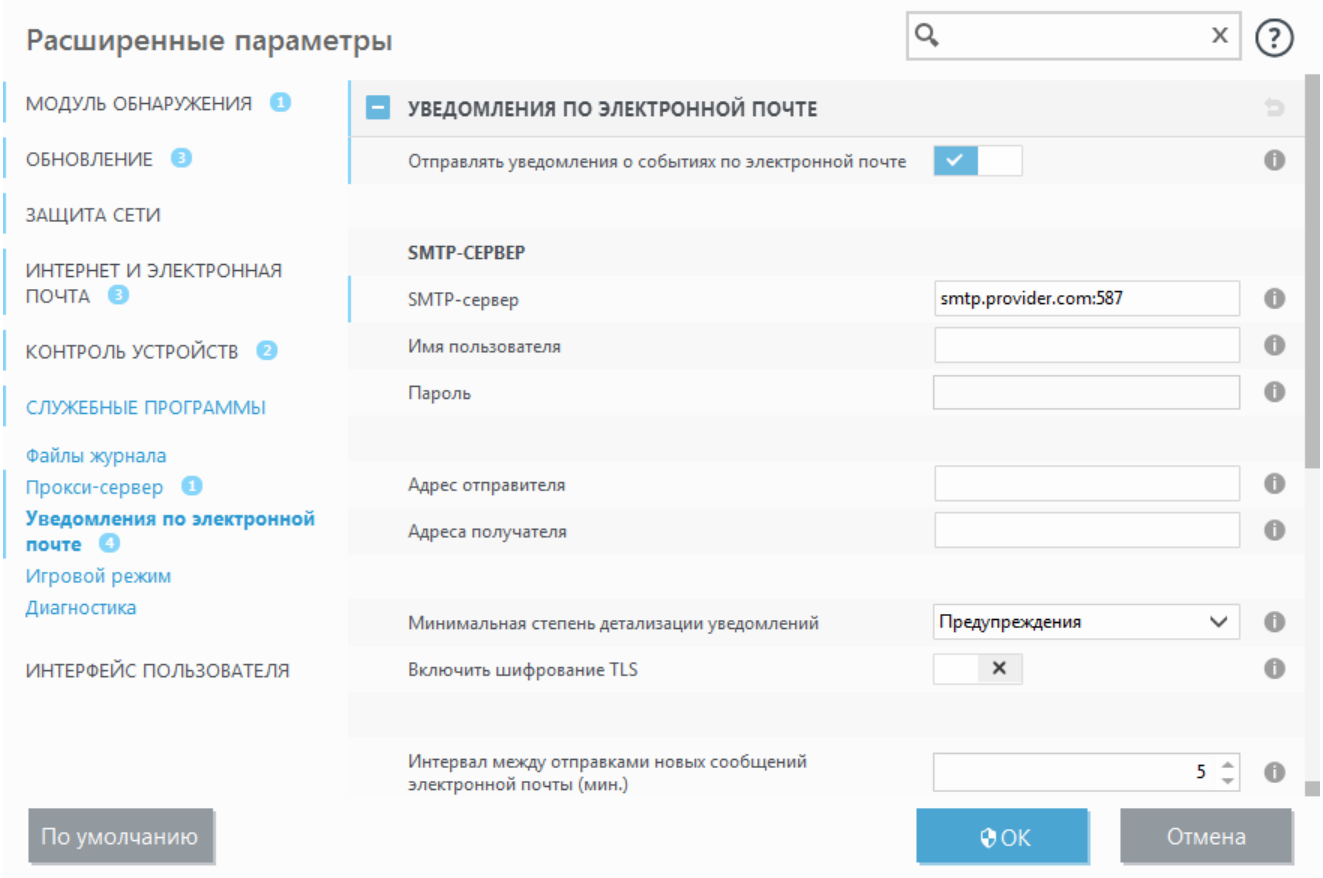
В этом диалоговом окне отображаются подтверждения, выводимые ESET Security Ultimate перед выполнением какого-либо действия. Установите или снимите флажок рядом с каждым типом подтверждения, чтобы включить или отключить его.

Дополнительные сведения о функциях, связанных с подтверждениями:

- Запрашивать подтверждение перед удалением журналов ESET SysInspector
- Запрашивать подтверждение перед удалением всех журналов ESET SysInspector
- Запрашивать подтверждение перед удалением объекта из карантина
- Запрашивать подтверждение перед отменой настроек в разделе "Дополнительные настройки"
- Запрашивать подтверждение, если решено не удалять все найденные угрозы в окне предупреждения
- Запрашивать подтверждение перед удалением записи из журнала
- Запрашивать подтверждение перед удалением запланированной в планировщике задачи
- Запрашивать подтверждение перед удалением всех записей из журнала
- Запрашивать подтверждение перед сбросом статистики
- Запрашивать подтверждение перед восстановлением объекта из карантина
- Запрашивать подтверждение перед восстановлением объектов из карантина и исключением их из сканирования
- Запрашивать подтверждение перед запуском запланированной в планировщике задачи
- Показывать оповещения о результатах работы модуля защиты от спама
- Показывать оповещения о результатах работы модуля защиты от спама для почтовых клиентов
- Показывать диалоговые окна подтверждения продукта для почтовых клиентов Outlook Express и Windows Mail
- Показывать диалоговые окна подтверждения продукта для Windows Live Mail
- Показывать диалоговые окна подтверждения продукта для почтового клиента Outlook

Переадресация

ESET Security Ultimate поддерживает отправку сообщений электронной почты при возникновении событий с заданной степенью детализации. Чтобы активировать эту функцию, откройте Расширенные параметры > **Уведомления** > **Переадресация** и включите параметр **Пересылать уведомления на электронную почту**.



В раскрывающемся списке **Минимальная степень детализации уведомлений** можно выбрать начальный уровень отправляемых уведомлений.

- **Диагностика**: в журнал вносится информация, необходимая для тщательной настройки программы, и все перечисленные выше записи.
- **Информационные**: записываются информационные сообщения, такие как нестандартные сетевые события, включая сообщения об успешной операции обновления, а также все перечисленные выше записи.
- **Предупреждения**: в журнал вносится информация обо всех критических ошибках и предупреждениях (например, о невыполненном обновлении).
- **Ошибки**: записываются ошибки (не активирована защита документов) и критические ошибки.
- **Критические ошибки**: запись в журнал только сведений о критических ошибках (например, об ошибках при запуске защиты от вирусов или об обнаружении угроз).

Отправлять уведомления в отдельных сообщениях электронной почты: если этот параметр активирован, получатель будет получать каждое уведомление в сообщении. Это может привести к получению большого количества почты за короткий промежуток времени.

Интервал между отправками новых сообщений электронной почты (мин.): время в минутах, через которое по электронной почте будут отправлены новые уведомления. Если задать значение 0, уведомления будут отправляться сразу.

Адрес отправителя: выбор адреса отправителя, который будет отображаться в заголовке сообщений электронной почты с уведомлением.

Адреса получателя: указание адресов получателей, которые будут отображаться в заголовке сообщений электронной почты с уведомлением. Можно указать несколько адресов. В качестве разделителя используйте точку с запятой.

SMTP сервер

SMTP-сервер: SMTP-сервер, используемый для отправки уведомлений (например, smtp.provider.com:587, предварительно заданный номер порта — 25).

ESET Security Ultimate поддерживает SMTP-серверы, использующие шифрование TLS.

Имя пользователя и **пароль**: если на SMTP-сервере требуется проверка подлинности, укажите действительные имя пользователя и пароль для доступа к SMTP серверу.

Включить шифрование TLS: предупреждения об угрозе и уведомления с использованием шифрования TLS.

Проверить SMTP-соединение: на адрес электронной почты получателя будет отправлено письмо для проверки. Нужно указать SMTP-сервер, имя пользователя, пароль, адрес отправителя и адрес получателя.

Формат сообщений

Обмен данными между программой и удаленным пользователем или системным администратором осуществляется посредством электронной почты или сообщений в локальной сети (используется служба обмена сообщениями Windows). **Формат предупреждений и уведомлений**, установленный по умолчанию, будет оптимален в большинстве случаев. В некоторых случаях может понадобиться изменить формат сообщений о событиях.

Формат сообщений о событиях: формат сообщений о событиях, отображаемых на удаленных компьютерах.

Формат предупреждений об угрозах: предупреждения об угрозе и уведомления имеют предварительно заданный формат по умолчанию. Рекомендуем оставить предварительно заданный формат. Однако в некоторых случаях (например, при наличии системы автоматизированной обработки электронной почты) может понадобиться изменить формат сообщений.

Кодировка: преобразование сообщения электронной почты в кодировку символов ANSI, основанную на региональных настройках Windows (например, windows-1250, Unicode (UTF-8), ACSII 7-bit, или японский (ISO-2022-JP)). В результате, "á" будет изменен на "a", а неизвестный символ на "?".

Использовать кодировку Quoted-printable: сообщение будет преобразовано в формат Quoted Printable ((QP)), в котором используются символы ASCII, что позволяет правильно передавать символы национальных алфавитов по электронной почте в 8-битном формате (áéíóú).

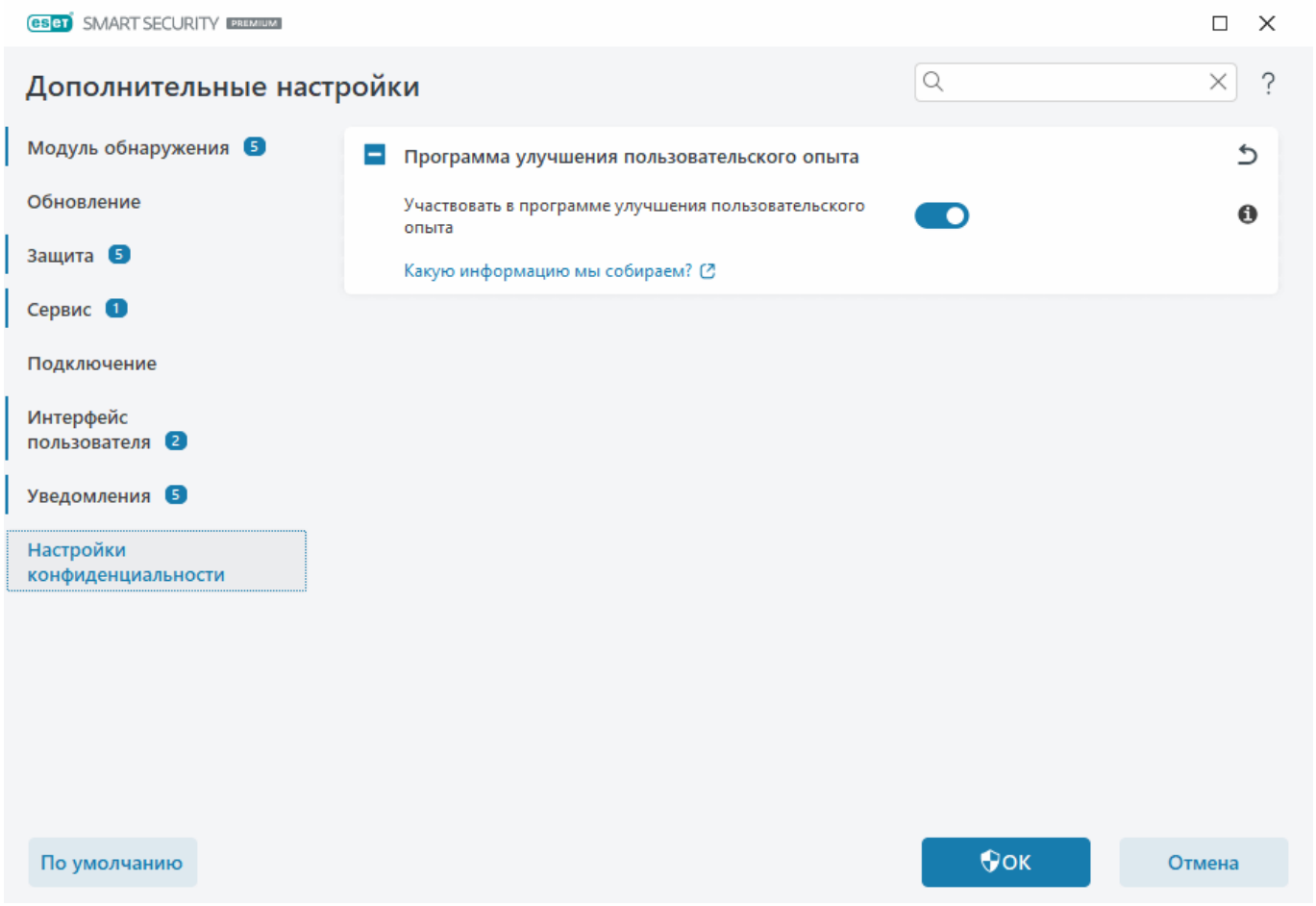
- **%TimeStamp%** — дата и время события.
- **%Scanner%** — задействованный модуль.

- **%ComputerName%** — имя компьютера, на котором появилось оповещение.
- **%ProgramName%** — программа, создавшая оповещение.
- **%InfectedObject%** — имя зараженного файла, сообщения и т. п.
- **%VirusName%** — идентифицирующие данные заражения.
- **%Action%** — действие, предпринимаемое в случае заражения.
- **%ErrorDescription%** — описание события, не имеющего отношения к вирусам.

Ключевые слова **%InfectedObject%** и **%VirusName%** используются только в предупреждениях об угрозах, а **%ErrorDescription%** — только в сообщениях о событиях.

Настройки конфиденциальности

Откройте Расширенные параметры > **Настройки конфиденциальности**.



Программа улучшения пользовательского опыта

Включите ползунок рядом с элементом **Участвовать в программе улучшения пользовательского опыта**, чтобы присоединиться к данной программе. Присоединившись, вы будете предоставлять компании ESET анонимные сведения об использовании наших продуктов. Собранные данные помогут нам улучшить удобство использования программы и ни в коем

случае не будут передаваться третьим сторонам. Какие сведения мы собираем?

Восстановление параметров по умолчанию

Нажмите **По умолчанию** в расширенных параметрах, чтобы скинуть все настройки программы для всех модулей. Они вернутся к состоянию после новой установки.

См. также Параметры импорта и экспорта.

Восстановление всех параметров в этом разделе

Нажмите на стрелку с изгибом , чтобы скинуть все настройки в этом разделе до настроек по умолчанию, определенных ESET.

Обратите внимание, что после нажатия **Вернуть значения по умолчанию** все созданные изменения будут потеряны.

Восстановить содержимое таблиц: при активации этой функции все правила, задачи и профили, добавленные автоматически или вручную, будут удалены.

См. также Параметры импорта и экспорта.

При сохранении конфигурации произошла ошибка

Это сообщение об ошибке показывает, что настройки не были корректно сохранены из-за ошибки.

