ESET ENDPOINT ANTIVIRUS 6

Руководство пользователя

Microsoft® Windows® 10/8.1/8/7/Vista/XP x86 SP3/XP x64 SP2

Щелкните здесь, чтобы загрузить актуальную версию этого документа

ENJOY SAFER TECHNOLOGY™

ESET **ENDPOINT ANTIVIRUS 6**

Программное обеспечение ESET Endpoint Antivirus разработано компанией ESET, spol. s r. o.

Дополнительные сведения см. на веб-сайте www.eset.com.

Международная служба поддержки клиентов: www.eset.com/support

Версия 3/14/2017

Содержание

1. ESET Endpoint Antivirus

ESET Endpoint Antivirus 6 представляет собой новый подход к созданию действительно комплексной системы безопасности компьютера. Новейшая версия модуля сканирования ThreatSense® работает быстро и точно для обеспечения безопасности компьютера. Таким образом, продукт представляет собой интеллектуальную систему непрерывной защиты от атак и вредоносных программ, которые могут угрожать безопасности компьютера.

ESET Endpoint Antivirus 6 — это комплексное решение для обеспечения безопасности, являющееся результатом долгих усилий, направленных на достижение оптимального сочетания максимальной степени защиты с минимальным влиянием на производительность компьютера. Современные технологии, основанные на применении искусственного интеллекта, способны превентивно противодействовать заражениям вирусами, шпионскими, троянскими, рекламными программами, червями, руткитами и другими атаками из Интернета без влияния на производительность компьютера и перерывов в работе.

ESET Endpoint Antivirus 6 предназначено в первую очередь для использования на рабочих станциях в средах небольших предприятий. Использование ESET Endpoint Antivirus в сочетании с ESET Remote Administrator в корпоративной среде позволяет с легкостью управлять любым количеством клиентских рабочих станций, применять политики и правила, отслеживать обнаруживаемые угрозы и удаленно конфигурировать клиентов с любого подключенного к сети компьютера.

1.1 Новые возможности

Графический интерфейс пользователя ESET Endpoint Antivirus полностью изменен: внешний вид стал лучше, а работа с приложением — более интуитивно понятной. Ниже приведены некоторые улучшения в ESET Endpoint Antivirus (версия 6).

Улучшенная функциональность и практичность

- Контроль устройств: теперь можно определять тип и серийный номер устройства и задавать одно правило на несколько устройств.
- Новый интеллектуальный режим HIPS: располагается между автоматическим и интерактивным режимом и дает возможность идентифицировать подозрительные действия и вредоносные процессы в системе.
- Улучшения средства обновления/зеркала: теперь можно возобновлять прерванные загрузки баз данных сигнатур вирусов и модули продуктов.
- Новый подход к удаленному управлению компьютерами с помощью ESET Remote Administrator: теперь можно повторно отправлять журналы в случае повторной установки ERA или для тестирования, устанавливать решения ESET для обеспечения безопасности в удаленном режиме, получать общие сведения о состоянии безопасности сетевой среды и сортировать различные данные для последующего использования.
- Улучшения интерфейса: теперь вручную запускать обновление базы данных сигнатур вирусов и модулей с панели задач Windows можно одним щелчком. Поддержка сенсорных экранов и экранов с высоким разрешением.
- Улучшенное обнаружение и удаление сторонних решений для обеспечения безопасности.

Новые функции

- Защита от фишинга: защищает от попыток получить пароли и другую конфиденциальную информацию, запрещая доступ к вредоносным веб-сайтам, которые принимают вид нормальных веб-сайтов.
- Повышенная скорость сканирования: использование общего локального кэша в виртуализированных средах.

Технологии обнаружения и защиты

- Повышенная скорость и надежность установки.
- Дополнительный модуль сканирования памяти: отслеживает поведение процессов и сканирует зловредные процессы, когда они снимают маскировку в памяти.
- Усовершенствованный 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 теперь поддерживает Java и помогает улучшить выявление связанных с Java уязвимостей и защиту от них.
- Улучшенное обнаружение и удаление руткитов.
- Модуль сканирования в состоянии простоя: автоматически сканирует локальные диски, если компьютер находится в состоянии простоя.

1.2 Системные требования

Для правильной работы ESET Endpoint Antivirus система должна отвечать перечисленным ниже аппаратным и программным требованиям (настройки программы по умолчанию).

Процессор:

• 32-разрядный (x86) или 64-разрядный (x64) процессор, 1 ГГц и выше (см. примечание 1).

Операционная система: Microsoft® Windows® 10/8.1/8/7/Vista/XP с пакетом обновления 3 (32-разрядная)/XP с пакетом обновления 2 (64-разрядная).

• Операционная система и пакет обновления должны поддерживаться установленной версией продукта ESET.
• Операционная система и другое ПО, установленное на компьютере, должны соответствовать системным требованиям.
• 0,3 ГБ свободной системной памяти (см. примечание 2).
• 1 ГБ свободного места на диске (см. примечание 3).
• Минимальное разрешение дисплея должно составлять 1024 x 768.
• Подключение через Интернет или локальную сеть к источнику обновления продукта (см. примечание 4).

Хотя и существует возможность установить и запустить продукт в системах, которые не соответствуют этим требованиям, рекомендуется сначала провести тестирование возможностей использования на основании требований к производительности.

ПРИМЕЧАНИЕ.
1. В случае использования ОС Windows XP минимальная частота процессора может быть более низкой.
2. Программа может использовать больше памяти, если на сильно зараженном компьютере память не используется для других задач, а также когда в программу импортируются огромные списки данных (например, «белые» списки URL-адресов).
3. Дисковое пространство, необходимое, чтобы загрузить программу установки, установить программу и хранить копию установочного пакета в данных программы, а также резервные копии обновлений программы, которые нужны для функции отката. Программа может использовать больше дискового пространства при разных настройках (например, когда хранится большее количество резервных копий обновлений, когда хранятся дампы памяти или огромные количества записей журнала) либо на зараженном компьютере (например, вследствие использования функции карантина). Рекомендуется поддерживать достаточное количество свободного дискового пространства, чтобы обеспечить возможность обновления операционной системы и обновления программы ESET.
4. Хотя это и не рекомендуется, программу можно обновить вручную со съемного носителя.

1.3 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 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 Live Grid, тысячи новых уникальных заражений появляются ежедневно. Они предназначены для обхода существующих мер безопасности и приносят доход их авторам за счет других пользователей. Специалисты вирусной лаборатории ESET ежедневно анализируют такие угрозы, подготавливают и выпускают обновления для непрерывного улучшения 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

Авторы вредоносных программ обычно не заботятся о пользователях, 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. Рекомендуется выполнять полное сканирование компьютера по крайней мере один раз в месяц, поскольку вредоносные программы изменяются, а база данных сигнатур вирусов обновляется каждый день.

Следуйте основным правилам безопасности

Это наиболее эффективное и полезное правило из всех — 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.