Обычно это означает, что пользователь, пытавшийся изменить параметры программы:

• имеет недостаточно прав доступа или не имеет необходимых разрешений операционной системы, необходимых для изменения файлов конфигурации и системного реестра.
> Для внесения необходимых изменений системный администратор должен авторизоваться.

• недавно включил режим «Обучение» в системе HIPS или файерволе и попытался внести изменения в расширенные параметры.
> Чтобы сохранить конфигурацию и избежать конфликта конфигурации, закройте расширенные параметры без сохранения и повторите попытку внести необходимые изменения.

Второй наиболее распространенной причиной может быть неправильная работа программы, ее повреждение и, соответственно, необходимость переустановки.

Сканер командной строки

Модуль защиты от вирусов ESET Security Ultimate может быть запущен из командной строки вручную (с помощью команды ecls) или в пакетном режиме (с помощью bat-файла).

Использование модуля сканирования ESET для командной строки:

```
ecls [OPTIONS..] FILES..
```

Следующие параметры и аргументы могут использоваться при запуске сканера по требованию из командной строки.

Параметры

/base-dir=ПАПКА	загрузить модули из ПАПКИ
/quar-dir=ПАПКА	ПАПКА карантина
/exclude=МАСКА	исключить из сканирования файлы, соответствующие МАСКЕ
/subdir	сканировать вложенные папки (по умолчанию)
/no-subdir	не сканировать вложенные папки
/max-subdir-level=УРОВЕНЬ	максимальная степень вложенности папок для сканирования
/symlink	следовать по символическим ссылкам (по умолчанию)
/no-symlink	пропускать символические ссылки
/ads	сканировать ADS (по умолчанию)
/no-ads	не сканировать ADS
/log-file=ФАЙЛ	вывод журнала в ФАЙЛ
/log-rewrite	перезаписывать выходной файл (по умолчанию — добавлять)
/log-console	вывод журнала в окно консоли (по умолчанию)
/no-log-console	не выводить журнал в консоль
/log-all	регистрировать также незараженные файлы
/no-log-all	не регистрировать незараженные файлы (по умолчанию)
/aind	показывать индикатор работы
/auto	сканирование и автоматическая очистка всех локальных дисков

Параметры модуля сканирования

/files	сканировать файлы (по умолчанию)
/no-files	не сканировать файлы
/memory	сканировать память
/boots	сканировать загрузочные секторы
/no-boots	не сканировать загрузочные секторы (по умолчанию)
/arch	сканировать архивы (по умолчанию)
/no-arch	не сканировать архивы

/max-obj-size=РАЗМЕР	сканировать файлы, только если их размер не превышает РАЗМЕР в мегабайтах (по умолчанию 0 = без ограничений)
/max-arch-level=УРОВЕНЬ	максимальная степень вложенности архивов для сканирования
/scan-timeout=ПРЕДЕЛ	сканировать архивы не более указанного в ОГРАНИЧЕНИИ количества секунд
/max-arch-size=РАЗМЕР	сканировать файлы в архивах, только если их размер не превышает РАЗМЕР (по умолчанию 0 = без ограничений)
/max-sfx-size=РАЗМЕР	сканировать файлы в самораспаковывающихся архивах, только если их размер не превышает РАЗМЕР в мегабайтах (по умолчанию 0 = без ограничений)
/mail	сканировать файлы электронной почты (по умолчанию)
/no-mail	не сканировать файлы электронной почты
/mailbox	сканировать почтовые ящики (по умолчанию)
/no-mailbox	не сканировать почтовые ящики
/sfx	сканировать самораспаковывающиеся архивы (по умолчанию)
/no-sfx	не сканировать самораспаковывающиеся архивы
/rtp	сканировать упаковщики (по умолчанию)
/no-rtp	не сканировать упаковщики
/unsafe	сканировать на наличие потенциально опасных приложений
/no-unsafe	не сканировать на наличие потенциально опасных приложений (по умолчанию)
/unwanted	сканировать на наличие потенциально нежелательных приложений
/no-unwanted	не сканировать на наличие потенциально нежелательных приложений (по умолчанию)
/suspicious	сканировать на наличие подозрительных приложений (по умолчанию)
/no-suspicious	не сканировать на наличие подозрительных приложений
/pattern	использовать сигнатуры (по умолчанию)
/no-pattern	не использовать сигнатуры
/heur	включить эвристический анализ (по умолчанию)
/no-heur	отключить эвристический анализ
/adv-heur	включить расширенную эвристику (по умолчанию)
/no-adv-heur	отключить расширенную эвристику
/ext-exclude=РАСШИРЕНИЯ	исключить из сканирования РАСШИРЕНИЯ файлов, разделенные двоеточием

/clean-mode=РЕЖИМ	использовать РЕЖИМ очистки для зараженных объектов. Доступны следующие варианты: • none (по умолчанию) автоматическая очистка не выполняется. • standard — Приложение ecls.exe попытается автоматически очистить или удалить зараженные файлы. • Тщательная: приложение ecls.exe попытается автоматически очистить или удалить зараженные файлы без вмешательства пользователя (вам не будет предложено подтвердить удаление файлов). • Наиболее тщательная: приложение ecls.exe удалит все файлы без проведения очистки независимо от их типа. • Удаление: приложение ecls.exe удалит без проведения очистки все файлы, кроме важных, таких как системные файлы Windows.
/quarantine	копировать зараженные файлы, если они очищены, в карантин (дополнительно к действию, выполняемому при очистке)
/no-quarantine	не копировать зараженные файлы в карантин

Общие параметры

/help	показать справку и выйти
/version	показать сведения о версии и выйти
/preserve-time	сохранить последнюю отметку о времени доступа

Коды завершения

0	угроз не обнаружено
1	угроза обнаружена и очищена
10	некоторые файлы не удалось просканировать (могут быть угрозами)
50	угроза найдена
100	ошибка

Значение кода завершения больше 100 означает, что файл не был просканирован и может быть заражен.

Вопросы и ответы

Ниже вы можете найти некоторые из наиболее часто задаваемых вопросов и возникающих проблем. Нажмите ссылку, описывающую вашу проблему.

- Выполнение обновления ESET Security Ultimate
- Решение ESET Security Ultimate обнаружило угрозу
- Удаление вируса с компьютера
- Разрешение обмена данными определенному приложению
- Включение родительского контроля для учетной записи

- Создание задачи в планировщике
- Планирование задачи сканирования (еженедельно)
- Разблокировка дополнительных настроек
- Решение проблемы деактивации продукта с помощью ESET HOME

Если вашей проблемы нет в приведенном выше списке, попробуйте выполнить поиск в интерактивной справке ESET Security Ultimate.

Если не удается найти решение вашей проблемы/вопроса в интерактивной справке ESET Security Ultimate, посетите нашу регулярно обновляемую интерактивную базу знаний ESET. Ссылки на самые популярные статьи нашей базы знаний приведены ниже:

- Как продлить подписку?
- Во время установки программы ESET появилось сообщение об ошибке. Что это означает?
- Активация Windows-продукта ESET для домашнего использования с помощью ключа активации
- Удаление или повторная установка моего продукта ESET для дома.
- Во время установки программы ESET появилось сообщение, что установка преждевременно завершена.
- Что делать после обновления подписки? (пользователи домашней версии)
- Что делать, если мой адрес электронной почты изменится?
- Перенос продукта ESET на новый компьютер или устройство
- Запуск Windows в безопасном режиме или в безопасном режиме с поддержкой сети
- Исключение безопасного веб-сайта из блокировки
- Разрешить доступ средств чтения с экрана к графическому интерфейсу пользователя ESET

При необходимости с вопросами и проблемами можно обратиться в нашу службу технической поддержки.

Обновление ESET Security Ultimate

Обновлять ESET Security Ultimate можно вручную или автоматически. Чтобы запустить обновление, в главном окне программы выберите команду **Обновить**, а затем щелкните **Проверить наличие обновлений**.

При установке программы с параметрами по умолчанию создается задача автоматического обновления. Она запускается каждый час. Чтобы изменить интервал, последовательно выберите **Служебные программы** > Планировщик.

Удаление вируса с компьютера

Если компьютер проявляет какие-либо признаки заражения вредоносной программой, например работает медленнее или часто зависает, рекомендуется сделать следующее.

1. В главном окне программы щелкните **Сканирование компьютера**.

2. Щелкните элемент **Сканировать компьютер**, чтобы запустить сканирование компьютера.

3. После завершения сканирования просмотрите журнал на предмет количества проверенных, зараженных и очищенных файлов.

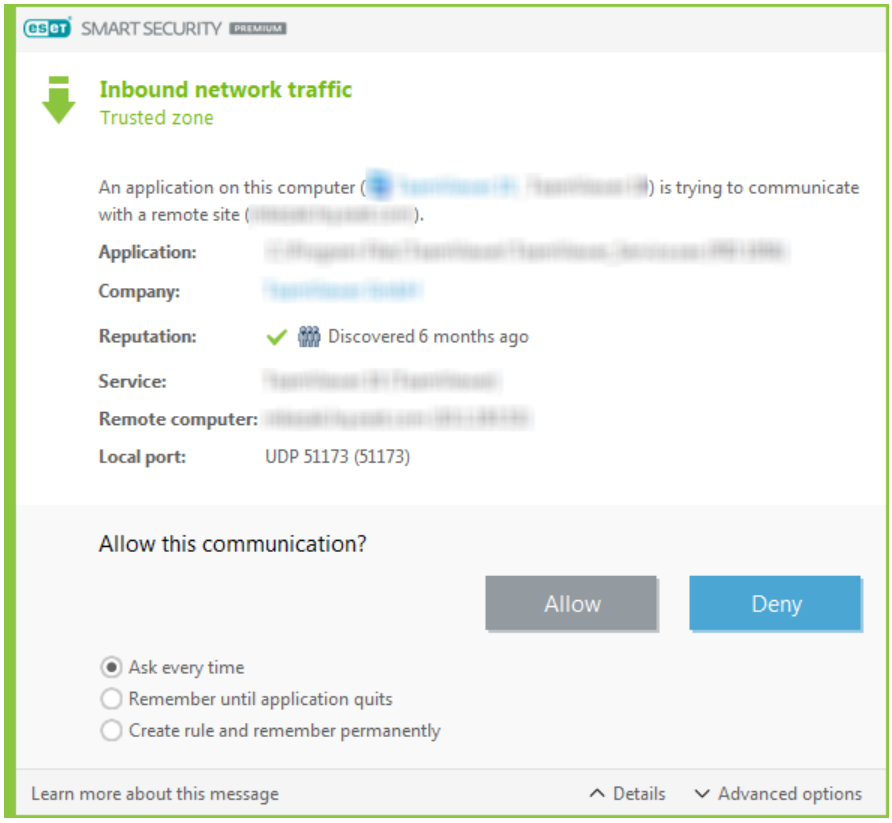
4. Если нужно просканировать только определенную часть диска, выберите вариант **Выборочное сканирование** и укажите объекты, которые нужно просканировать на наличие вирусов.

Для получения дополнительных сведений см.:

- Статья в базе знаний ESET
- Карантин

Разрешение обмена данными определенному приложению

Если в интерактивном режиме обнаруживается новое подключение, но соответствующего правила не найдено, пользователь получает запрос, предлагающий **разрешить** или **запретить** его. Если нужно, чтобы программа ESET Security Ultimate выполняла одно и то же действие при каждой попытке приложения установить подключение, установите флажок **Создать правило и запомнить навсегда**.



В настройках файервола можно создать новые правила файервола для приложений еще до их обнаружения программой ESET Security Ultimate. Откройте главное окно программы и выберите **Настройка** > **Защита сети** > щелкните значок ⚙ рядом с элементом **Файервол** > **Настроить** > **Дополнительно** > **Правила** > **Изменить**.

Нажмите кнопку **Добавить** и на вкладке **Общие** укажите имя, направление и протокол передачи данных для правила. В этом окне можно определить действие, которое нужно выполнить при применении правила.

Введите путь к исполняемому файлу приложения и порт передачи данных на локальном компьютере на вкладке **Локальный компьютер**. Перейдите на вкладку **Удаленный компьютер** и введите удаленный адрес и порт (при необходимости). Новое правило начнет действовать немедленно и сработает сразу, как только данное приложение попытается установить подключение.

Включение родительского контроля для учетной записи

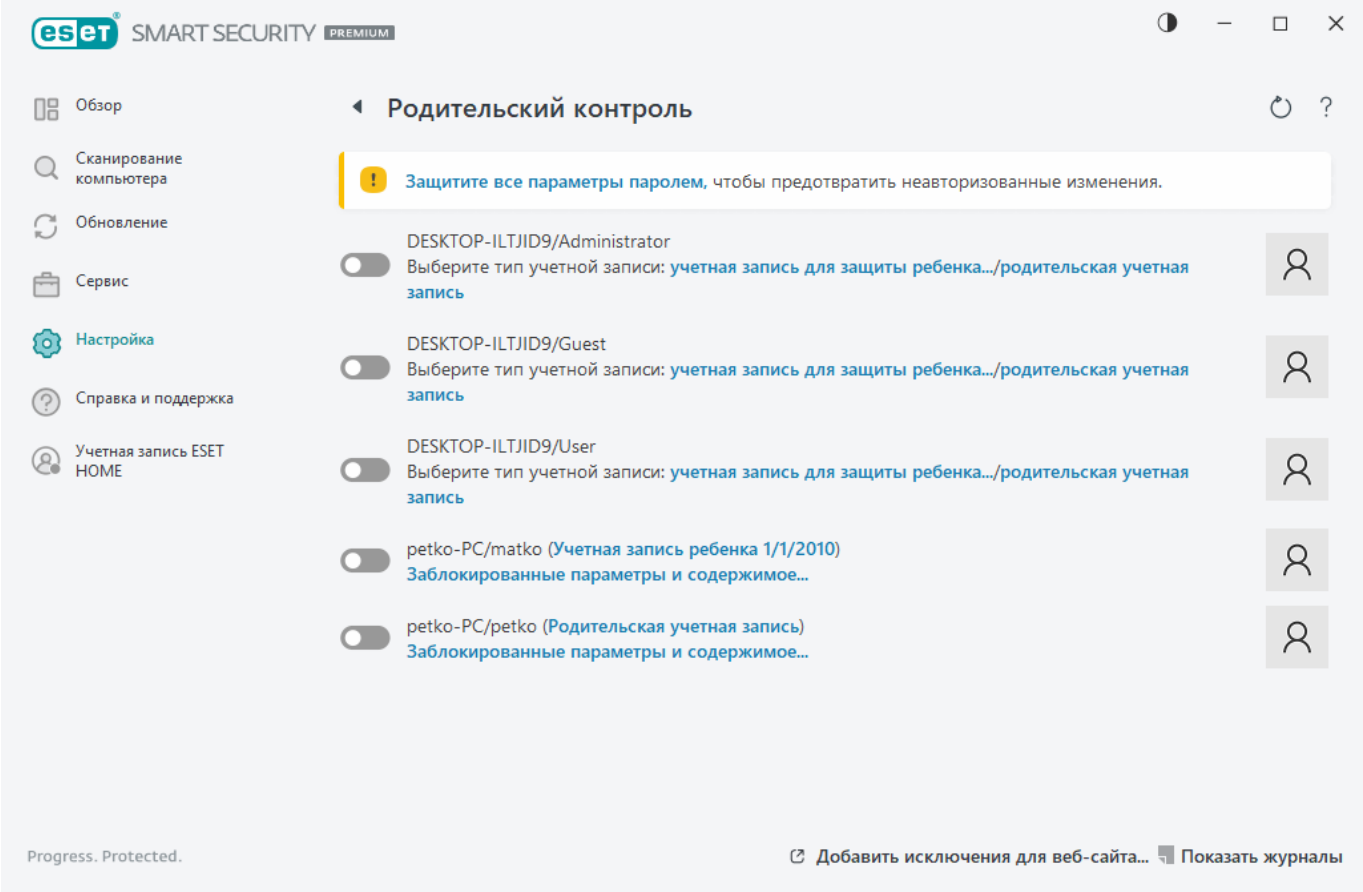
Чтобы активировать родительский контроль для определенной учетной записи пользователя, выполните следующие действия.