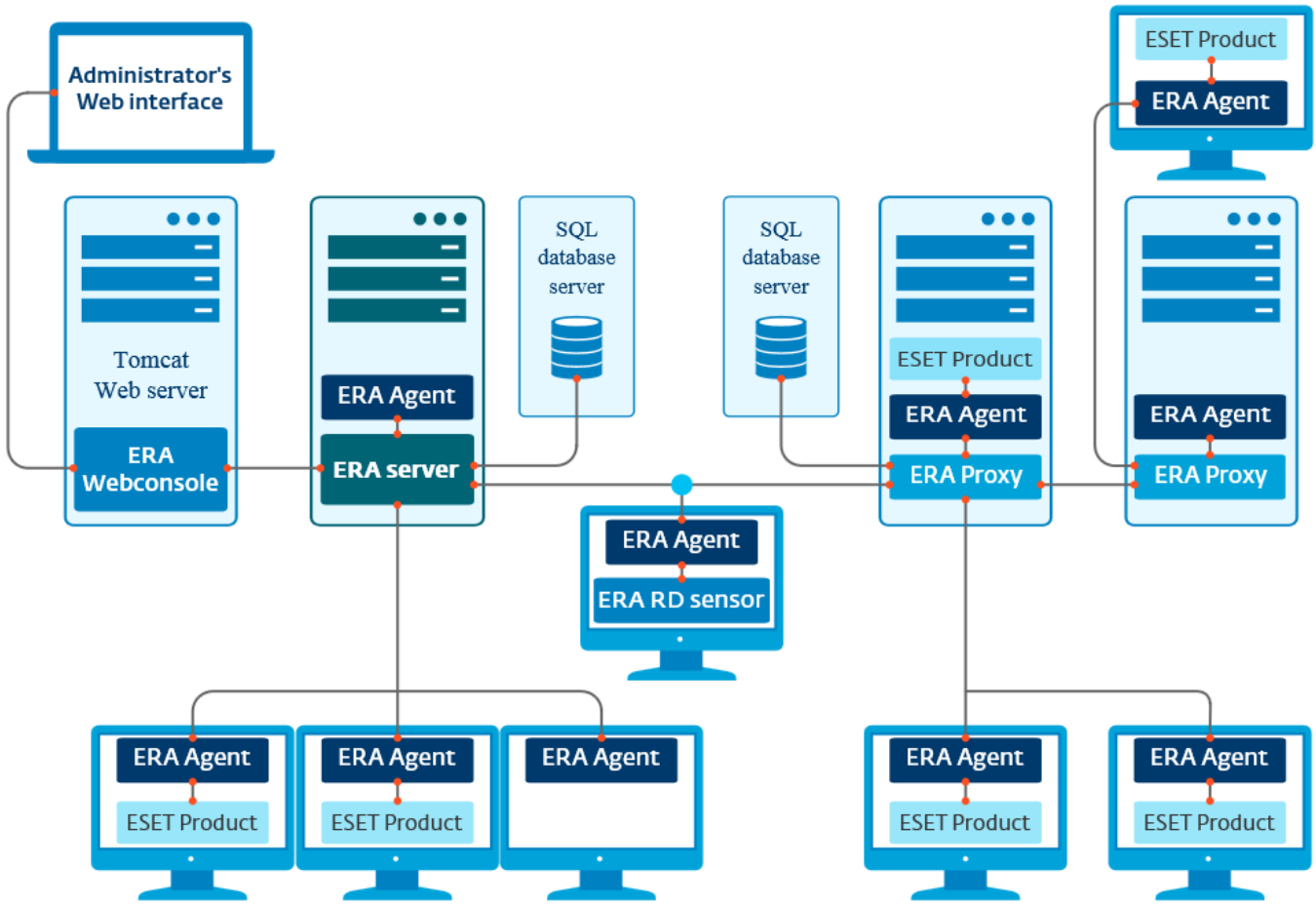
- Не посещайте подозрительные веб-сайты с множеством всплывающих окон и анимированной рекламой.
- Будьте осторожны при установке бесплатных программ, пакетов кодеков и т. п.. Используйте только безопасные программы и посещайте безопасные веб-сайты.
- Будьте осторожны, открывая вложения в сообщения электронной почты (особенно это касается сообщений, рассылаемых массово и отправленных неизвестными лицами).
- Не используйте учетную запись с правами администратора для повседневной работы на компьютере.

2. Документация для пользователей, подключенных с помощью ESET Remote Administrator

ESET Remote Administrator (ERA) — это приложение, позволяющее осуществлять централизованное управление продуктами ESET, установленными в сетевой среде. Система управления задачами ESET Remote Administrator позволяет установить на удаленные компьютеры решения ESET для обеспечения безопасности и быстро реагировать на новые проблемы и угрозы. Приложение ESET Remote Administrator не предоставляет защиту от вредоносного кода, а полагается на то, что на каждом клиенте установлено и используется решение ESET.

В решениях ESET для обеспечения безопасности предусмотрена поддержка сетей, использующих несколько платформ различных типов. В сети могут сосуществовать операционные системы Microsoft, Linux и Mac OS, а также системы, работающие на мобильных устройствах (мобильные телефоны и планшеты).

На рисунке ниже представлен пример архитектуры сети, защищенной решениями ESET для обеспечения безопасности. Этими решениями управляет приложение ERA.



ПРИМЕЧАНИЕ.
Дополнительные сведения см. в справке о решении ESET Remote Administrator в Интернете.

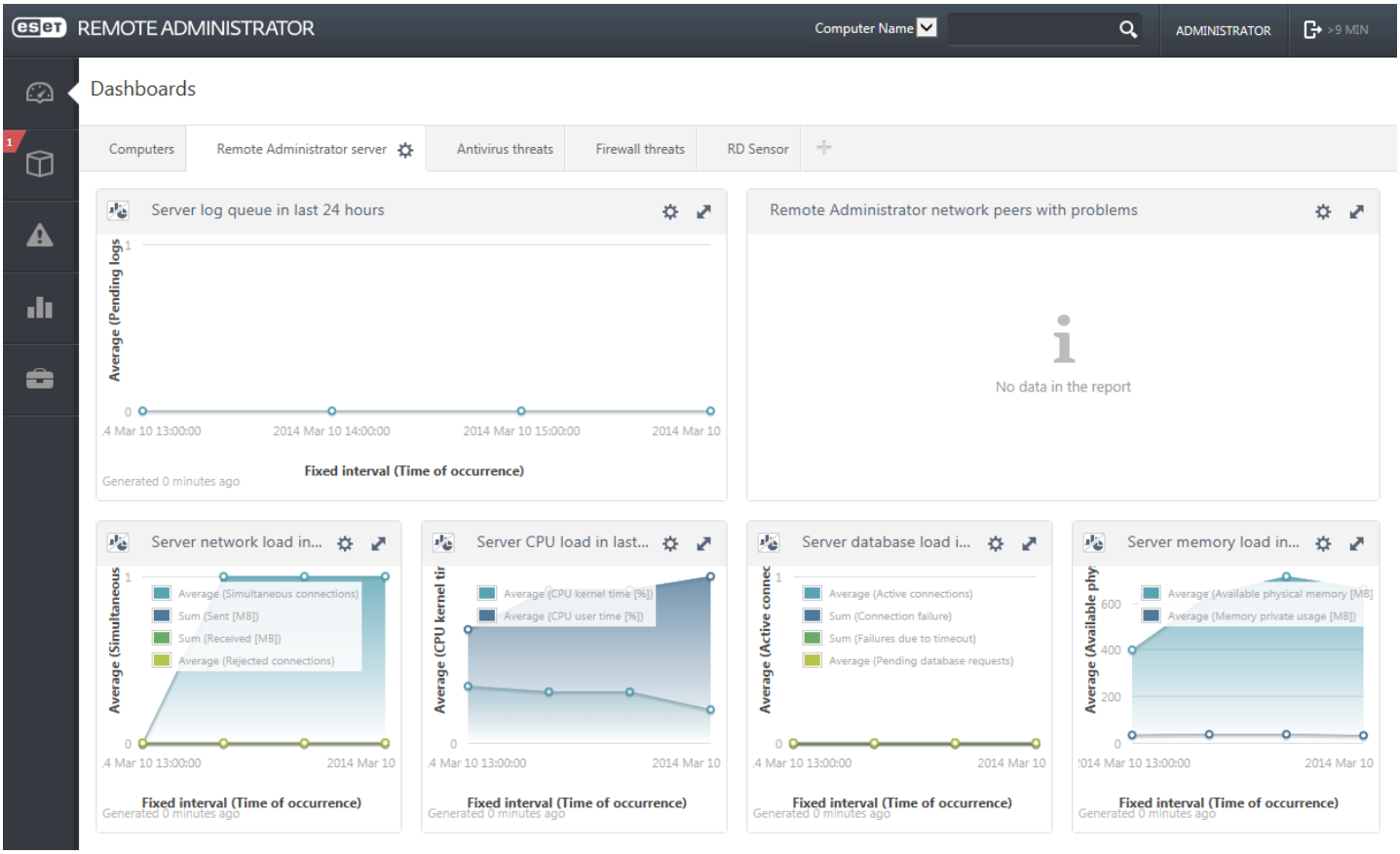
2.1 ESET Remote Administrator Server

Сервер **ESET Remote Administrator Server** является главным компонентом продукта ESET Remote Administrator. Это исполняющее приложение, которое обрабатывает все данные, получаемые от клиентов, подключенных к серверу посредством агента ERA. Агент ERA упрощает обмен данными между клиентом и сервером. Данные (журналы клиентов, файлы конфигурации и репликации агентов и т. д.) хранятся в базе данных. Для правильной обработки данных серверу ERA требуется стабильное соединение с сервером базы данных. Для оптимальной производительности рекомендуется устанавливать сервер ERA и базу данных на разные серверы. Компьютер, на котором установлен сервер ERA, должен быть настроен на прием всех запросов на подключение от агентов, прокси-сервера и компонента RD Sensor. Такие подключения проходят проверку с использованием сертификатов. После установки можно открыть веб-консоль ERA, подключающуюся к серверу ERA (см. диаграмму). При управлении решениями безопасности ESET в сети все операции с сервером ERA выполняются в веб-консоли.

2.2 Веб-консоль

Веб-консоль ERA — это приложение с веб-интерфейсом, которое отображает данные, полученные с сервера ERA, и позволяет управлять решениями безопасности ESET в вашей сети. Доступ к веб-консоли можно получить с помощью браузера. В ней отображаются общие сведения о статусах клиентов в сети. Кроме того, веб-консоль можно использовать для удаленного развертывания решений ESET на неуправляемых компьютерах. Если разрешить доступ к веб-серверу из Интернета, ESET Remote Administrator можно будет использовать практически в любом месте и на любом устройстве.

Вот так выглядит панель мониторинга веб-консоли.



В верхней части консоли расположено средство **Быстрый поиск**. Из раскрывающегося меню выберите пункт **Имя компьютера**, **Адрес IPv4/IPv6** или **Имя угрозы**, введите поисковую фразу в текстовом поле и щелкните значок лупы или нажмите клавишу **ВВОД**, чтобы выполнить поиск. Вы будете перенаправлены в раздел **Группы**, где будут показаны результаты поиска.

ПРИМЕЧАНИЕ.
Дополнительные сведения см. в справке о решении ESET Remote Administrator в Интернете.

2.3 Прокси-сервер

Прокси-сервер ERA является еще одним компонентом ESET Remote Administrator и выполняет две функции. В сетях среднего размера и корпоративных сетях с большим количеством клиентов (например, 10 000 и больше) прокси-сервер ERA может использоваться для распределения нагрузки между несколькими прокси-серверами ERA, снижая таким образом нагрузку на главный сервер ERA. Другим преимуществом прокси-сервера ERA является то, что его можно использовать для подключения к удаленном филиалу со слабой связью. Это означает, что установленные на всех клиентах агенты ERA подключаются не к главному серверу ERA, а к прокси-серверу ERA, который находится в локальной сети филиала. Таким образом освобождается канал связи с филиалом. Прокси-сервер ERA принимает подключения от всех локальных агентов ERA, получает от них данные и передает их на главный сервер ERA (или другой прокси-сервер ERA). Это позволяет включить в сеть больше клиентов без ухудшения ее производительности и скорости обработки запросов к базе данных.

В зависимости от конфигурации сети прокси-сервер ERA может подключаться к главному серверу ERA через другой прокси-сервер.

Чтобы обеспечить надлежащую работу прокси-сервера ERA, на главном компьютере, на который вы устанавливаете прокси-сервер ERA, нужно установить агент ESET, а сам компьютер нужно подключить к верхнему уровню сети (к серверу ERA или прокси-серверу ERA верхнего уровня, если такой имеется).

2.4 Агент

Агент ERA является важной частью программы ESET Remote Administrator. Решения безопасности ESET, работающие на клиентских компьютерах (например, ESET Endpoint Security) обмениваются данными с сервером ERA через агент. Это позволяет централизованно управлять решениями безопасности ESET, установленными на удаленных клиентах. Агент собирает информацию клиента и отправляет ее на сервер. Когда сервер отправляет задачу клиенту, ее вначале получает агент, который затем направляет ее клиенту. Передача данных по сети происходит между агентом и верхним уровнем сети ERA — сервером и прокси-сервером.

Для связи с сервером агент ESET использует один из трех методов, указанных ниже:

1. Агент клиента напрямую связывается с сервером.
2. Агент клиента связывается с сервером через прокси-сервер.
3. Агент клиента связывается с сервером через несколько прокси-серверов.

Агент ESET обменивается данными с установленными на клиенте решениями ESET, собирает информацию о программах, используемых на таком клиенте, и передает клиенту полученные от сервера сведения о конфигурации.

ПРИМЕЧАНИЕ.
Прокси-сервер ESET имеет собственного агента, отвечающего за обмен данными с клиентами, другими прокси-серверами и сервером.

2.5 RD Sensor

RD (Rogue Detection) Sensor — это входящий в ESET Remote Administrator инструмент поиска компьютеров в сети. Он позволяет быстро добавлять новые компьютеры в ESET Remote Administrator без необходимости искать и добавлять их вручную. Каждый обнаруженный в сети компьютер отображается в веб-консоли и добавляется в стандартную группу **Все**. После этого вы можете выполнять последующие действия уже с отдельными клиентскими компьютерами.

Компонент RD Sensor пассивно прослушивает сеть, обнаруживает находящиеся в ней компьютеры и направляет информацию о них серверу ERA. Затем сервер ERA проверяет, являются ли обнаруженные ПК неизвестными или уже находятся под его управлением.

3. Использование только продукта ESET Endpoint Antivirus

Эта часть руководства предназначена для пользователей, использующих ESET Endpoint Antivirus без ESET Remote Administrator. Доступность тех или иных функций и возможностей ESET Endpoint Antivirus полностью зависит от прав учетной записи пользователя.

3.1 Установка с помощью средства ESET AV Remover

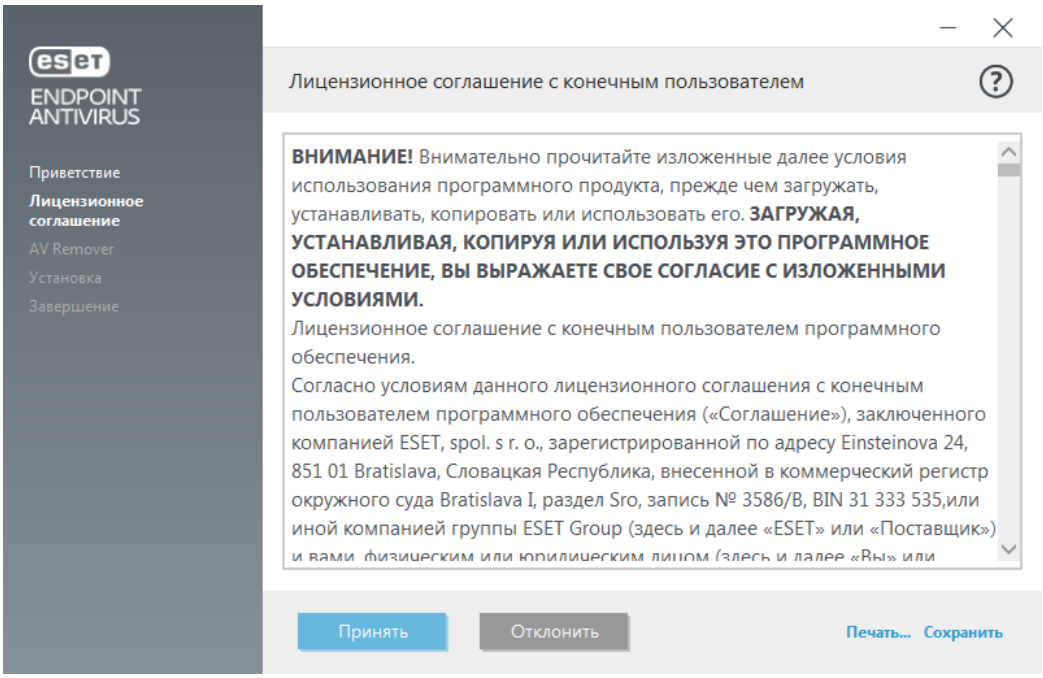
Прежде чем приступить к установке, необходимо удалить все установленные на компьютере приложения для обеспечения безопасности. Установите флажок **Я хочу удалить ненужные антивирусные программы с помощью средства ESET AV Remover**. Средство ESET AV Remover просканирует систему и удалит все поддерживаемые программы. Если вы хотите установить ESET Endpoint Antivirus без использования ESET AV Remover, нажмите кнопку **Продолжить**, не устанавливая этот флажок.