1. По умолчанию родительский контроль в программе ESET Security Ultimate отключен. Существует два способа активации родительского контроля.

   • В главном окне программы щелкните элемент и последовательно выберите элементы **Настройка** > **Защита интернета** > **Родительский контроль**, после чего включите функцию родительского контроля.

• Откройте раздел Расширенные параметры > **Защита** > **Защита доступа в Интернет** > **Родительский контроль**, а затем включите переключатель рядом с элементом **Включить родительский контроль**.

2. В главном окне программы выберите элементы **Настройка** > **Защита интернета** > **Родительский контроль**. Хотя для параметра **Родительский контроль** и отображается значение **Включено**, необходимо настроить родительский контроль для нужной учетной записи. Для этого щелкните значок стрелки, а в следующем окне выберите элемент **Защитить детскую учетную запись** или **Родительская учетная запись**. В следующем окне укажите дату рождения, чтобы определить уровень доступа и подходящие для этого возраста веб-страницы. Теперь родительский контроль включен для указанной учетной записи. Рядом с именем учетной записи щелкните элемент **Заблокированные параметры и содержимое**, чтобы задать категории, которые требуется разрешить или заблокировать, на вкладке Категории. Чтобы разрешить или заблокировать определенные веб-страницы, которые не соответствуют категории, откройте вкладку Исключения.



Создание задачи в планировщике

Чтобы создать новую задачу, выберите **Служебные программы** > **Планировщик**, а затем нажмите кнопку **Добавить задачу** или щелкните правой кнопкой мыши и в контекстном меню выберите команду **Добавить**. Доступно пять типов задач.

• **Запуск внешнего приложения**: планирование выполнения внешнего приложения.

• **Обслуживание журнала**: в файлах журнала также содержатся остатки удаленных записей. Эта задача регулярно оптимизирует записи в файлах журнала для эффективной работы.

• **Проверка файлов при загрузке системы**: проверка файлов, исполнение которых разрешено при запуске или входе пользователя в систему.

• **Создать снимок состояния компьютера**: создание снимка состояния компьютера в ESET SysInspector, для которого собираются подробные сведения о компонентах системы (например, драйверах, приложениях) и оценивается уровень риска для каждого их них.

• **Сканирование компьютера по требованию**: сканирование файлов и папок на компьютере.

• **Обновление**: планирование задачи обновления путем обновления модулей.

Поскольку **Обновление** - одна из самых часто используемых запланированных задач, ниже описан порядок добавления задачи обновления.

В раскрывающемся меню **Запланированная задача** выберите пункт **Обновление**. Введите имя задачи в поле **Имя задачи** и нажмите кнопку **Далее**. Выберите частоту выполнения задачи. Доступны следующие варианты: **Однократно**, **Многократно**, **Ежедневно**, **Еженедельно** и **При определенных условиях**. Установите флажок **Пропускать задачу, если устройство работает от аккумулятора**, чтобы свести к минимуму потребление системных ресурсов, когда ноутбук работает от аккумулятора. Задача будет выполняться в день и время, указанные в полях области **Выполнение задачи**. Затем укажите, какое действие следует предпринимать, если задача не может быть выполнена в установленное время. Доступны указанные ниже варианты.

• **В следующее запланированное время**

• **Как можно скорее**

• **Незамедлительно, если с момента последнего запуска прошло больше времени, чем указано** (интервал можно указать в поле **Время с момента последнего запуска (ч)**).

На следующем этапе отображается окно сводной информации о текущей планируемой задаче. После внесения всех необходимых изменений нажмите **Готово**.

На экран будет выведено диалоговое окно, в котором можно выбрать профили, используемые для запланированной задачи. Здесь можно задать основной и вспомогательный профили. Вспомогательный профиль используется, если задачу невозможно выполнить с применением основного профиля. Подтвердите внесенные изменения, нажав кнопку **Готово**, после чего новая задача появится в списке существующих запланированных задач.

Планирование еженедельного сканирования компьютера

Чтобы запланировать регулярную задачу, откройте главное окно программы и выберите **Сервис** > **Планировщик**. Ниже приведено краткое описание процедуры планирования задачи, предусматривающей сканирование локальных дисков каждую неделю. Подробные инструкции см. в статье нашей базы знаний.

Для того чтобы запланировать задачу сканирования, выполните следующие действия.

1. В главном окне планировщика нажмите **Добавить**.

2. Введите имя задачи и выберите **Сканирование компьютера по требованию** в раскрывающемся меню **Тип задачи**.

3. Для частоты выполнения задачи выберите **Еженедельно**.

4. Задайте день и время выполнения задачи.

5. Выберите установку **Выполнить задачу как можно скорее**, чтобы выполнить задачу позже, в случае если запланированное выполнение задачи не запустится по какой-либо причине (например, если компьютер выключен).

6. Просмотрите сводную информацию о запланированной задаче и нажмите **Готово**.

7. В раскрывающемся меню **Объекты** выберите пункт **Жесткие диски**.

8. Нажмите кнопку **Готово** для применения задачи.

Разблокировка дополнительных настроек, защищенных паролем

Когда вы хотите получить доступ к защищенным расширенным параметрам, открывается окно для ввода пароля. Если вы забудете или потеряете свой пароль, щелкните **Восстановить пароль** и введите адрес электронной почты, указанный при регистрации подписки. ESET отправит вам сообщение электронной почты с кодом проверки. Введите этот код, а затем укажите новый пароль и подтвердите его. Код проверки действителен в течение семи дней.

Восстановление пароля с помощью учетной записи ESET HOME: выберите этот параметр, если подписка, использованная для активации, связана с вашей учетной записью ESET HOME. Введите адрес электронной почты, который вы используете для авторизации в своей учетной записи ESET HOME.

Если вы не помните свой адрес электронной почты или у вас возникли трудности с восстановлением пароля, щелкните **Обратиться в службу технической поддержки**. Вы будете перенаправлены на веб-сайт ESET, где сможете связаться с нашей службой технической поддержки.

Создать код для службы технической поддержки: с помощью этого параметра можно создать код для службы технической поддержки. Скопируйте код, предоставленный службой технической поддержки, и щелкните **У меня есть код проверки**. Введите код проверки, а затем укажите новый пароль и подтвердите его. Код проверки действителен в течение семи дней.

Для получения дополнительных сведений см. раздел Разблокировка пароля для настроек в Windows-продуктах ESET для домашнего использования.

Решение проблемы деактивации продукта с помощью ESET HOME

Программа не активирована

Это сообщение об ошибке появляется, когда владелец подписки деактивирует ваш продукт ESET Security Ultimate на портале ESET HOME или когда пропадает общий доступ к подписке, которая была доступна для вашей учетной записи ESET HOME. Чтобы решить эту проблему, выполните следующие действия.

• Щелкните **Активировать** и воспользуйтесь одним из методов активации, чтобы активировать ESET Security Ultimate.

• Обратитесь к владельцу подписки и сообщите ему о том, что он деактивировал ваш продукт ESET Security Ultimate или вы утратили общий доступ к подписке. Владелец может решить эту проблему на ESET HOME.

Продукт деактивирован, устройство отключено

Это сообщение об ошибке появляется после удаления устройства с ESET HOME. Чтобы решить эту проблему, выполните следующие действия.

• Щелкните **Активировать** и воспользуйтесь одним из методов активации, чтобы активировать ESET Security Ultimate.

• Свяжитесь с владельцем подписки и сообщите ему о том, что ваш продукт ESET Security Ultimate деактивирован, а устройство отключено от ESET HOME.

• Если вы владелец подписки и не знаете об этих изменениях, просмотрите канал действий ESET HOME. При обнаружении подозрительных действий измените пароль учетной записи ESET HOME и обратитесь в службу технической поддержки ESET.

Продукт деактивирован, устройство отключено

Это сообщение об ошибке появляется после удаления устройства с ESET HOME. Чтобы решить эту проблему, выполните следующие действия.

• Щелкните **Активировать** и воспользуйтесь одним из методов активации, чтобы активировать ESET Security Ultimate.

• Свяжитесь с владельцем подписки и сообщите ему о том, что ваш продукт ESET Security Ultimate деактивирован, а устройство отключено от ESET HOME.

• Если вы владелец подписки и не знаете об этих изменениях, просмотрите канал действий ESET HOME. При обнаружении подозрительных действий измените пароль учетной записи ESET HOME и обратитесь в службу технической поддержки ESET.

Программа не активирована

Это сообщение об ошибке появляется, когда владелец подписки деактивирует ваш продукт ESET Security Ultimate на портале ESET HOME или когда пропадает общий доступ к подписке, которая была доступна для вашей учетной записи ESET HOME. Чтобы решить эту проблему, выполните следующие действия.

• Щелкните **Активировать** и воспользуйтесь одним из методов активации, чтобы активировать ESET Security Ultimate.

• Обратитесь к владельцу подписки и сообщите ему о том, что он деактивировал ваш продукт ESET Security Ultimate или вы утратили общий доступ к подписке. Владелец может решить эту проблему на ESET HOME.

0

Программа улучшения пользовательского опыта

Присоединившись к программе улучшения пользовательского опыта, вы предоставляете компании ESET анонимные сведения об использовании наших продуктов. Дополнительные сведения об обработке данных доступны в нашей политике конфиденциальности.

Ваше согласие

Участие в программе является добровольным и зависит от вашего согласия. После присоединения вы пассивно участвуете в программе, то есть вам не нужно предпринимать каких-либо дальнейших действий. В любой момент вы можете отозвать свое согласие, изменив настройки продукта. Сделав так, вы запретите нам обрабатывать ваши анонимные данные.

В любой момент вы можете отозвать свое согласие, изменив настройки продукта:

- Изменение параметров программы улучшения пользовательского опыта в продуктах ESET для Windows для домашнего использования

Какие виды информации мы собираем?

Данные о взаимодействии с продуктом

Эти сведения показывают нам, как используются наши продукты. Благодаря этому мы знаем, например, какие функции используются часто, какие настройки пользователи изменяют и сколько времени они тратят на использование продукта.

Данные об устройствах

Мы собираем эти сведения, чтобы понять, где и на каких устройствах используются наши продукты. Типичные примеры таких сведений: модель устройства, страна, версия и имя операционной системы.

Данные диагностики ошибок

Собираются также сведения о возникновении ошибок и аварийных ситуаций. Например, какая ошибка произошла, и какие действия привели к ней.

Почему мы собираем эту информацию?

Эти анонимные сведения дают нам возможность улучшать наши продукты для вас, наших пользователей. Они помогают избавить продукты от ошибок и сделать их максимально полезными и простыми в использовании.

Кто контролирует эту информацию?

Компания ESET, spol. s r.o. является единственным оператором данных, собираемых в рамках Программы. Эти сведения не передаются третьим лицам.

Лицензионное соглашение с конечным пользователем

Вступает в силу с 19 октября 2021 года.

ВАЖНО! Внимательно прочитайте изложенные далее условия использования программного продукта, прежде чем загружать, устанавливать, копировать или использовать его. **ЗАГРУЖАЯ, УСТАНАВЛИВАЯ, КОПИРУЯ ИЛИ ИСПОЛЬЗУЯ ЭТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, ВЫ ВЫРАЖАЕТЕ СВОЕ СОГЛАСИЕ С ИЗЛОЖЕННЫМИ УСЛОВИЯМИ И С ПОЛИТИКОЙ КОНФИДЕНЦИАЛЬНОСТИ.**

Лицезионное соглашение с конечным пользователем

Согласно условиям данного Лицензионного соглашения с конечным пользователем («Соглашение»), заключенного компанией ESET, spol. s r. o., зарегистрированной по адресу Einsteinova 24, 85101 Bratislava, Slovak Republic, внесенной в коммерческий регистр окружного суда Bratislava I, раздел Sro, запись № 3586/B, BIN 31333532 (ESET или Поставщик) и вами, физическим или юридическим лицом (Вы или Конечный пользователь), Вы получаете право использовать Программное обеспечение, указанное в статье 1 настоящего Соглашения. Программное обеспечение, указанное в статье 1 настоящего Соглашения, может храниться на носителях данных, отправляться по электронной почте, загружаться через Интернет, загружаться с серверов Поставщика или получаться из других источников, которые удовлетворяют перечисленным ниже условиям.

ЭТО СОГЛАШЕНИЕ КАСАЕТСЯ ПРАВ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ И НЕ ЯВЛЯЕТСЯ ДОГОВОРОМ ПРОДАЖИ. Поставщик остается владельцем экземпляра Программного обеспечения и материального носителя, на котором Программное обеспечение было поставлено в торговой упаковке, а также всех копий Программного обеспечения, на которые Конечный пользователь имеет право в соответствии с настоящим Соглашением.

Выбор варианта «Принимаю» в процессе установки, загрузки, копирования или использования этого Программного обеспечения выражает Ваше согласие с условиями настоящего Соглашения и Политики конфиденциальности. Если Вы не согласны с каким-либо из условий

настоящего Соглашения или Политики конфиденциальности, немедленно выберите вариант отмены, отмените установку или загрузку, уничтожьте или верните Программное обеспечение, установочные носители, сопроводительную документацию, а также квитанцию об оплате Поставщику или в организацию, в которой было приобретено Программное обеспечение.

ИСПОЛЬЗОВАНИЕ ВАМИ ЭТОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОЗНАЧАЕТ, ЧТО ВЫ ПРОЧЛИ ДАННОЕ СОГЛАШЕНИЕ, ПОНЯЛИ ЕГО ПОЛОЖЕНИЯ И СОГЛАСНЫ СЧИТАТЬ ИХ ОБЯЗЫВАЮЩИМИ.

1. **Программное обеспечение.** Термин "Программное обеспечение" в настоящем Соглашении означает: (i) компьютерную программу, которая сопровождается настоящим Соглашением, и все ее компоненты; (ii) все содержимое на дисках, компакт-дисках, DVD-дисках, в электронных сообщениях и каких-либо вложениях или на других носителях, которые были поставлены вместе с настоящим Соглашением, в том числе форму объектного кода Программного обеспечения, поставляемую на носителе данных, по электронной почте или загружаемую через Интернет; (iii) любые пояснительные материалы или любую другую возможную документацию, связанную с Программным обеспечением, главным образом какое-либо описание Программного обеспечения, его спецификации, какое-либо описание свойств или работы Программного обеспечения, какое-либо описание рабочей среды, в которой используется Программное обеспечение, инструкции по использованию или установке Программного обеспечения или какое-либо описание использования Программного обеспечения (Документация); (iv) копии Программного обеспечения, пакеты исправления возможных ошибок Программного обеспечения, дополнения к Программному обеспечению, расширения Программного обеспечения, измененные версии Программного обеспечения и обновления компонентов Программного обеспечения (при наличии), на которые Поставщик предоставил Вам лицензию в соответствии со статьей 3 настоящего Соглашения. Программное обеспечение предоставляется исключительно в форме исполняемого объектного кода.

2. **Установка, компьютер и лицензионный ключ**. Программное обеспечение, поставляемое на носителе данных, по электронной почте, загруженное через Интернет или с серверов Поставщика или полученное из других источников, подлежит установке. Установка Программного обеспечения должна происходить на должным образом настроенном компьютере, который отвечает минимальным требованиям, изложенным в Документации. Способ установки описан в Документации. Компьютер, на котором выполняется установка, не должен содержать программное или аппаратное обеспечение, которое может негативно повлиять на работу Программного обеспечения. Компьютер означает оборудование, в том числе, среди прочего, персональные компьютеры, ноутбуки, рабочие станции, карманные компьютеры, смартфоны, карманные или другие электронные устройства, для которых разрабатывается Программное обеспечение, на котором его будут устанавливать и/или использовать. Лицензионный ключ означает уникальную последовательность символов, букв, цифр или специальных знаков, предоставляемых конечному пользователю, чтобы разрешить законно использовать Программное обеспечение или его определенную версию либо продлить срок действия Лицензии в соответствии с настоящим Соглашением.

3. **Лицензия**. Если Вы приняли все условия, предусмотренные в настоящем Соглашении, и соблюдаете их, Поставщик предоставляет Вам следующие права (Лицензия).

a) **Установка и использование.** Вы получаете неисключительное не подлежащее передаче право установить Программное обеспечение на жесткий диск компьютера или иной носитель для хранения данных, установки и хранения Программного обеспечения в памяти компьютера, а также внедрить, хранить и отображать Программное обеспечение.

b) **Оговорка по количеству лицензий.** Право на использование Программного обеспечения

ограничено определенным количеством Конечных пользователей. Под одним Конечным пользователем подразумевается (i) установка Программного обеспечения на один компьютер или (ii) в случае ограничения лицензии количеством почтовых ящиков пользователь компьютера, который принимает электронную почту через пользовательский почтовый агент («Пользовательский почтовый агент»). Если Пользовательский почтовый агент принимает электронную почту, а затем автоматически распределяет ее среди нескольких пользователей, количество Конечных пользователей должно определяться в соответствии с фактическим количеством пользователей, получающих электронную почту. Если почтовый сервер выполняет функции почтового шлюза, количество Конечных пользователей будет равняться количеству пользователей почтового сервера, которых обслуживает этот шлюз. Если один пользователь владеет несколькими адресами электронной почты (например, при использовании псевдонимов) и принимает почту по ним, а почта не распределяется автоматически клиентом другим пользователям, необходима Лицензия только для одного компьютера. Одну Лицензию нельзя использовать одновременно на нескольких компьютерах. Конечный пользователь имеет право вводить Лицензионный ключ в Программное обеспечение только в той степени, в которой Конечный пользователь имеет право использовать Программное обеспечение в соответствии с ограничением по количеству Лицензий, выданных Поставщиком. Лицензионный ключ считается конфиденциальной информацией. Вы не должны передавать Лицензию третьим сторонам или разрешать третьим сторонам использовать Лицензионный ключ, если это не разрешено настоящим Соглашением или Поставщиком. Если Ваш Лицензионный ключ взломан, немедленно сообщите об этом Поставщику.

c) **Выпуск для дома или для бизнеса.** Версия Программного обеспечения для дома должна использоваться исключительно в личной и/или некоммерческой средах и предназначена только для домашнего и семейного использования. Для использования Программного обеспечения в коммерческих средах, а также на почтовых серверах, серверах ретрансляции электронной почты, почтовых шлюзах и шлюзах Интернета необходимо приобрести версию Программного обеспечения для бизнеса.

d) **Срок Лицензии.** Ваше право на использование Программного обеспечения ограничено определенным сроком.

e) **Программное обеспечение, получаемое через изготовителей комплектного оборудования.** Программное обеспечение, классифицированное как OEM (распространяется через изготовителей комплектного оборудования), можно использовать только на том компьютере, на котором оно было получено. Такое программное обеспечение нельзя перенести на другой компьютер.

f) **Не предназначенные для продажи и пробные версии Программного обеспечения.** Программное обеспечение, классифицированное как не предназначенная для продажи или пробная версия, не может быть связано с каким-либо платежом и должно использоваться исключительно для демонстрации или тестирования функций Программного обеспечения.

g) **Прекращение действия Лицензии.** Действие Лицензии прекращается автоматически по окончании периода, на который она была выдана. Если Вы нарушаете любое положение настоящего Соглашения, Поставщик получает право выйти из него, что никак не повлияет на его возможности воспользоваться любыми правами и средствами судебной защиты, доступными ему в таких обстоятельствах. В случае отмены Лицензии Вы обязаны незамедлительно за собственный счет удалить, уничтожить или вернуть Программное обеспечение и все его резервные копии в компанию ESET или в точку продажи, в которой оно было приобретено. В случае прекращения действия Лицензии Поставщик также имеет право запретить Конечному пользователю использовать функции Программного обеспечения,

которые требуют подключения к серверам Поставщика или серверам третьих лиц.

4. **Функции, для которых необходим сбор данных и подключение к Интернету.** Для корректной работы Программного обеспечения необходимо подключение к Интернету, поскольку Программное обеспечение должно регулярно подключаться к серверам Поставщика или третьих лиц, а также собирать соответствующие данные в соответствии с документом Политика конфиденциальности. Подключение к Интернету необходимо для использования перечисленных далее функций Программного обеспечения.

a) **Обновление Программного обеспечения.** Поставщик имеет право время от времени выпускать обновления Программного обеспечения (далее — «Обновления»), но не обязан их предоставлять. Эта функция включена при использовании стандартных параметров Программного обеспечения. Это значит, что Обновления устанавливаются автоматически, если Конечный пользователь не отключит их автоматическую установку. Для предоставления обновлений необходима проверка подлинности лицензии, включая информацию о компьютере и/или платформе, на которой установлено Программное обеспечение, в соответствии с Политикой конфиденциальности.

Предоставление любых Обновлений может регулироваться политикой в отношении окончания срока службы (далее — «Политика ОСС»), которая доступна по адресу https://go.eset.com/eol_home. После наступления даты окончания срока службы, которая устанавливается политикой ОСС для Программного обеспечения или какой-либо из его функций, Обновления предоставляться не будут.

b) **Отправка зараженных файлов и информации Поставщику.** Программное обеспечение оснащено функциями, которые собирают образцы компьютерных вирусов и других вредоносных программ, а также подозрительные, проблемные, потенциально нежелательные или потенциально опасные объекты, такие как файлы, URL-адреса, IP-пакеты и кадры Ethernet («Заражения»), и отправляют их Поставщику, в том числе, среди прочего, информацию о процессе установки, о Компьютере и/или платформе, на которых установлено Программное обеспечение, а также информацию об операциях и функциональности Программного обеспечения («Информация»). Информация и Заражения могут содержать данные (в том числе случайно или непредумышленно полученные персональные данные) о Конечном пользователе или других пользователях компьютера, на котором установлено Программное обеспечение, и о файлах, пораженных Заражениями с соответствующими метаданными.

Информацию и Заражения могут собирать следующие функции Программного обеспечения:

i. Функция LiveGrid Reputation System отвечает за сбор и отправку Поставщику в одном направлении хэшей, связанных с Заражениями. Эта функция включена при использовании стандартных параметров Программного обеспечения.

ii. Система обратной связи LiveGrid отвечает за сбор и отправку Поставщику Заражений со связанными метаданными и Информации. Конечный пользователь может активировать эту функцию в процессе установки Программного обеспечения.

Поставщик обязуется использовать полученные Заражения и Информацию только для анализа и исследования Заражений, улучшения Программного обеспечения и усовершенствования проверки подлинности Лицензии, а также принять необходимые меры предосторожности по сохранению конфиденциальности Информации и Заражений. Активируя эту функцию Программного обеспечения, Вы соглашаетесь на отправку Заражений и Информации Поставщику, а также даете ему необходимое разрешение, регулируемое соответствующими

правовыми нормами, на обработку полученной Информации. Данную функцию можно отключить в любой момент.

Для целей настоящего Соглашения необходимо собирать, обрабатывать и хранить данные, позволяющие Поставщику идентифицировать Вас в соответствии с документом Политика конфиденциальности. Настоящим Вы подтверждаете, что Поставщик с помощью своих средств может проверять, используете ли Вы Программное обеспечение в соответствии с положениями настоящего Соглашения. Вы соглашаетесь на передачу информации в процессе обмена данными между Программным обеспечением и компьютерными системами Поставщика или его коммерческих партнеров, входящих в сеть распространения и поддержки Поставщика, с целью обеспечения работы и проверки возможности использования Программного обеспечения и защиты прав Поставщика.

После заключения этого Соглашения Поставщик или любой из его коммерческих партнеров, входящих в сеть распространения и поддержки Поставщика, получат право передавать, обрабатывать и хранить важные данные, позволяющие идентифицировать Вашу личность, в целях оплаты и исполнения настоящего Соглашения, а также для отправки уведомлений на Ваш компьютер.

Сведения о конфиденциальности, защите персональных данных и Ваших правах как субъекта персональных данных приведены в Политике конфиденциальности, которая доступна на веб-сайте Поставщика, а также непосредственно в процессе установки. Вы также можете открыть ее из справки Программного обеспечения.

5. **Использование прав Конечного пользователя**. Права Конечного пользователя необходимо использовать лично, либо их могут использовать Ваши сотрудники. Вы имеете право на использование Программного обеспечения только для защиты своих действий и компьютеров или компьютерных систем, на которые приобретена Лицензия.

6. **Ограничения прав.** Не разрешается копировать, распространять Программное обеспечение, извлекать его компоненты и создавать производные работы на его основе. При использовании Программного обеспечения Вы обязаны соблюдать перечисленные далее ограничения.

a) Вы можете создать одну резервную копию Программного обеспечения на носителе постоянного хранения данных при условии, что эта резервная копия не установлена и не используется ни на каком компьютере. Создание любых иных копий Программного обеспечения является нарушением этого Соглашения.

b) Вы не должны использовать, изменять, переводить или воспроизводить Программное обеспечение и передавать права на использование Программного обеспечения или копии Программного обеспечения любым способом, отличным от описанного в настоящем Соглашении.

c) Вы не должны продавать, передавать на условиях сублицензии, сдавать в аренду или передавать во временное пользование Программное обеспечение, а также использовать Программное обеспечение для предоставления коммерческих услуг.

d) Запрещается вскрывать технологию, декомпилировать или разбирать код Программного обеспечения и иными способами пытаться получить исходный код Программного обеспечения за исключением того, в чем данное ограничение противоречит действующему законодательству.

e) Вы соглашаетесь использовать Программное обеспечение только способом, соответствующим всем действующим законодательным нормам страны, в которой используется Программное обеспечение, в том числе применимым ограничениям относительно авторского права, других прав на интеллектуальную собственность и так далее.

f) Вы соглашаетесь использовать Программное обеспечение и его функции только способом, который не ограничивает возможности доступа к этим услугам других Конечных пользователей. Поставщик оставляет за собой право ограничить объем услуг, предоставляемых отдельным Конечным пользователям, чтобы обеспечить использование услуг максимально возможным числом Конечных пользователей. Ограничение объема услуг должно также означать полное прекращение возможности использовать любую из функций Программного обеспечения, а также удаление Данных и информации на серверах Поставщика или сторонних серверах, относящихся к определенной функции Программного обеспечения.

g) Вы обязуетесь не предпринимать действий, связанных с использованием Лицензионного ключа, которые противоречат условиям настоящего Соглашения или приводят к предоставлению Лицензионного ключа лицу, не имеющему права использовать Программное обеспечение, например передачу использованного или неиспользованного Лицензионного ключа в любой форме, а также несанкционированное воспроизведение или распространение дублированных или сгенерированных лицензионных ключей или использование Программного обеспечения с помощью Лицензионного ключа, полученного не от Поставщика.

7. **Авторское право**. Программное обеспечение и все права на него, в том числе, среди прочего, право собственности и права на объекты интеллектуальной собственности, принадлежат компании ESET и/или ее лицензиарам. Эти права защищены международными соглашениями и всеми прочими применимыми законодательными нормами страны, в которой используется Программное обеспечение. Внутренняя структура, устройство и код Программного обеспечения являются ценной коммерческой тайной и конфиденциальной информацией, принадлежащими компании ESET и/или ее лицензиарам. Запрещается копировать Программное обеспечение кроме случаев, описанных в статье 6(a). Любые копии, которые разрешено создать в соответствии с Соглашением, должны содержать оригинальные отметки о защите авторских прав и другие уведомления о правах интеллектуальной собственности, которые присутствуют в самом Программном обеспечении. Если Вы вскрываете технологию, декомпилируете, разбираете исходный код Программного обеспечения или иным способом пытаетесь получить исходный код Программного обеспечения в нарушение положений этого Соглашения, любая полученная таким образом информация автоматически и безоговорочно должна считаться подлежащей передаче Поставщику и принадлежащей ему полностью с момента создания вне зависимости от прав Поставщика в отношении нарушения этого Соглашения.

8. **Сохранение прав**. Настоящим Поставщик сохраняет за собой все права на Программное обеспечение, за исключением прав, явно предоставленных Вам как Конечному пользователю Программного обеспечения в соответствии с условиями настоящего Соглашения.

9. **Несколько языковых версий, программное обеспечение на носителях двух типов, несколько копий**. Если Программное обеспечение поддерживает несколько платформ или языков или если Вы получили несколько экземпляров программного обеспечения, разрешается использовать Программное обеспечение только на том количестве компьютеров и в тех версиях, на которые была приобретена Лицензия. Запрещается продавать, передавать на условиях сублицензии, сдавать в аренду, передавать во временное или постоянное пользование версии или копии Программного обеспечения, которые не используются Вами.