3.1.1 ESET AV Remover

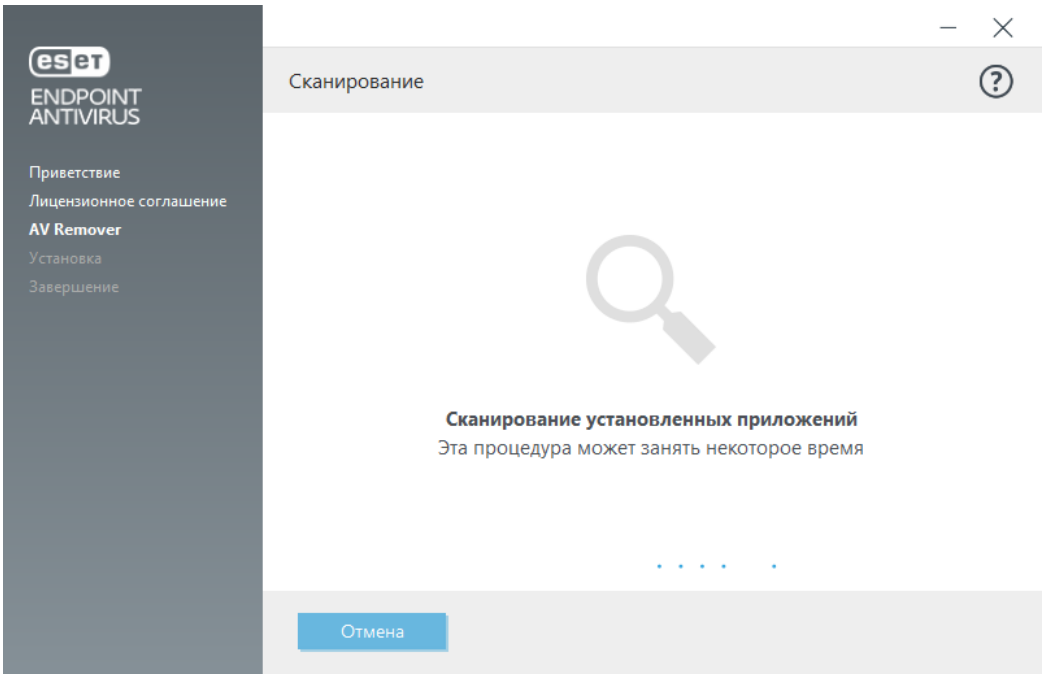
Средство ESET AV Remover поможет удалить практически любую установленную в системе антивирусную программу. Процедура удаления антивирусной программы с помощью средства ESET AV Remover приведена ниже.

1. Чтобы просмотреть список антивирусных программ, которые можно удалить с помощью ESET AV Remover, ознакомьтесь с соответствующей статьей базы знаний ESET.

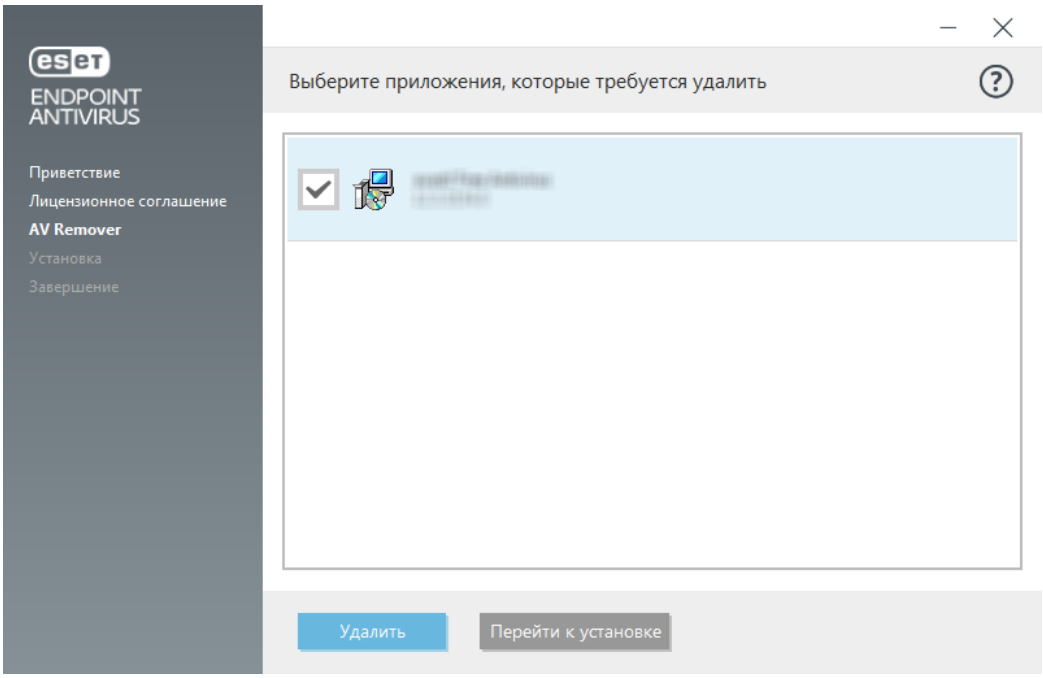
2. Прочтите лицензионное соглашение с конечным пользователем и нажмите кнопку **Принять**, чтобы подтвердить свое согласие с его условиями. Нажав кнопку **Отклонить**, вы перейдете к установке ESET Endpoint Antivirus. При этом уже установленное на компьютере приложение для обеспечения безопасности удалено не будет.



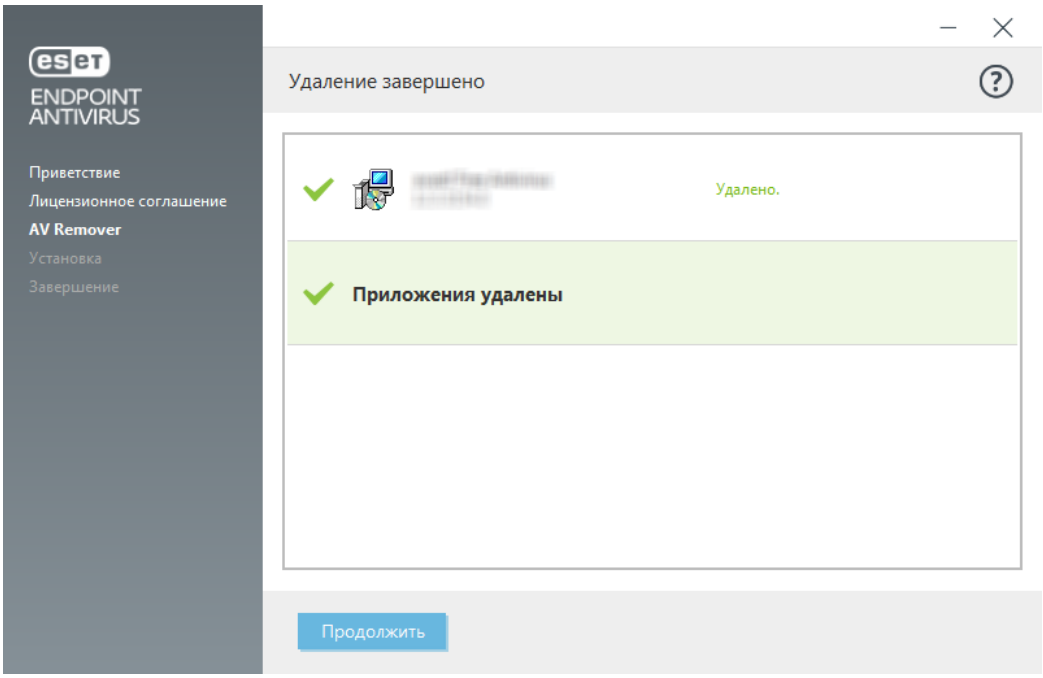
3. Средство ESET AV Remover начнет поиск установленного в системе антивирусного ПО.