10. **Момент вступления в силу и прекращение действия Соглашения.** Настоящее Соглашение вступает в законную силу с дня, когда Вы согласились с его условиями. Завершить действие Соглашения можно в любой момент, необратимо удалив, разрушив или вернув за свой счет Программное обеспечение, все резервные копии и любые относящиеся к нему материалы, предоставленные Поставщиком или одним из его коммерческих партнеров. Ваше право на использование Программного обеспечения и любых его функций может регулироваться политикой в отношении окончания срока службы. После наступления даты окончания срока службы, которая устанавливается политикой в отношении окончания срока службы для Программного обеспечения или какой-либо из его функций, ваше право на использование Программного обеспечения прекратится. Независимо от способа прекращения действия этого Соглашения положения статей 7, 8, 11, 13, 19 и 21 остаются действительными без ограничения по времени.

11. **ГАРАНТИИ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ**. ВЫСТУПАЯ В КАЧЕСТВЕ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ, ВЫ ПОДТВЕРЖДАЕТЕ СВОЮ ОСВЕДОМЛЕННОСТЬ В ТОМ, ЧТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПОСТАВЛЯЕТСЯ НА УСЛОВИЯХ «КАК ЕСТЬ» БЕЗ КАКИХ-ЛИБО ПРЯМЫХ ИЛИ ВМЕНЕННЫХ ГАРАНТИЙ ЛЮБОГО ТИПА, НАСКОЛЬКО ЭТО ПОЗВОЛЯЮТ СООТВЕТСТВУЮЩИЕ ЗАКОНОДАТЕЛЬНЫЕ НОРМЫ. НИ ПОСТАВЩИК, НИ ЕГО ПАРТНЕРЫ, ВЫСТУПАЮЩИЕ В КАЧЕСТВЕ ЛИЦЕНЗИАРОВ ИЛИ АФФИЛИРОВАННЫХ ЛИЦ, НИ ПРАВООБЛАДАТЕЛИ НЕ ДЕЛАЮТ НИКАКИХ ЗАЯВЛЕНИЙ И НЕ ПРЕДОСТАВЛЯЮТ НИКАКИХ ПРЯМЫХ ИЛИ ВМЕНЕННЫХ ОБЯЗАТЕЛЬСТВ ИЛИ ГАРАНТИЙ, В ЧАСТНОСТИ ГАРАНТИЙ ПРОДАЖ ИЛИ ГАРАНТИЙ ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННОГО ИСПОЛЬЗОВАНИЯ, А ТАКЖЕ ГАРАНТИЙ ТОГО, ЧТО ЭТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НЕ НАРУШАЕТ НИКАКИХ ПАТЕНТОВ, АВТОРСКИХ ПРАВ, ПРАВ НА ТОВАРНЫЕ ЗНАКИ И ДРУГИХ ПРАВ ТРЕТЬИХ ЛИЦ. ПОСТАВЩИК И ЛЮБЫЕ ДРУГИЕ ЛИЦА НЕ ГАРАНТИРУЮТ, ЧТО ФУНКЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ БУДУТ СООТВЕТСТВОВАТЬ ВАШИМ ТРЕБОВАНИЯМ ИЛИ ЧТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ БУДЕТ РАБОТАТЬ БЕЗ СБОЕВ И ОШИБОК. РИСК ПРИ ВЫБОРЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ДОСТИЖЕНИЯ НУЖНЫХ РЕЗУЛЬТАТОВ, А ТАКЖЕ ПРИ УСТАНОВКЕ, ИСПОЛЬЗОВАНИИ И ПОЛУЧЕНИИ РЕЗУЛЬТАТОВ, КОТОРЫХ ВЫ БУДЕТЕ ДОСТИГАТЬ С ПОМОЩЬЮ ЭТОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ЛЕЖИТ НА ВАС.

12. **Отказ от других обязательств**. Настоящее Соглашение не предусматривает никаких обязательств для Поставщика и его лицензиаров за исключением тех, которые изложены в настоящем Соглашении.

13. **ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ**. В ТОЙ СТЕПЕНИ, В КОТОРОЙ ЭТО РАЗРЕШЕНО ПРИМЕНИМЫМ ЗАКОНОДАТЕЛЬСТВОМ, НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ ПОСТАВЩИК, ЕГО СОТРУДНИКИ ИЛИ ЛИЦЕНЗИАРЫ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА КАКУЮ-ЛИБО УПУЩЕННУЮ ПРИБЫЛЬ, ВЫРУЧКУ, ПРОДАЖИ, ДАННЫЕ ИЛИ РАСХОДЫ НА ЗАКУПКУ ВЗАИМОЗАМЕНЯЕМЫХ ТОВАРОВ ИЛИ УСЛУГ, ПОВРЕЖДЕНИЕ ИМУЩЕСТВА, ТЕЛЕСНЫЕ ПОВРЕЖДЕНИЯ, ПРИОСТАНОВКУ РАБОТЫ, ПОТЕРЮ КОММЕРЧЕСКОЙ ИНФОРМАЦИИ ИЛИ ЗА КАКИЕ-ЛИБО ФАКТИЧЕСКИЕ, ПРЯМЫЕ, НЕПРЯМЫЕ, ПОБОЧНЫЕ, ЭКОНОМИЧЕСКИЕ, КОМПЕНСИРУЕМЫЕ, ШТРАФНЫЕ, КОСВЕННЫЕ ИЛИ ПРЕДСКАЗУЕМЫЕ КОСВЕННЫЕ УБЫТКИ, НАНЕСЕННЫЕ В РЕЗУЛЬТАТЕ ВЫПОЛНЕНИЯ СОГЛАШЕНИЯ, ГРАЖДАНСКОГО ПРАВОНАРУШЕНИЯ ИЛИ НЕБРЕЖНОСТИ, НЕЗАВИСИМО ОТ ПРИЧИНЫ И ВИДА ОТВЕТСТВЕННОСТИ, ВОЗНИКАЮЩИЕ В РЕЗУЛЬТАТЕ УСТАНОВКИ, ИСПОЛЬЗОВАНИЯ ИЛИ ОТСУТСТВИЯ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ДАЖЕ ЕСЛИ ПОСТАВЩИК, ЕГО ЛИЦЕНЗИАРЫ ИЛИ АФФИЛИРОВАННЫЕ ЛИЦА ОСВЕДОМЛЕНЫ О ВОЗМОЖНОСТИ ВОЗНИКНОВЕНИЯ ТАКОГО УЩЕРБА. ПОСКОЛЬКУ ЗАКОНОДАТЕЛЬСТВО НЕКОТОРЫХ СТРАН И ОТДЕЛЬНЫЕ ЗАКОНЫ НЕ РАЗРЕШАЮТ ИСКЛЮЧАТЬ ТАКУЮ ОТВЕТСТВЕННОСТЬ, НО ПОЗВОЛЯЮТ ОГРАНИЧИВАТЬ ЕЕ, В ТАКИХ СЛУЧАЯХ ОТВЕТСТВЕННОСТЬ ПОСТАВЩИКА, ЕГО СОТРУДНИКОВ, ЛИЦЕНЗИАРОВ ИЛИ АФФИЛИРОВАННЫХ ЛИЦ ОГРАНИЧИВАЕТСЯ СУММОЙ, ВЫПЛАЧЕННОЙ ВАМИ ЗА ЛИЦЕНЗИЮ.

14. Ни одно из положений настоящего Соглашения не затрагивает законные права любой стороны, выступающей в качестве потребителя, даже если они противоречат таким правам.

15. **Техническая поддержка**. ESET или привлеченные компанией ESET третьи лица предоставляют техническую поддержку по собственному усмотрению без каких-либо гарантий или заявлений. После наступления даты окончания срока службы, которая устанавливается политикой ОСС для Программного обеспечения или какой-либо из его функций, техническая поддержка предоставляться не будет. Конечный пользователь обязан создать резервную копию всех существующих данных, программного обеспечения или программных средств, прежде чем обратиться за технической поддержкой. ESET и (или) третьи лица, привлеченные ESET, не могут принять на себя ответственность за повреждение или потерю данных, собственности, программного обеспечения или оборудования, а также за упущенную прибыль, которые связаны с предоставлением технической поддержки. ESET и (или) привлеченные ESET третьи лица оставляют за собой право принять решение о том, что устранить конкретную проблему невозможно в рамках технической поддержки. ESET оставляет за собой право отказать в предоставлении технической поддержки, приостановить или прекратить ее оказание по своему собственному усмотрению. Сведения о лицензии, Информация и другие данные в соответствии с Политикой конфиденциальности могут потребоваться для предоставления технической поддержки.

16. **Передача лицензии**. Программное обеспечение может быть перенесено с одного компьютера на другой, если это не противоречит условиям настоящего Соглашения. Если это не противоречит условиям Соглашения, Конечный пользователь может только перманентно передать Лицензию и все права по настоящему Соглашению другому Конечному пользователю с согласия Поставщика, если соблюдаются следующие условия: (i) у первого Конечного пользователя не остается никаких экземпляров Программного обеспечения; (ii) передача прав должна быть непосредственной, т. е. от исходного Конечного пользователя к новому; (iii) новый Конечный пользователь должен принять все права и обязательства исходного Конечного пользователя по настоящему Соглашению; (iv) исходный Конечный пользователь должен предоставить новому Конечному пользователю документацию, позволяющую проверить подлинность Программного обеспечения в соответствии со статьей 17.

17. **Проверка подлинности Программного обеспечения.** Конечный пользователь может продемонстрировать наличие у него прав на использование Программного обеспечения одним из следующих способов: (i) с помощью лицензионного сертификата, выданного Поставщиком или третьим лицом, которое назначено Поставщиком; (ii) письменным лицензионным соглашением, если таковое было заключено; (iii) путем предоставления отправленного Поставщиком сообщения электронной почты, в котором содержатся сведения о лицензии (имя пользователя и пароль). Сведения о лицензии и идентификационные данные Конечного пользователя в соответствии с Политикой конфиденциальности могут потребоваться для проверки подлинности программного обеспечения.

18. **Предоставление лицензии органам власти и правительству США**. Программное обеспечение будет предоставлено органам власти, в том числе правительству Соединенных Штатов Америки, в соответствии с правами и ограничениями, описанными в настоящем Соглашении.

19. **Соответствие нормам регулирования внешней торговли**.

a) Вы не будете прямо или косвенно экспортировать, реэкспортировать, передавать или иным образом предоставлять Программное обеспечение кому-либо, а также не будете использовать его каким-либо образом либо иметь отношение к каким-либо действиям, в результате чего

компания ESET или ее холдинговые компании, ее филиалы, филиалы ее холдинговых компаний, прочие субъекты, находящиеся под управлением ее холдинговых компаний («Аффилированные лица»), может стать нарушителем Законодательства по регулированию внешней торговли либо получить негативные последствия в связи с его применением. К законодательству по регулированию внешней торговли относится:

i. Любое законодательство, которое предназначено для регулирования, ограничения или введения лицензионных требований в сфере экспорта, реэкспорта или передачи товаров, программного обеспечения, технологий, услуг и которое принимается любыми правительственными, государственными или регулятивными органами Соединенных Штатов Америки, Сингапура, Великобритании, Европейского Союза или любого входящего в него государства, а также любой страны, в которой должны выполняться обязательства согласно настоящему Соглашению или в которой зарегистрирована либо действует компания ESET или какие-либо ее Аффилированные лица

ii. Любые экономические, финансовые, торговые и прочие санкции, ограничения, эмбарго, запреты на импорт или экспорт, запреты на перевод денежных средств или активов либо на предоставление услуг, а также эквивалентные меры, которые вводятся в действие любыми правительственными, государственными или регулятивными органами Соединенных Штатов Америки, Сингапура, Великобритании, Европейского Союза или любого входящего в него государства, а также любой страны, в которой должны выполняться обязательства согласно настоящему Соглашению или в которой зарегистрирована либо действует компания ESET или какие-либо ее Аффилированные лица.

(Законодательные акты, упомянутые в пунктах i и ii выше, совместно именуются «Законодательство по регулированию внешней торговли».)

b) Компания ESET имеет право приостановить выполнение своих обязательств согласно настоящим Условиям либо незамедлительно прекратить действие настоящих Условий в следующих случаях:

i. В случае, если компания ESET устанавливает, что по ее обоснованному мнению Пользователь нарушил или может нарушить положения Статьи 19 a) настоящего Соглашения.

ii. В случае, если Конечный пользователь и/или Программное обеспечение попадут под действие Законодательства по регулированию внешней торговли, и, как результат, компания ESET установит, что по ее обоснованному мнению продолжение выполнения своих обязательств согласно настоящему Соглашению может привести к тому, что компания ESET или ее Аффилированные лица может стать нарушителем Законодательства по регулированию внешней торговли либо получить негативные последствия в связи с его применением.

c) Ни одна часть настоящего Соглашения не предназначена, не может интерпретироваться или истолковываться так, чтобы побуждать либо обязывать любую его сторону действовать или воздерживаться от действий (или согласиться действовать или воздерживаться от действий) каким-либо образом, который противоречит любому применимому Законодательству по регулированию внешней торговли, преследуется или запрещается им.

20. **Уведомления**. Все уведомления, возвращаемые Программное обеспечение и документация должны быть доставлены по адресу: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, что не ограничивает право ESET сообщать Вам о любых изменениях в настоящем Соглашении, политиках конфиденциальности, политике в отношении окончания срока службы и документации в соответствии со статьей 22 настоящего Соглашения. ESET может отправлять

Вам письма по электронной почте и уведомления в Программном обеспечении, а также публиковать сообщения на нашем веб-сайте. Вы соглашаетесь получать юридически значимые сообщения от компании ESET в электронной форме, в том числе любые сообщения об изменении Условий, Специальных условий или Политик конфиденциальности, любые предложения и принятие условий договоров, приглашения вести переговоры о заключении договора, уведомления или другие юридически значимые сообщения. Такие электронные сообщения считаются полученными в письменной форме, если только действующее законодательство не требует другого формата коммуникации.

21. **Применимое законодательство**. Данное Соглашение регулируется и толкуется в соответствии с законодательством Словацкой Республики. Конечный пользователь и Поставщик согласны, что принципы коллизионного права и Конвенция Организации Объединенных Наций о договорах международной купли-продажи товаров не применяются. Вы явным образом соглашаетесь с тем, что эксклюзивная юрисдикция по решению любых споров и вопросов с Поставщиком или относительно способа использования Программного обеспечения принадлежит окружному суду I в Братиславе.

22. **Общие положения**. Если любое положение настоящего Соглашения оказывается недействительным или невыполнимым, это не отражается на действительности остальных положений Соглашения, которые по-прежнему будут действительными и выполнимыми в соответствии с указанными здесь условиями. Настоящее Соглашение составлено на английском языке. В случае подготовки перевода настоящего Соглашения для удобства или любой иной цели либо при наличии любых расхождений между разными языковыми версиями настоящего Соглашения преимуществом обладает версия на английском языке.

Компания ESET оставляет за собой право вносить изменения в Программное обеспечение и пересматривать условия настоящего Соглашения, приложений и дополнений к нему, Политики конфиденциальности, Политики ОСС и документации или какой-либо их части в любое время путем обновления соответствующего документа (а) для отображения изменений в Программном обеспечении либо в способе осуществления деятельности компанией ESET, (б) для соблюдения нормативно-правовых норм или из соображений безопасности либо (в) для недопущения нарушений или нанесения вреда. В случае изменения настоящего Соглашения Вы будете уведомлены с помощью электронной почты, уведомления в приложении или другими электронными средствами. Если Вы не согласны с предлагаемыми изменениями к настоящему Соглашению, Вы можете расторгнуть его в соответствии со статьей 10 в течение 30 дней после получения уведомления об изменении. Если Вы не расторгнете настоящее Соглашение в течение этого срока, предлагаемые изменения будут считаться принятыми и вступят в силу в отношении Вас с даты получения Вами уведомления об изменении.

Это полное Соглашение между Поставщиком и Вами относительно использования Программного обеспечения, которое заменяет все предыдущие заверения, обсуждения, гарантии или уведомления или рекламные материалы в отношении Программного обеспечения.

ДОПОЛНЕНИЕ К СОГЛАШЕНИЮ

Оценка безопасности подключенных к сети устройств. В отношении оценки безопасности подключенных к сети устройств применяются следующие дополнительные положения.

Программное обеспечение оснащено функцией проверки безопасности локальной сети Конечного пользователя и безопасности устройств в ней, для которой требуются имя локальной сети и сведения об устройствах в ней, такие как присутствие, тип, имя, IP- и MAC-

адрес устройства в локальной сети в сочетании с информацией о лицензии. К информации также относятся тип безопасности беспроводной сети и тип шифрования в беспроводной сети для маршрутизаторов. Кроме того, эта функция может предоставлять сведения о наличии программы безопасности для защиты устройств в локальной сети.

Защита от неправильного использования данных. В отношении защиты от неправильного использования данных применяются следующие дополнительные положения.

Программное обеспечение включает в себя функцию, предотвращающую потерю или ненадлежащее использование важных данных в связи с кражей компьютера. Эта функция Программного обеспечения отключена по умолчанию. Для ее активации должна быть создана Учетная запись ESET HOME, с помощью которой функция активирует сбор данных в случае кражи компьютера. Если Вы активируете эту функцию Программного обеспечения, Вы соглашаетесь со сбором и отправкой Поставщику данных об украденном компьютере, которые могут включать в себя данные о сетевом расположении компьютера, данные о содержимом, которое отображается на экране компьютера, данные о конфигурации компьютера или данные, записанные подключенной к компьютеру камерой (далее — «Данные»). Конечный пользователь имеет право использовать Данные, полученные этой функцией и предоставленные с помощью учетной записи ESET HOME, исключительно для решения вопроса с кражей компьютера. Исключительно в целях работы данной функции Поставщик обрабатывает Данные согласно Политике конфиденциальности и соответствующим правовым нормам. Поставщик разрешает Конечному пользователю получать доступ к Данным в течение периода, необходимого для достижения цели, для которой Данные были получены. Однако такой период не может превышать срок хранения, указанный в Политике конфиденциальности. Функция защиты от ненадлежащего использования данных должна использоваться исключительно с компьютерами и учетными записями, к которым Конечный пользователь имеет законный доступ. Обо всех случаях ее незаконного использования будет сообщаться в компетентные органы. Поставщик обязуется соблюдать соответствующие законы и оказывать содействие правоохранительным органам в случае ненадлежащего использования. Вы подтверждаете и признаете, что вы несете ответственность за сохранность пароля для доступа к Учетной записи ESET HOME, и обязуетесь не разглашать свой пароль каким бы то ни было третьим лицам. Конечный пользователь несет ответственность за любые действия (разрешенные или нет), осуществляемые с использованием функции защиты от ненадлежащего использования данных и Учетной записи ESET HOME. Если Учетная запись ESET HOME взломана, следует немедленно уведомить Поставщика. Дополнительные положения по защите от неправильного использования данных применяются исключительно к Конечным пользователям ESET Internet Security и ESET Smart Security Premium.

ESET Secure Data. В отношении ESET Secure Data применяются следующие дополнительные положения.

1. Определения. В настоящих дополнительных положениях для ESET Secure Data указанные ниже слова имеют следующие значения.

a) «Информация»— любые сведения или данные, зашифрованные или расшифрованные с использованием программного обеспечения.

b) «Продукты»— программное обеспечение ESET Secure Data и соответствующая документация.

c) «ESET Secure Data»— программное обеспечение, используемое для шифрования и расшифровки электронных данных.

Все упоминания во множественном числе относятся также к единственному числу, а все упоминания в мужском роде также относятся к женскому и среднему родам и наоборот. Слова без определения следует использовать в соответствии с определениями, приведенными в Соглашении.

2. Дополнительные заверения конечного пользователя. Вы признаете и принимаете перечисленное далее.

a) Вы несете ответственность за обеспечение защиты, поддержки и резервного копирования информации.

b) Вы обязуетесь создать полную резервную копию всей информации и данных (в том числе, среди прочего, любой критически важной информации и данных) на Компьютере, прежде чем устанавливать программное обеспечение ESET Secure Data.

c) Вы обязуетесь хранить в безопасном месте все пароли и другие сведения, которые требуются для настройки и использования программы ESET Secure Data, а также обязуетесь создать на отдельном носителе данных резервные копии всех ключей шифрования, кодов лицензии, файлов ключей и других создаваемых данных.

d) Вы берете на себя ответственность за использование Продуктов. Поставщик не несет ответственности за любые убытки, ущерб или претензии, возникающие в результате любого несанкционированного или выполненного по ошибке шифрования либо расшифровки Информации или других данных, вне зависимости от места и условий хранения такой информации или других данных.

e) Невзирая на то, что Поставщиком приняты все обоснованные меры для обеспечения целостности и безопасности программы ESET Secure Data, Продукты (вместе или по отдельности) не должны использоваться в областях, требующих максимальной отказоустойчивости или являющихся потенциально опасными, в том числе, среди прочего, на атомных электростанциях, в системах аэронавигации, системах управления и коммуникаций, системах оборонно-промышленного комплекса, а также в системах поддержки жизнедеятельности и медицинского мониторинга.

f) Вы обязуетесь удостовериться, что обеспечиваемый продуктами уровень безопасности и шифрования соответствует Вашим требованиям.

g) Вы несете ответственность за использование Вами Продуктов (вместе или по отдельности), в том числе, среди прочего, Вы обязуетесь удостовериться, что такое использование осуществляется в рамках действующего законодательства и нормативно-правовых актов Словацкой Республики или другого государства, региона или штата, в котором используется Продукт. Перед любым использованием Продуктов Вы должны удостовериться, что такое использование не нарушает каких-либо правительственных запретов (на территории Словацкой Республики или другого государства).

h) программа ESET Secure Data может время от времени обращаться к серверам Поставщика в целях уточнения сведений о лицензии, а также для проверки на наличие исправлений, пакетов обновлений и прочих обновлений, которые могут использоваться для улучшения, поддержки, изменения или усовершенствования работы программы ESET Secure Data. Программа может отправлять общие сведения о компьютере, связанные с работой программы в соответствии с документом Политика конфиденциальности.

i) Поставщик не несет ответственности за какие-либо убытки, ущерб, затраты или претензии, возникающие в результате потери, кражи, ненадлежащего использования, повреждения или уничтожения паролей, информации о настройке, ключей шифрования, кодов активации лицензии и других данных, которые были созданы или сохранены в процессе использования программного обеспечения.

Дополнительные положения для ESET Secure Data применяются исключительно в отношении конечных пользователей программы ESET Smart Security Premium.

Password Manager Программное обеспечение. В отношении программы Password Manager применяются следующие дополнительные положения:

1. Дополнительные заверения конечного пользователя. Вы признаете и принимаете перечисленное далее.

a) применять программу Password Manager для использования каких-либо критически важных приложений, от которых зависит человеческая жизнь или имущество. Вы понимаете, что программа Password Manager не предназначена для таких целей, что в таких случаях сбой в работе программы может привести к смерти или травмированию человека или может причинить серьезный ущерб имуществу или окружающей среде и что Поставщик не несет ответственности за такие последствия.

ПРОГРАММА PASSWORD MANAGER НЕ РАССЧИТАНА, НЕ ПРЕДНАЗНАЧЕНА И НЕ ПРЕДОСТАВЛЯЕТСЯ НА ПРАВАХ ЛИЦЕНЗИИ ДЛЯ ИСПОЛЬЗОВАНИЯ В ОПАСНЫХ СРЕДАХ, ТРЕБУЮЩИХ НАЛИЧИЯ ОТКАЗОУСТОЙЧИВОЙ СИСТЕМЫ УПРАВЛЕНИЯ, В ТОМ ЧИСЛЕ, СРЕДИ ПРОЧЕГО, ДЛЯ ИСПОЛЬЗОВАНИЯ В СИСТЕМАХ ПРОЕКТИРОВАНИЯ, СТРОИТЕЛЬСТВА, ОБСЛУЖИВАНИЯ ИЛИ РАБОТЫ АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ, СИСТЕМАХ АЭРОНАВИГАЦИИ ИЛИ КОММУНИКАЦИЙ, АЭРОДИСПЕТЧЕРСКИХ СЛУЖБАХ, А ТАКЖЕ В СИСТЕМАХ ПОДДЕРЖКИ ЖИЗНЕДЕЯТЕЛЬНОСТИ И СИСТЕМАХ ОБОРОННО-ПРОМЫШЛЕННОГО КОМПЛЕКСА. ПОСТАВЩИК НАПРЯМУЮ ОТКАЗЫВАЕТСЯ ОТ КАКИХ БЫ ТО НИ БЫЛО ЯВНО ВЫРАЖЕННЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ В ОТНОШЕНИИ ПРИГОДНОСТИ ПРОДУКТОВ ДЛЯ ТАКИХ ЦЕЛЕЙ;

b) Использовать программу Password Manager таким способом, который нарушает условия настоящего Соглашения, законы Словацкой Республики или законы Вашей юрисдикции. В частности, запрещено использовать программу Password Manager для совершения незаконных действий или содействия им, в том числе выгружать данные вредоносного содержимого или содержимого, которое может использоваться для незаконных действий или каким бы то ни было образом нарушает закон или права какой-либо третьей стороны (в том числе какие-либо права на объекты интеллектуальной собственности), в том числе, среди прочего, запрещено осуществлять какие бы то ни было попытки получения доступа к учетным записям Хранилища (в настоящих дополнительных условиях для программы Password Manager термин «Хранилище» означает пространство хранения данных под управлением Поставщика или третьей стороны, не являющейся Поставщиком или пользователем, которое используется в целях синхронизации и резервного копирования пользовательских данных) либо к любым учетным записям или данным других пользователей программы Password Manager или Хранилища. В случае нарушения Вами каких-либо из указанных положений Поставщик имеет право незамедлительно расторгнуть настоящее Соглашение и предъявить Вам счет на оплату суммы понесенного ущерба, а также принять все необходимые меры, чтобы предотвратить дальнейшее использование Вами программы Password Manager без возможности возмещения расходов.

2. ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ. ПРОГРАММА PASSWORD MANAGER ПРЕДОСТАВЛЯЕТСЯ НА

УСЛОВИИ «КАК ЕСТЬ». НИКАКИЕ ЯВНО ВЫРАЖЕННЫЕ ИЛИ ПРЕДПОЛАГАЕМЫЕ ГАРАНТИИ НЕ ПРЕДОСТАВЛЯЮТСЯ. ВЫ ПРИНИМАЕТЕ НА СЕБЯ ВЕСЬ РИСК, СВЯЗАННЫЙ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММЫ. ПРОИЗВОДИТЕЛЬ НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА ПОТЕРЮ ДАННЫХ, УБЫТКИ, ОГРАНИЧЕНИЕ ДОСТУПНОСТИ УСЛУГ, В ТОМ ЧИСЛЕ В ОТНОШЕНИИ КАКИХ-ЛИБО ДАННЫХ, ОТПРАВЛЯЕМЫХ ПРОГРАММОЙ PASSWORD MANAGER В АДРЕС ВНЕШНЕГО ХРАНИЛИЩА В ЦЕЛЯХ СИНХРОНИЗАЦИИ И РЕЗЕРВНОГО КОПИРОВАНИЯ ДАННЫХ. ШИФРОВАНИЕ ДАННЫХ С ПОМОЩЬЮ ПРОГРАММЫ PASSWORD MANAGER НЕ ПРЕДПОЛАГАЕТ, ЧТО ПОСТАВЩИК НЕСЕТ КАКУЮ БЫ ТО НИ БЫЛО ОТВЕТСТВЕННОСТЬ ЗА БЕЗОПАСНОСТЬ ТАКИХ ДАННЫХ. ВЫ ПРЯМО СОГЛАШАЕТЕСЬ, ЧТО ДАННЫЕ, ПОЛУЧАЕМЫЕ, ИСПОЛЬЗУЕМЫЕ, ШИФРУЕМЫЕ, СОХРАНЯЕМЫЕ, СИНХРОНИЗИРУЕМЫЕ ИЛИ ОТПРАВЛЯЕМЫЕ С ПОМОЩЬЮ ПРОГРАММЫ PASSWORD MANAGER, МОГУТ ТАКЖЕ ХРАНИТЬСЯ НА СТОРОННИХ СЕРВЕРАХ (ЭТО КАСАЕТСЯ ТОЛЬКО ТЕХ СЛУЧАЕВ ИСПОЛЬЗОВАНИЯ ПРОГРАММЫ PASSWORD MANAGER, КОГДА ВКЛЮЧЕНЫ СЛУЖБЫ СИНХРОНИЗАЦИИ И РЕЗЕРВНОГО КОПИРОВАНИЯ). ЕСЛИ ПОСТАВЩИК ПО СВОЕМУ СОБСТВЕННОМУ УСМОТРЕНИЮ РЕШАЕТ ИСПОЛЬЗОВАТЬ ТАКОЕ СТОРОННЕЕ ХРАНИЛИЩЕ, ВЕБ-САЙТ, ВЕБ-ПОРТАЛ, СЕРВЕР ИЛИ СЛУЖБУ, ПОСТАВЩИК НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА КАЧЕСТВО, БЕЗОПАСНОСТЬ ИЛИ ДОСТУПНОСТЬ ТАКОЙ СТОРОННЕЙ СЛУЖБЫ. КРОМЕ ТОГО, ПОСТАВЩИК НИ В КОЕЙ МЕРЕ НЕ НЕСЕТ ПЕРЕД ВАМИ ОТВЕТСТВЕННОСТИ ЗА КАКОЕ-ЛИБО НАРУШЕНИЕ ТРЕТЬЕЙ СТОРОНОЙ ДОГОВОРНЫХ ИЛИ ЮРИДИЧЕСКИХ ОБЯЗАТЕЛЬСТВ, ИЛИ ЗА УЩЕРБ, УПУЩЕННУЮ ВЫГОДУ, МАТЕРИАЛЬНЫЕ ИЛИ НЕМАТЕРИАЛЬНЫЕ УБЫТКИ, ИЛИ ЗА ДРУГИЕ УБЫТКИ ЛЮБОГО ХАРАКТЕРА, ПОНЕСЕННЫЕ ВСЛЕДСТВИЕ ИСПОЛЬЗОВАНИЯ ПРОГРАММЫ. ПОСТАВЩИК НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА СОДЕРЖИМОЕ КАКИХ БЫ ТО НИ БЫЛО ДАННЫХ, ПОЛУЧАЕМЫХ, ИСПОЛЬЗУЕМЫХ, ШИФРУЕМЫХ, СОХРАНЯЕМЫХ, СИНХРОНИЗИРУЕМЫХ ИЛИ ОТПРАВЛЯЕМЫХ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММЫ PASSWORD MANAGER ИЛИ ХРАНИЛИЩА. ВЫ ПРИЗНАЕТЕ, ЧТО ПОСТАВЩИК НЕ ИМЕЕТ ДОСТУПА К СОДЕРЖИМОМУ СОХРАНЕННЫХ ДАННЫХ, А ТАКЖЕ НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА МОНИТОРИНГ ТАКИХ ДАННЫХ И НЕ ИМЕЕТ ВОЗМОЖНОСТИ ОСУЩЕСТВЛЯТЬ ТАКОЙ МОНИТОРИНГ ЛИБО УДАЛЯТЬ НЕЗАКОННОЕ ИЛИ ОПАСНОЕ СОДЕРЖИМОЕ.