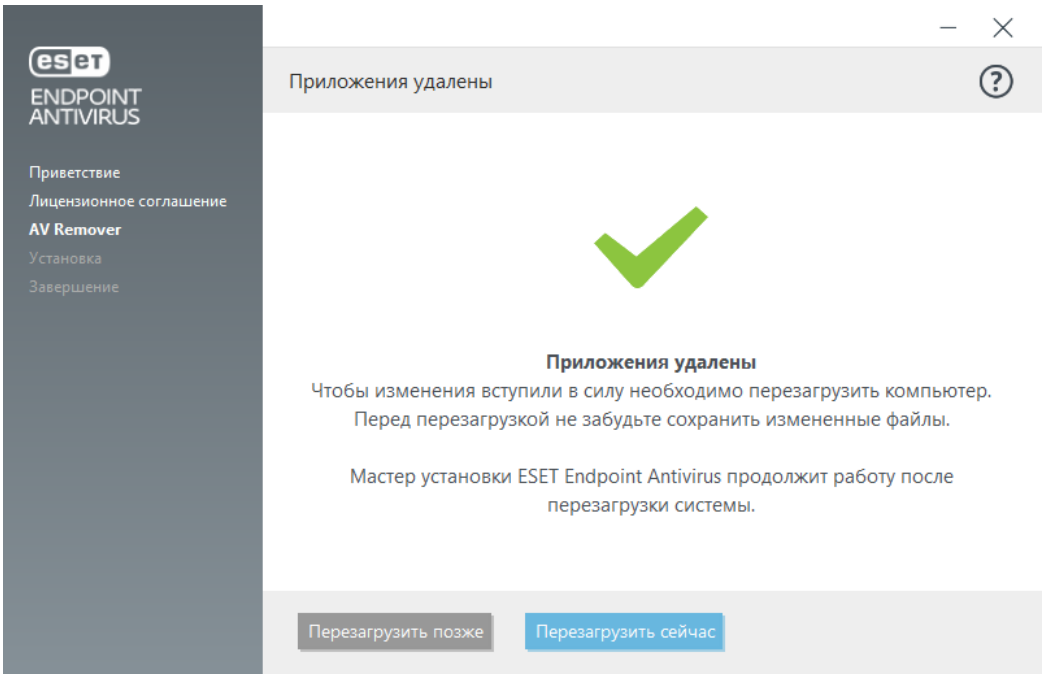
4. Выберите все обнаруженные приложения и нажмите кнопку **Удалить**. Процедура удаления может занять некоторое время.



5. После завершения удаления нажмите кнопку **Продолжить**.



6. Чтобы изменения вступили в силу и продолжить установку ESET Endpoint Antivirus, перезагрузите компьютер. Если во время удаления произошла ошибка, см. раздел настоящего руководства Ошибка во время удаления с помощью средства ESET AV Remover.



3.1.2 Ошибка во время удаления с помощью средства ESET AV Remover

Если удалить антивирусную программу с помощью ESET AV Remover не удалось, появится сообщение, что средство ESET AV Remover, возможно, не поддерживает удаляемое приложение. Чтобы узнать, можно ли удалить эту программу, просмотрите список поддерживаемых продуктов или программ удаления распространенного антивирусного ПО для Windows. Эти списки можно найти в базе знаний ESET.

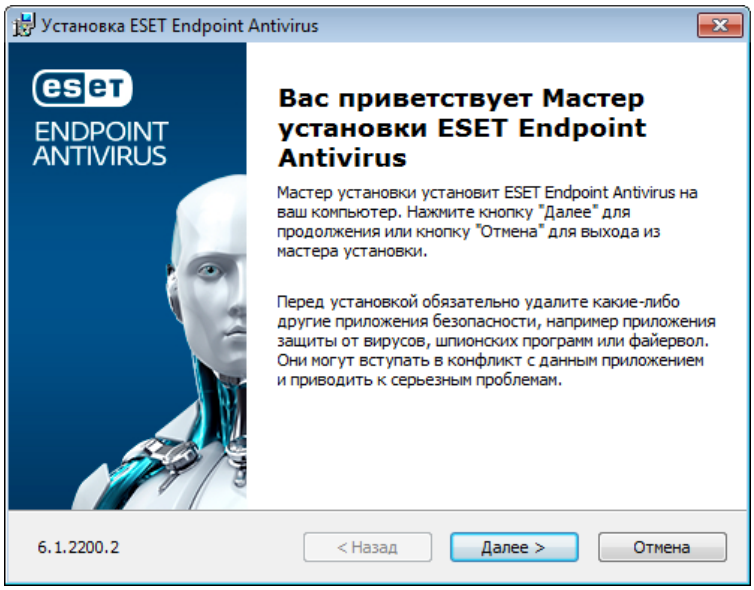
Если удалить продукт для обеспечения безопасности не удалось или некоторые из его компонентов были удалены частично, появится предложение перезагрузить компьютер и повторно выполнить сканирование. После перезагрузки появится предупреждение системы контроля учетных записей. Разрешите запуск программы, повторно просканируйте систему и удалите имеющиеся антивирусные приложения.

В случае необходимости обратитесь в службу поддержки клиентов ESET, создайте запрос на обслуживание и приготовьте файл **AppRemover.log** (он потребуется специалистам ESET). Файл **AppRemover.log** расположен в папке **eset**. Эта папка хранится в расположении *%TEMP%*. Для доступа к нему используйте проводник Windows. Сотрудники службы поддержки клиентов ESET свяжутся с вами, как только появится возможность.

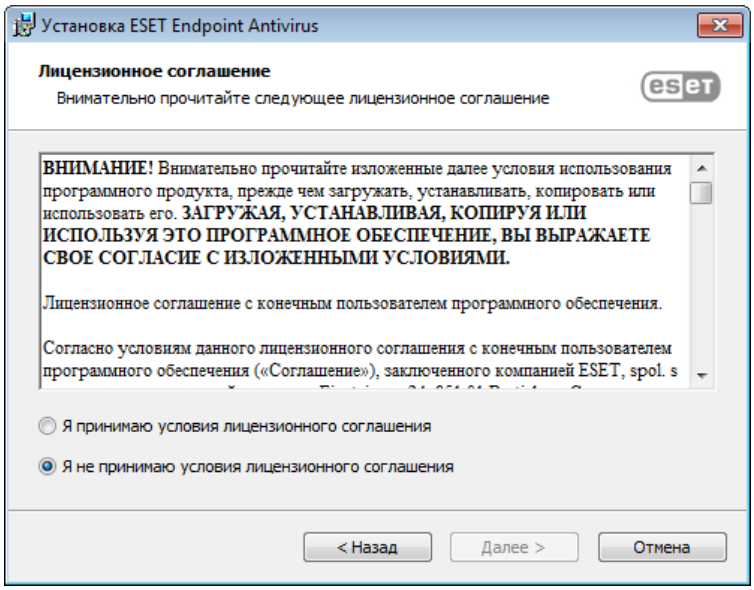
3.2 Установка

После запуска программы установки мастер установки поможет установить программу.

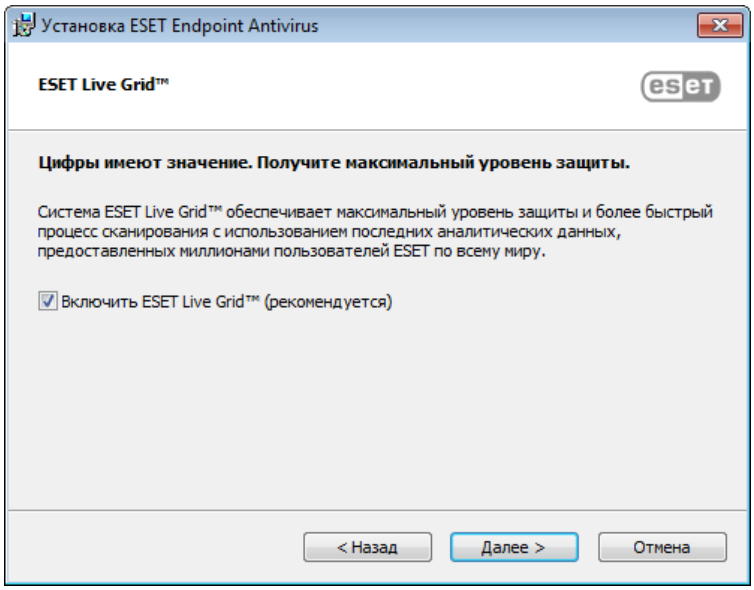
ВАЖНО!
Убедитесь в том, что на компьютере не установлены другие программы защиты от вирусов. Если на одном компьютере установлено два и более решения для защиты от вирусов, между ними может возникнуть конфликт. Рекомендуется удалить все прочие программы защиты от вирусов с компьютера. Список инструментов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



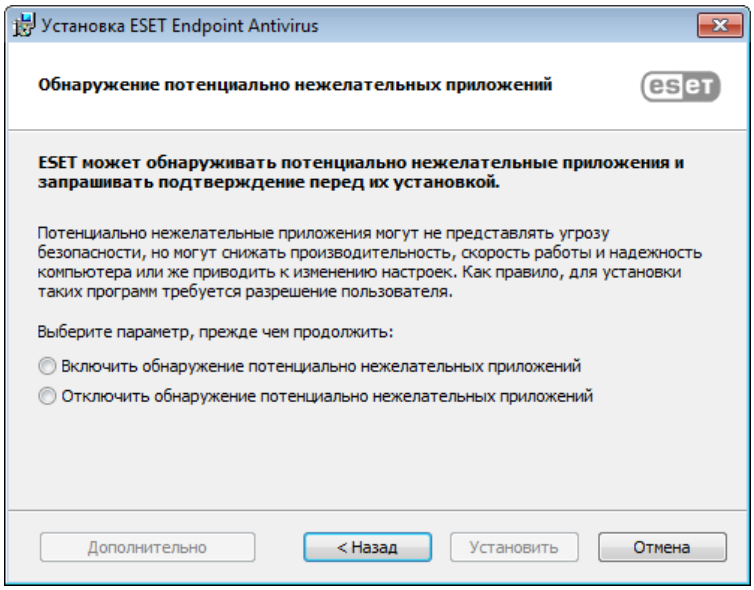
На следующем этапе на экран будет выведено лицензионное соглашение с конечным пользователем. Прочтите его и нажмите кнопку **Принять**, чтобы подтвердить свое согласие с его условиями. Приняв условия, нажмите кнопку **Далее**, чтобы продолжить установку.



После выбора варианта «Я принимаю...» и нажатия кнопки **Далее** на экран будет выведен запрос на включение ESET Live Grid. ESET Live Grid дает возможность незамедлительно и постоянно информировать компанию ESET о новых заражениях, благодаря чему мы можем защищать своих клиентов более качественно. Эта система позволяет отправлять новые угрозы в вирусную лабораторию ESET, где они анализируются, обрабатываются и добавляются в базу данных сигнатур вирусов.



Следующий шаг установки: следует настроить обнаружение потенциально нежелательных приложений, которые — хоть и не обязательно зловредные — могут негативно повлиять на поведение ОС. Дополнительные сведения см. в главе Потенциально нежелательные приложения. Доступ к дополнительным настройкам можно получить, нажав **Дополнительные настройки** (это может понадобиться, например, чтобы указать определенную папку для установки приложения ESET или чтобы включить автоматическое сканирование после установки).



Последний шаг: подтверждение установки. Для этого нужно нажать **Установить**.

3.2.1 Расширенная установка

При расширенной установке можно настроить ряд параметров установки, которые при стандартной установке недоступны.

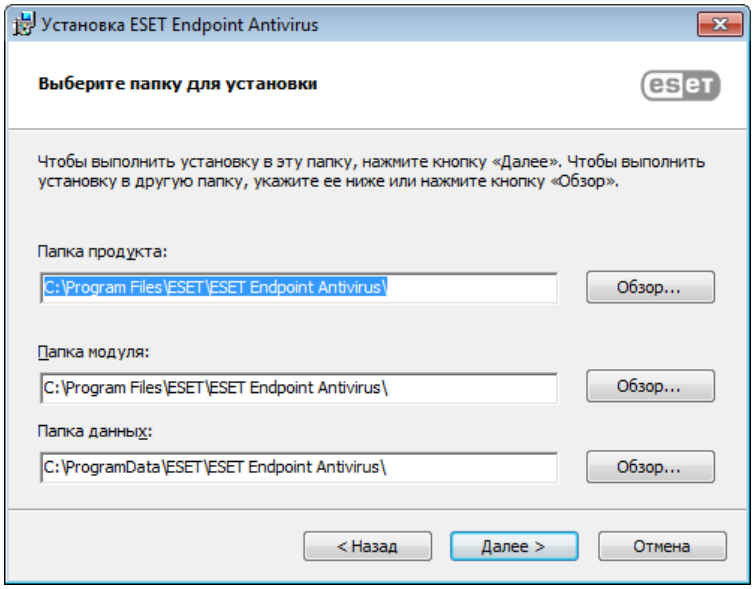
Когда вы включите обнаружение потенциально нежелательных приложений и нажмете **Дополнительные настройки**, вам будет предложено выбрать расположение для папки установки продукта. По умолчанию программа устанавливается в указанную ниже папку.

C:\Program Files\ESET\ESET Endpoint Antivirus

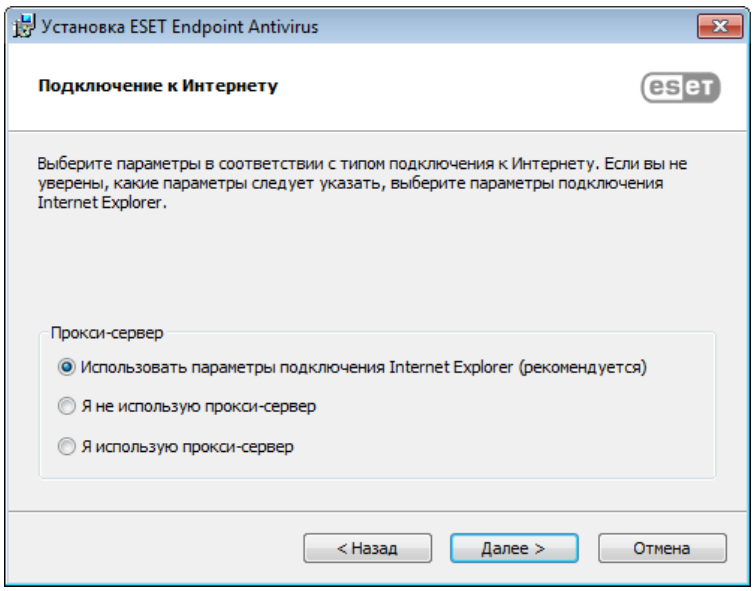
Можно указать расположение для модулей и данных программы. По умолчанию они устанавливаются в указанные ниже папки (в том же порядке):

C:\Program Files\ESET\ESET Endpoint Antivirus
C:\ProgramData\ESET\ESET Endpoint Antivirus

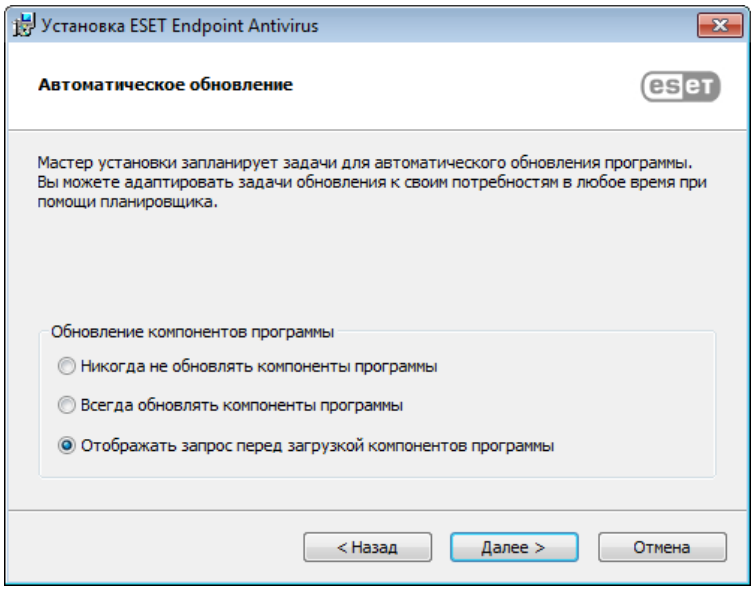
Нажмите кнопку **Обзор...**, чтобы изменить расположения (не рекомендуется).