Поставщику принадлежат все права на улучшения, обновления и исправления программы Password MANAGER (далее — «Улучшения»), даже если такие Улучшения создаются на основании Ваших отзывов, идей или предложений, предоставленных в любой форме. У Вас нет права на какую-либо компенсацию, в том числе на роялти, в связи с такими Улучшениями.

КОМПАНИИ И ЛИЦЕНЗИАРЫ ПОСТАВЩИКА НЕ НЕСУТ ПЕРЕД ВАМИ ОТВЕТСТВЕННОСТИ В СВЯЗИ С КАКИМИ БЫ ТО НИ БЫЛО ПРЕТЕНЗИЯМИ И ОБЯЗАТЕЛЬСТВАМИ, ТАК ИЛИ ИНАЧЕ ВОЗНИКАЮЩИМИ ВСЛЕДСТВИЕ ИЛИ В ОТНОШЕНИИ ИСПОЛЬЗОВАНИЯ ВАМИ ИЛИ ТРЕТЬИМИ СТОРОНАМИ ПРОГРАММЫ PASSWORD MANAGER, ИСПОЛЬЗОВАНИЯ ИЛИ НЕИСПОЛЬЗОВАНИЯ КАКОЙ-ЛИБО БРОКЕРСКОЙ ФИРМЫ (ИЛИ АГЕНТА) ИЛИ ПРОДАЖИ (ИЛИ ПРИОБРЕТЕНИЯ) КАКИХ-ЛИБО ЦЕННЫХ БУМАГ, ВНЕ ЗАВИСИМОСТИ ОТ ТОГО, НА ЧЕМ ОСНОВАНЫ ТАКИЕ ПРЕТЕНЗИИ, БУДЬ ТО ЮРИДИЧЕСКИЕ НОРМЫ ИЛИ ПРИНЦИПЫ СПРАВЕДЛИВОСТИ.

КОМПАНИИ И ЛИЦЕНЗИАРЫ ПОСТАВЩИКА НЕ НЕСУТ ПЕРЕД ВАМИ ОТВЕТСТВЕННОСТИ ЗА КАКИЕ-ЛИБО И ВСЕ ПРЯМЫЕ, НЕПРЕДНАМЕРЕННЫЕ, ФАКТИЧЕСКИЕ, КОСВЕННЫЕ ИЛИ ПРЕДСКАЗУЕМЫЕ КОСВЕННЫЕ УБЫТКИ, ВОЗНИКАЮЩИЕ ВСЛЕДСТВИЕ ИЛИ В ОТНОШЕНИИ ИСПОЛЬЗОВАНИЯ КАКОГО-ЛИБО СТОРОННЕГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, КАКИХ-ЛИБО ДАННЫХ, ДОСТУП К КОТОРЫМ БЫЛ ПОЛУЧЕН С ПОМОЩЬЮ ПРОГРАММЫ PASSWORD MANAGER, ИСПОЛЬЗОВАНИЯ ИЛИ НЕВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ВАМИ ПРОГРАММЫ PASSWORD MANAGER (ИЛИ ПОЛУЧЕНИЯ ДОСТУПА К НЕЙ) ИЛИ КАКИХ-ЛИБО ДАННЫХ, ПРЕДОСТАВЛЯЕМЫХ С ПОМОЩЬЮ ПРОГРАММЫ PASSWORD MANAGER, ВНЕ ЗАВИСИМОСТИ ОТ ТОГО, НА ЧЕМ ОСНОВАНЫ ТАКИЕ СВЯЗАННЫЕ С ПОНЕСЕННЫМ УЩЕРБОМ ПРЕТЕНЗИИ, БУДЬ ТО ЮРИДИЧЕСКИЕ НОРМЫ ИЛИ ПРИНЦИПЫ СПРАВЕДЛИВОСТИ. К УЩЕРБУ, ИСКЛЮЧАЕМОМУ НАСТОЯЩИМ ПОЛОЖЕНИЕМ, СРЕДИ ПРОЧЕГО, ОТНОСИТСЯ ПОТЕРЯ ДЕЛОВЫХ ВОЗМОЖНОСТЕЙ, ФИЗИЧЕСКИЙ ИЛИ МАТЕРИАЛЬНЫЙ УЩЕРБ,

ПРИОСТАНОВКА ХОЗЯЙСТВЕННОЙ ДЕЯТЕЛЬНОСТИ, ПОТЕРЯ ДЕЛОВОЙ ИЛИ ЛИЧНОЙ ИНФОРМАЦИИ. В НЕКОТОРЫХ ЮРИСДИКЦИЯХ ЗАПРЕЩЕНО ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ ЗА ПРИЧИНЕНИЕ НЕПРЕДНАМЕРЕННЫХ ИЛИ ПРЕДСКАЗУЕМЫХ КОСВЕННЫХ УБЫТКОВ, ПОЭТОМУ НАСТОЯЩЕЕ ОГРАНИЧЕНИЕ МОЖЕТ НЕ РАСПРОСТРАНЯТЬСЯ НА ВАС. В ТАКОМ СЛУЧАЕ ОТВЕТСТВЕННОСТЬ ПОСТАВЩИКА ОГРАНИЧИВАЕТСЯ МИНИМАЛЬНЫМ ОБЪЕМОМ, ПРЕДУСМОТРЕННЫМ ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ.

ИНФОРМАЦИЯ, ПРЕДОСТАВЛЯЕМАЯ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММЫ PASSWORD MANAGER, В ТОМ ЧИСЛЕ БИРЖЕВЫЕ СВОДКИ, ДАННЫЕ АНАЛИЗА, ИНФОРМАЦИЯ О СОСТОЯНИИ РЫНКА, НОВОСТИ И ФИНАНСОВЫЕ ПОКАЗАТЕЛИ, МОЖЕТ ПРЕДОСТАВЛЯТЬСЯ С ЗАДЕРЖКОЙ, СОДЕРЖАТЬ НЕТОЧНОСТИ, ОШИБКИ ИЛИ ПРОПУСКИ, ПРИ ЭТОМ КОМПАНИИ И ЛИЦЕНЗИАРЫ ПОСТАВЩИКА НЕ НЕСУТ ОТВЕТСТВЕННОСТИ В СВЯЗИ С ЭТИМ. ПОСТАВЩИК МОЖЕТ ИЗМЕНЯТЬ ИЛИ УДАЛЯТЬ ЛЮБЫЕ АСПЕКТЫ ИИЛ ФУНКЦИИ ПРОГРАММЫ PASSWORD MANAGER, А ТАКЖЕ МОЖЕТ В ЛЮБОЕ ВРЕМЯ БЕЗ ПРЕДВАРИТЕЛЬНОГО УВЕДОМЛЕНИЯ ИСПОЛЬЗОВАТЬ В ПРОГРАММЕ PASSWORD MANAGER ВСЕ ИЛИ ЛЮБЫЕ ФУНКЦИИ ИЛИ ТЕХНОЛОГИИ.

ЕСЛИ ПОЛОЖЕНИЯ НАСТОЯЩЕГО РАЗДЕЛА ПО КАКОЙ-ЛИБО ПРИЧИНЕ УТРАЧИВАЮТ СВОЮ ЮРИДИЧЕСКУЮ СИЛУ ИЛИ ЕСЛИ ПОСТАВЩИК ПРИЗНАН ОТВЕТСТВЕННЫМ ЗА НАНЕСЕНИЕ УЩЕРБА, УБЫТКОВ И Т. Д. В РАМКАХ ДЕЙСТВУЮЩЕГО ЗАКОНОДАТЕЛЬСТВА, СТОРОНЫ СОГЛАШАЮТСЯ, ЧТО ОТВЕТСТВЕННОСТЬ ПОСТАВЩИКА ПЕРЕД ВАМИ ОГРАНИЧИВАЕТСЯ ОБЩЕЙ СУММОЙ, УПЛАЧЕННОЙ ВАМИ В КАЧЕСТВЕ ЛИЦЕНЗИОННОГО СБОРА.

ВЫ СОГЛАШАЕТЕСЬ ГАРАНТИРОВАТЬ НЕОБХОДИМЫЕ ВЫПЛАТЫ И ОБЕСПЕЧИТЬ ПРАВОВУЮ ЗАЩИТУ, С ТЕМ ЧТОБЫ ОГРАДИТЬ ПОСТАВЩИКА, ЕГО СОТРУДНИКОВ, ДОЧЕРНИЕ КОМПАНИИ, СВЯЗАННЫЕ СУБЪЕКТЫ, ПАРТНЕРОВ ПО ВОПРОСАМ РЕБРЕНДИНГА И В ДРУГИХ ОБЛАСТЯХ ОТ КАКИХ БЫ ТО НИ БЫЛО И ВСЕХ ПРЕТЕНЗИЙ ТРЕТЬИХ СТОРОН (В ТОМ ЧИСЛЕ ВЛАДЕЛЬЦЕВ УСТРОЙСТВА ИЛИ ЛИЦ, ЧЬИ ПРАВА ЗАТРАГИВАЮТ ДАННЫЕ, ИСПОЛЬЗУЕМЫЕ В ПРОГРАММЕ PASSWORD MANAGER ИЛИ В ХРАНИЛИЩЕ) И ОБЯЗАТЕЛЬСТВ ПЕРЕД НИМИ, А ТАКЖЕ ОТ УЩЕРБА, УБЫТКОВ, ЗАТРАТ, ВЫПЛАТ И РАСХОДОВ, КОТОРЫЕ ТАКИЕ СТОРОНЫ МОГУТ ПОНЕСТИ В РЕЗУЛЬТАТЕ ИСПОЛЬЗОВАНИЯ ВАМИ ПРОГРАММЫ PASSWORD MANAGER.

3. Данные в программе Password Manager. Если другое не предусмотрено и прямо не указано Вами, все данные, вводимые Вами и сохраняемые в базе данных программы Password Manager, сохраняются в зашифрованном виде на Вашем компьютере или на другом указанном Вами устройстве хранения. Вы понимаете, что в случае удаления или повреждения базы данных либо иных файлов программы Password Manager все содержащиеся в них данные будут безвозвратно потеряны. Вы также понимаете и принимаете на себя риск такой потери. Тот факт, что Ваши персональные данные хранятся на компьютере в зашифрованном виде, не означает, что информация не может быть похищена или ненадлежащим образом использована кем-то, у кого есть основной пароль или доступ к определяемому пользователем устройству активации, для того чтобы открыть базу данных. Вы несете ответственность за обеспечение безопасности всех способов получения доступа.

4. Передача персональных данных поставщику или в Хранилище. По Вашему желанию и исключительно в целях своевременного выполнения синхронизации и резервного копирования данных программа Password Manager передает или отправляет персональные данные из базы данных программы Password Manager — в частности, пароли, учетные данные, сведения об учетных записях и удостоверениях — посредством Интернета в Хранилище. Данные передаются исключительно в зашифрованном виде. Использование программы Password Manager для заполнения веб-форм с помощью паролей, учетных или иных данных может требовать отправки необходимых сведений по Интернету на указанный Вами веб-сайт. Такая передача данных не инициируется программой Password Manager, и, стало быть, Поставщик не

может нести ответственность за безопасность такого взаимодействия с каким бы то ни было веб-сайтом, поддерживаемым различными поставщиками. Любые транзакции, осуществляемые с помощью Интернета, вне зависимости от того, используется или не используется программа Password Manager, осуществляются по Вашему единоличному усмотрению, и Вы берете на себя весь риск и всю ответственность за какой бы то ни было ущерб, связанный с работой компьютера или потерей данных в результате загрузки и/или использования каких-либо подобных материалов или услуг. Чтобы минимизировать риск потери важных данных, Поставщик рекомендует клиентам время от времени выполнять резервное копирование базы данных и других файлов, содержащих конфиденциальную информацию, на внешние устройства. Поставщик не имеет возможности каким-либо способом помочь Вам восстановить потерянные или поврежденные данные. Если Поставщик предоставляет услуги резервного копирования для файлов пользовательской базы данных в случае повреждения или удаления файлов на компьютере пользователя, такие услуги резервного копирования предоставляются без какой-либо гарантии и не дают основания полагать, что Поставщик несет какую бы то ни было ответственность перед Вами.

Используя программу Password Manager, Вы соглашаетесь, что программа может время от времени обращаться к серверам Поставщика в целях уточнения сведений о лицензии, а также для проверки на наличие исправлений, пакетов обновлений и прочих обновлений, которые могут использоваться для улучшения, поддержки, изменения или усовершенствования работы программы Password Manager. Программное обеспечение может отправлять общие сведения о компьютере, связанные с работой программы Password Manager в соответствии с документом Политика конфиденциальности.

5. Сведения и инструкции по удалению. Любую информацию, которую Вы хотите получить из базы данных, необходимо экспортировать, прежде чем удалять программу Password Manager.

Дополнительные положения для программы Password Manager применяются исключительно в отношении конечных пользователей программы ESET Smart Security Premium.

ESET LiveGuard. В отношении ESET LiveGuard применяются следующие дополнительные положения.

Программное обеспечение содержит функцию дополнительного анализа файлов, отправленных Конечным пользователем. Поставщик должен использовать файлы, отправленные Конечным пользователем, и результаты анализа исключительно в соответствии с Политикой конфиденциальности и соответствующими правовыми нормами.