Для настройки параметров прокси-сервера выберите вариант **Я использую прокси-сервер** и нажмите кнопку **Далее**. Введите IP-адрес или URL-адрес прокси-сервера в поле **Адрес**. Если вы не уверены, что для подключения к Интернету используется прокси-сервер, выберите параметр **Использовать параметры подключения Internet Explorer (рекомендуется)** и нажмите кнопку **Далее**. Если прокси-сервер не используется, выберите вариант **Я не использую прокси-сервер**. Для получения дополнительных сведений см. раздел Прокси-сервер.

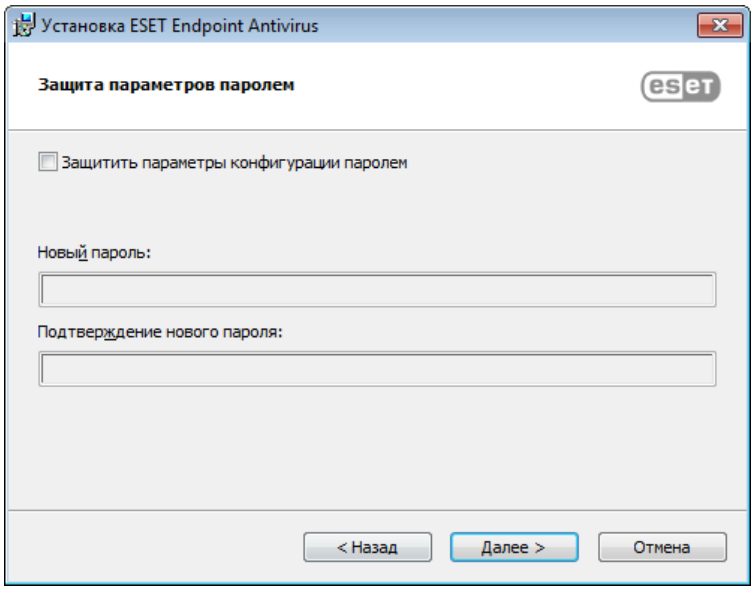


При выборочной установке можно указать, как должно происходить автоматическое обновление системы. Нажмите **Изменить...** для доступа к дополнительным параметрам.

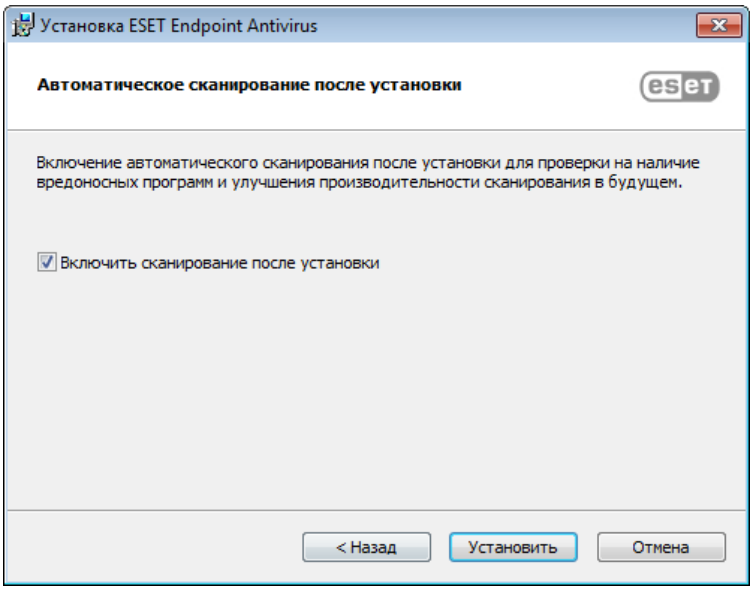


Если нет необходимости обновлять компоненты программы, выберите вариант **Никогда не обновлять компоненты программы**. Выберите параметр **Запросить подтверждение перед загрузкой компонентов**, чтобы перед каждой попыткой загрузить компоненты программы отображалось окно подтверждения. Для автоматической загрузки обновлений для компонентов программы выберите вариант **Всегда обновлять компоненты программы**.

В следующем окне предлагается создать пароль для защиты параметров программы. Выберите вариант **Защитить параметры конфигурации паролем** и введите пароль в поля **Новый пароль** и **Подтвердить новый пароль**. Он будет необходим для доступа к параметрам ESET Endpoint Antivirus, а также для их изменения. Когда в обоих полях введены совпадающие пароли, нажмите кнопку **Далее**, чтобы продолжить.



Чтобы отключить сканирование после установки, которое обычно выполняется после завершения установки, снимите флажок рядом с пунктом **Включить сканирование после установки**.



Нажмите кнопку **Установить**, чтобы начать установку.

3.3 Установка продукта с помощью ERA (командная строка)

Все приведенные ниже параметры предназначены для использования только с уровнями интерфейса **сокращенный**, **основной и отсутствующий**. Соответствующие параметры командной строки см. в документации для версии **msiexec**.

Поддерживаемые параметры:

APPDIR=<путь>
- Путь — действительный путь к каталогу.
- Каталог установки приложения.
- Например: `ees_nt64_ENU.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

APPDATADIR=<путь>
- Путь — действительный путь к каталогу.
- Каталог установки данных приложения.

MODULEDIR=<путь>
- Путь — действительный путь к каталогу.
- Каталог установки модуля.

ADDLOCAL=<список>
- Установка компонентов — список необязательных компонентов, которые нужно установить локально.
- Использование с пакетами MSI компании ESET: `ees_nt64_ENU.msi /qn ADDLOCAL=<list>`
- Дополнительные сведения о свойстве ADDLOCAL см. на странице http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx.

Правила

- **Список ADDLOCAL** — это разделенный запятыми список имен всех функций, которые нужно установить.
- При выборе функции, которую нужно установить, в список нужно добавить весь путь (указать все родительские функции).
- Чтобы все сделать верно, см. дополнительные правила.

Наличие функции

- **Обязательная**: функция будет установлена в любом случае.
- **Необязательная**: выбор функции можно отменить, чтобы не устанавливать ее.
- **Невидимая**: логическая функция, необходимая для правильной работы других функций.
- **Заполнитель**: функция, которая никак не влияет на продукт и которую нужно указать с подчиненными функциями.

Ниже представлено дерево функций Endpoint 6.1.