Дополнительные положения для ESET LiveGuard применяются исключительно в отношении конечных пользователей программы ESET Smart Security Premium.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

Политика конфиденц.

Компания ESET, spol. s r. o., зарегистрированная по адресу Einsteinova 24, 851 01 Bratislava, Slovak Republic, внесенная в реестр юридических лиц окружного суда I в Братиславе, раздел Sro, запись 3586/B, регистрационный номер предприятия 31333532, как контролер данных (далее — «ESET» или «Мы») уделяет особое внимание защите персональных данных. Мы стремимся соблюдать требования к прозрачности, устанавливаемые Общим регламентом ЕС по защите данных (GDPR). Поэтому Мы публикуем эту Политику конфиденциальности, исключительно чтобы

уведомить клиента, который является субъектом данных (далее — «Конечный пользователь» или «Вы»), о следующих аспектах защиты персональных данных:

- Правовые основания для обработки персональных данных.
- Передача данных третьим лицам и конфиденциальность.
- Защита данных.
- Ваши права как субъекта данных.
- Обработка персональных данных.
- Контактная информация.

Правовые основания для обработки персональных данных

У нас есть лишь несколько правовых оснований для обработки данных, которые Мы используем в соответствии с законодательными требованиями, предусмотренными защитой личных данных. ESET обрабатывает персональные данные главным образом для того, чтобы выполнить Лицензионное соглашение («Лицензионное соглашение») с Конечным пользователем (статья 6 (1) (b) GDPR), которое применяется при предоставлении Продуктов и Служб ESET, если прямо не указанно иное, например:

- Законные интересы — это правовое основание (статья 6 (1) (f) GDPR) для обработки данных о том, как наши клиенты используют наши Службы и насколько они ими удовлетворены. Это позволяет нам постоянно повышать уровень безопасности и поддержки для наших пользователей и улучшать предоставляемые продукты и услуги. В применимом законодательстве даже реклама признается законным интересом, поэтому, как правило, Мы руководствуемся этим при осуществлении маркетинговой коммуникации с клиентами.

- Согласие (статья 6 (1) (a) GDPR), которое Мы можем запросить у Вас в особых ситуациях, когда Мы считаем это правовое основание наиболее подходящим или если это необходимо по закону.

- Соблюдение правовых обязательств (статья 6 (1) (c) GDPR), например требований в отношении электронной переписки и хранения документов, связанных с выставлением счетов или накладных.

Передача данных третьим лицам и конфиденциальность

Мы не передаем Ваши данные третьим лицам. Однако ESET — это компания, ведущая деятельность в глобальных масштабах через сеть распространения, обслуживания и поддержки, которая состоит из аффилированных компаний и партнеров. В целях выполнения Лицензионного соглашения, например для предоставления услуг или поддержки, Мы можем обмениваться с аффилированными компаниями и партнерами информацией о лицензиях, оплате и технической поддержке, которую обрабатывает компания ESET.

Компания ESET обрабатывает данные преимущественно в странах Европейского Союза (ЕС). Однако в зависимости от Вашего местонахождения (при использовании наших продуктов и/или

служб за пределами ЕС) и/или выбранной Вами службы нам может понадобиться передать Ваши данные в страну за пределами ЕС. Например, мы используем сторонние службы облачных вычислений. В таких случаях мы тщательно выбираем поставщиков таких служб и обеспечиваем надлежащий уровень защиты данных с помощью договорных, а также технических и организационных мер. Как правило, мы применяем стандартные договорные условия, действующие в ЕС. При необходимости они могут дополняться другими условиями.

В некоторых странах за пределами ЕС, таких как Великобритания и Швейцария, сопоставимый уровень защиты данных уже определен законодательством ЕС. В связи с этим передача данных в эти страны не требует специального разрешения или соглашения.

Защита данных

ESET проводит соответствующие технические и организационные мероприятия, чтобы гарантировать уровень безопасности согласно возможным рискам. Мы прилагаем все усилия, чтобы обеспечить непрерывную конфиденциальность, целостность, доступность и надежность обрабатывающих служб и систем. Однако если произойдет утечка данных, которая будет угрожать Вашим правам и свободам, мы готовы уведомить об этом надзорные органы, а также затронутых Конечных пользователей как субъектов данных.

Права субъекта данных

Права каждого Конечного пользователя важны, поэтому Мы хотели бы рассказать Вам о правах, которые ESET гарантирует всем Конечным пользователям независимо от того, находятся ли они в странах ЕС или нет. Эти права описаны ниже. Чтобы воспользоваться своими правами субъекта данных, Вы можете обратиться к нам через форму для связи со службой поддержки или по адресу электронной почты dpo@eset.sk. В целях идентификации просим Вас предоставить следующую информацию: имя, адрес электронной почты и лицензионный ключ (если есть) или номер клиента и название компании. Не отправляйте другие персональные данные, такие как дата рождения. Чтобы рассмотреть Ваше обращение, а также в целях идентификации Мы обработаем Ваши персональные данные.

Право отозвать согласие. Право отозвать согласие действует только в том случае, если данные обрабатываются исключительно по согласию. Если Мы обрабатываем Ваши персональные данные на основании Вашего согласия, Вы имеете право в любое время отозвать его без указания причин. Отзыв согласия касается только обработки данных в будущем и не влияет на законность их обработки, выполнявшейся до этого.

Право на возражение. Право возразить против обработки данных действует в том случае, если данные обрабатываются на основании законного интереса ESET или третьей стороны. Если Мы обрабатываем Ваши персональные данные в своих законных интересах, Вы как субъект данных можете в любое время возразить против этого. Ваше возражение касается только обработки данных в будущем и не влияет на законность их обработки, выполнявшейся до этого. Если Мы обрабатываем Ваши персональные данные в целях прямого маркетинга, Вам не нужно указывать причину возражения. Это также относится к составлению профиля в той мере, насколько это связано с прямым маркетингом. Во всех остальных случаях Мы просим Вас кратко описать, почему Вы возражаете против законных интересов компании ESET обрабатывать Ваши персональные данные.

Обратите внимание, что в некоторых случаях, несмотря на Ваш отзыв согласия, Мы можем продолжить обрабатывать Ваши персональные данные на другом правовом основании,

например для выполнения договора.

Право доступа. Как субъект данных Вы имеете право в любое время бесплатно получить информацию о своих данных, которые хранятся в ESET.

Право на исправление. Если Мы непреднамеренно обрабатываем неверные персональные данные о Вас, Вы имеете право требовать их исправления.

Право на удаление и право на ограничение обработки. Как субъект данных Вы имеете право требовать удаления или ограничения обработки Ваших персональных данных. Если персональные данные обрабатываются с Вашего согласия, вы можете отозвать его и, если нет иных правовых оснований для обработки данных, например в целях выполнения договора, Мы немедленно их удалим. Ваши персональные данные также будут удалены по окончании нашего периода хранения, если они больше не требуются для указанных в их отношении целей.

Если Мы используем Ваши персональные данные исключительно в целях прямого маркетинга, а Вы отозвали свое согласие или выдвинули возражение против законных интересов ESET на сбор таких данных, Мы ограничим их обработку следующим образом: Ваши контактные данные будут внесены в наш внутренний черный список, чтобы не допускать нежелательных контактов. В противном случае Ваши персональные данные будут удалены.

Обратите внимание, что по закону или предписанию надзорного органа от нас может требоваться хранить персональные данные в течение определенного периода. Обязательства по хранению и периоды хранения могут также регулироваться законодательством Словакии. По окончании такого периода персональные данные удаляются.

Запросить переносимость данных. Как субъект данных Вы можете получить персональные данные, которые обрабатывает ESET, в файле формата XLS.

Право на подачу жалобы. Как субъект данных Вы имеете право в любое время подать жалобу в надзорный орган. ESET действует согласно словацким законам и законам о защите данных ЕС. Надзорным органом является Офис по защите персональных данных Словацкой Республики, расположенный по адресу Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Обработка персональных данных

Услуги, предоставляемые ESET и реализованные в нашем продукте, предоставляются в соответствии с договором, именуемым ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ, некоторые условия которого заслуживают особого внимания. Мы хотим рассказать Вам подробнее о сборе данных, связанных с предоставлением наших служб. Мы предоставляем различные услуги, перечисленные в Лицензионном соглашении и описании возможностей продукта, именуемом документация. Чтобы все это работало, нам необходимо собирать следующую информацию.

Данные лицензирования и выставления счетов. Таки данные, как имя, адрес электронной почты, лицензионный ключ и адрес (если требуется), название компании и платежные данные, собираются и обрабатываются компанией ESET для упрощения активации лицензии, доставки лицензионного ключа, отправки напоминаний об истечении срока действия и запросов в службу поддержки, проверки подлинности лицензии, предоставления наших услуг и рассылки уведомлений, в том числе маркетинговых сообщений, в соответствии с действующим законодательством или Вашим согласием. Компания ESET по закону обязана хранить информацию о выставленных счетах в течение 10 лет, однако сведения о лицензировании

становятся анонимными не позднее чем через 12 месяцев после окончания срока действия лицензии.

Сведения об обновлении и другая статистика. Мы также обрабатываем информацию, касающуюся процесса установки и Вашего компьютера, включая сведения о платформе, на которой установлен наш продукт, и информацию об операциях и функциях наших продуктов, такую как сведения об операционной системе и оборудовании, идентификаторы установки, идентификаторы лицензий, IP-адрес, MAC-адрес, настройки конфигурации продукта. Это делается для того, чтобы мы могли обновлять продукты с целью обслуживания, повышения уровня безопасности и оптимизации серверной инфраструктуры.

Эти данные изолированы от идентификационной информации, необходимой для лицензирования и выставления счетов, поскольку для них не требуется идентификация Конечного пользователя. Период хранения составляет до 4 лет.

Система репутации ESET LiveGrid®. Однонаправленные хеши, связанные с заражением, обрабатываются в целях работы системы репутации ESET LiveGrid®, которая повышает эффективность наших решений для защиты от вредоносных программ, сравнивая просканированные файлы с элементами белого и черного списков в облачной базе данных. Во время этого процесса Конечный пользователь не идентифицируется.

Система обратной связи ESET LiveGrid®. Подозрительные образцы метаданных из внешних источников в рамках системы обратной связи ESET LiveGrid®, благодаря которой ESET может мгновенно реагировать на нужды пользователей и своевременно адаптироваться под новейшие угрозы. Мы рассчитываем на то, что вы будете присылать нам:

- Зараженные элементы, такие как потенциальные образцы вирусов и прочих вредоносных программ; подозрительные, проблемные, потенциально нежелательные и небезопасные объекты, такие как исполняемые файлы, сообщения электронной почты, про которые сообщили вы как про спам или которые выявил наш продукт;

- Сведения о пользовании Интернетом, например IP-адрес, географическое расположение, пакеты IP, URL-адреса и кадры Ethernet;

- Файлы аварийных дампов и их содержимое.

Мы не стремимся собирать какие-либо данные, кроме обозначенных выше, но иногда этого невозможно избежать. Случайно собранные данные могут входить в состав вредоносных программ (будучи собранными без вашего ведома и одобрения) либо входить в имена файлов и URL-адреса, и Мы не намерены делать их частью наших систем или обрабатывать их для целей, указанных в настоящей Политике конфиденциальности.

Вся информация, получаемая и обрабатываемая с помощью системы обратной связи ESET LiveGrid®, не содержит данных, идентифицирующих Конечного пользователя.

Оценка безопасности подключенных к сети устройств. Чтобы функция оценки безопасности работала, Мы обрабатываем такие данные, как имя локальной сети и сведения об устройствах в ней (присутствие, тип, имя, IP- и MAC-адрес устройства в локальной сети, связанные с информацией о лицензии). К информации также относятся тип безопасности беспроводной сети и тип шифрования в беспроводной сети для маршрутизаторов. Сведения о лицензии, идентифицирующие Конечного пользователя, станут анонимными не позднее чем через 12 месяцев после окончания срока действия лицензии.

Техническая поддержка. Для обслуживания и предоставления поддержки может потребоваться контактная информация, сведения о лицензии и данные, указанные в Ваших запросах на поддержку. Исходя из выбранного способа общения, Мы можем фиксировать Ваш электронный адрес, номер телефона, информацию о лицензии, сведения о программах и описание Вашего инцидента. Мы можем запросить у Вас сведения, чтобы ускорить предоставление поддержки. Данные, используемые для оказания технической поддержки, хранятся в течение 4 лет.

Защита от неправильного использования данных. Если Учетная запись ESET HOME на сайте https://home.eset.com создана и Конечный пользователь активировал эту функцию в связи с кражей компьютера, будет собираться и обрабатываться следующая информация: данные о местоположении, снимки экрана, сведения о конфигурации компьютера и записи, полученные с камеры. Собранные данные хранятся на наших серверах или на серверах наших поставщиков услуг в течение 3 месяцев.

Password Manager. Если Вы активировали функцию диспетчера паролей Password Manager, сведения, связанные с вашими данными для входа, хранятся только в зашифрованном виде на Вашем компьютере или другом предназначенном для этого устройстве. Если Вы активируете службу синхронизации, зашифрованные данные хранятся на наших серверах или на серверах наших поставщиков услуг для обеспечения работы такой службы. Ни компания ESET, ни поставщики услуг не имеют доступа к зашифрованным данным. Только у Вас есть ключ для расшифровки данных. Данные будут удалены после деактивации функции.

ESET LiveGuard. Если Вы активируете функцию ESET LiveGuard, для ее работы потребуется отправка образцов, например файлов, которые предварительно отбираются Конечным пользователем. Образцы, которые Вы выберете для удаленного анализа, будут переданы в службу ESET, а результаты анализа будут отправлены на Ваш компьютер. Все подозрительные образцы обрабатываются так же, как информация, собираемая системой обратной связи ESET LiveGrid®.

Программа улучшения пользовательского опыта. Если вы решили активировать Программа улучшения пользовательского опыта , в соответствии с Вашим согласием будут собираться и использоваться анонимные данные телеметрии, касающиеся использования Наших продуктов.

Обратите внимание, что если лицо, использующее наши продукты и услуги, не является Конечным пользователем, который приобрел продукт или услугу и заключил Лицензионное соглашение с Нами (например, это сотрудник Конечного пользователя, член его семьи или лицо, которое иным способом получило право использовать продукт или услугу от Конечного пользователя в соответствии с Лицензионным соглашением), то обработка данных осуществляется в законных интересах ESET в соответствии со статьей 6 (1) (f) регламента GDPR в целях того, чтобы пользователь, уполномоченный Конечным пользователем, мог использовать продукты и услуги, предоставляемые Нами, в соответствии с Лицензионным соглашением.

Контактная информация

Если Вы хотите воспользоваться своими правами субъекта данных или у Вас возникнет вопрос или проблема, отправьте нам письмо по адресу:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24

85101 Bratislava
Slovak Republic
dpo@eset.sk