Дерево функций	Имя функции	Наличие функции
Компьютер	Компьютер	Обязательная
Компьютер/Защита от вирусов и шпионских программ	Защита от вирусов	Обязательная
Компьютер/Защита от вирусов и шпионских программ > Защита файловой системы в режиме реального времени	Защита в режиме реального времени	Обязательная
Компьютер/Защита от вирусов и шпионских программ > Сканирование компьютера	Сканирование	Обязательная
Компьютер/Защита от вирусов и шпионских программ > Защита документов	Защита документов	Необязательная
Компьютер/Контроль устройств	Контроль устройств	Необязательная
Сеть	Сеть	Заполнитель
Сеть/Персональный файервол	Файервол	Необязательная
Интернет и электронная почта	Интернет и электронная почта	Заполнитель
Интернет и фильтрация протоколов электронной почты	Фильтрация протоколов	Невидимая
Интернет и электронная почта/Защита доступа в Интернет	Защита доступа в Интернет	Необязательная
Интернет и электронная почта/Защита почтового клиента	Защита почтового клиента	Необязательная
Интернет и электронная почта/Защита почтового клиента/Почтовые модули	Почтовые модули	Невидимая
Интернет и электронная почта/Защита почтового клиента/Защита от спама	Защита от спама	Необязательная
Интернет и электронная почта/Контроль доступа в Интернет	Контроль доступа в Интернет	Необязательная
Зеркало обновлений	Зеркало обновлений	Необязательная
Поддержка технологии NAP (защиты доступа к сети) от Microsoft	Защита доступа к сети Microsoft	Необязательная

Дополнительные правила

- Если выбрана и будет устанавливаться функция или функции **Интернет и электронная почта**, нужно явным образом добавить в список невидимую функцию **Фильтрация протоколов**.
- Если выбрана и будет устанавливаться подчиненная функция или функции Защита почтового клиента**, нужно явным образом добавить в список невидимую функцию** Почтовые модули**.**

Примеры

```
ees_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,WebAccessProtection,ProtocolFiltering
```

```
ees_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,EmailClientProtection,Antispam,MailPlugins
```

Список свойств CFG_:

CFG_POTENTIALLYUNWANTED_ENABLED=1/0
• 0 — отключено, 1 — включено
• Потенциально нежелательные приложения

CFG_LIVEGRID_ENABLED=1/0
• 0 — отключено, 1 — включено
• LiveGrid

FIRSTSCAN_ENABLE=1/0
• 0 — выключить, 1 — включить
• Запланировать новое первое сканирование после установки.

CFG_EPFW_MODE=0/1/2/3
• 0 — автоматически, 1 — интерактивный режим, 2 — политика, 3 — обучение

CFG_PROXY_ENABLED=0/1
• 0 — отключено, 1 — включено

CFG_PROXY_ADDRESS=<IP-адрес>
• IP-адрес прокси-сервера.

CFG_PROXY_PORT=<порт>
• Номер порта прокси-сервера.

CFG_PROXY_USERNAME=<имя пользователя>
• Имя пользователя для проверки подлинности.

CFG_PROXY_PASSWORD=<пароль>
• Пароль для аутентификации.

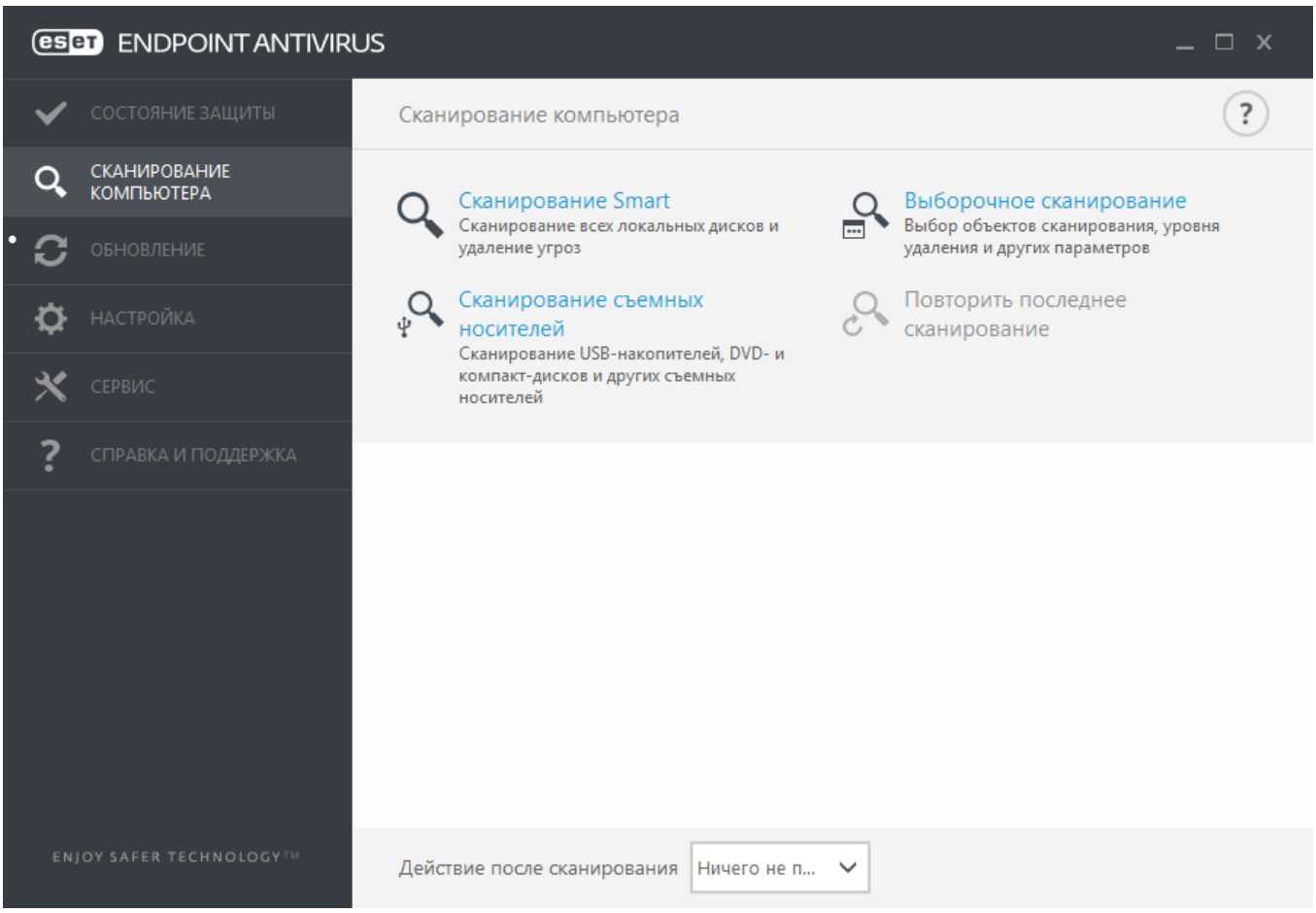
3.4 Активация программы

После завершения установки вам будет предложено активировать установленный продукт.

Выберите доступный метод активации ESET Endpoint Antivirus. См. раздел Активация ESET Endpoint Antivirus для получения дополнительных сведений.

3.5 Сканирование компьютера

В течение 15 минут после завершения установки (возможно, понадобится перезагрузка компьютера) приложение ESET Endpoint Antivirus выполнит сканирование компьютера. Кроме того, чтобы проверять компьютер на наличие угроз, рекомендуется регулярно сканировать компьютер вручную или запланировать регулярное сканирование. В главном окне программы выберите пункт **Сканирование компьютера**, а затем — **Сканирование Smart**. Для получения дополнительных сведений о сканировании компьютера см. раздел Сканирование компьютера.



3.6 Обновление до новой версии

Новые версии ESET Endpoint Antivirus выпускаются для реализации улучшений или исправления проблем, которые не могут быть устранены автоматическим обновлением модулей программы. Обновление до 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 конфигурации компьютеров, 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.
2. Вручную путем загрузки и установки новой версии поверх предыдущей.
3. Вручную с автоматическим развертыванием в сетевой среде посредством ESET Remote Administrator.

3.7 Руководство для начинающих

В этом разделе приводятся общие сведения о программном обеспечении ESET Endpoint Antivirus и его основных параметрах.

3.7.1 Пользовательский интерфейс

Главное окно ESET Endpoint Antivirus разделено на две основные части. Основное окно справа содержит информацию, относящуюся к параметру, выбранному в главном меню слева.

Ниже описаны пункты главного меню.

Состояние защиты - этот пункт предоставляет информацию о состоянии защиты ESET Endpoint Antivirus.

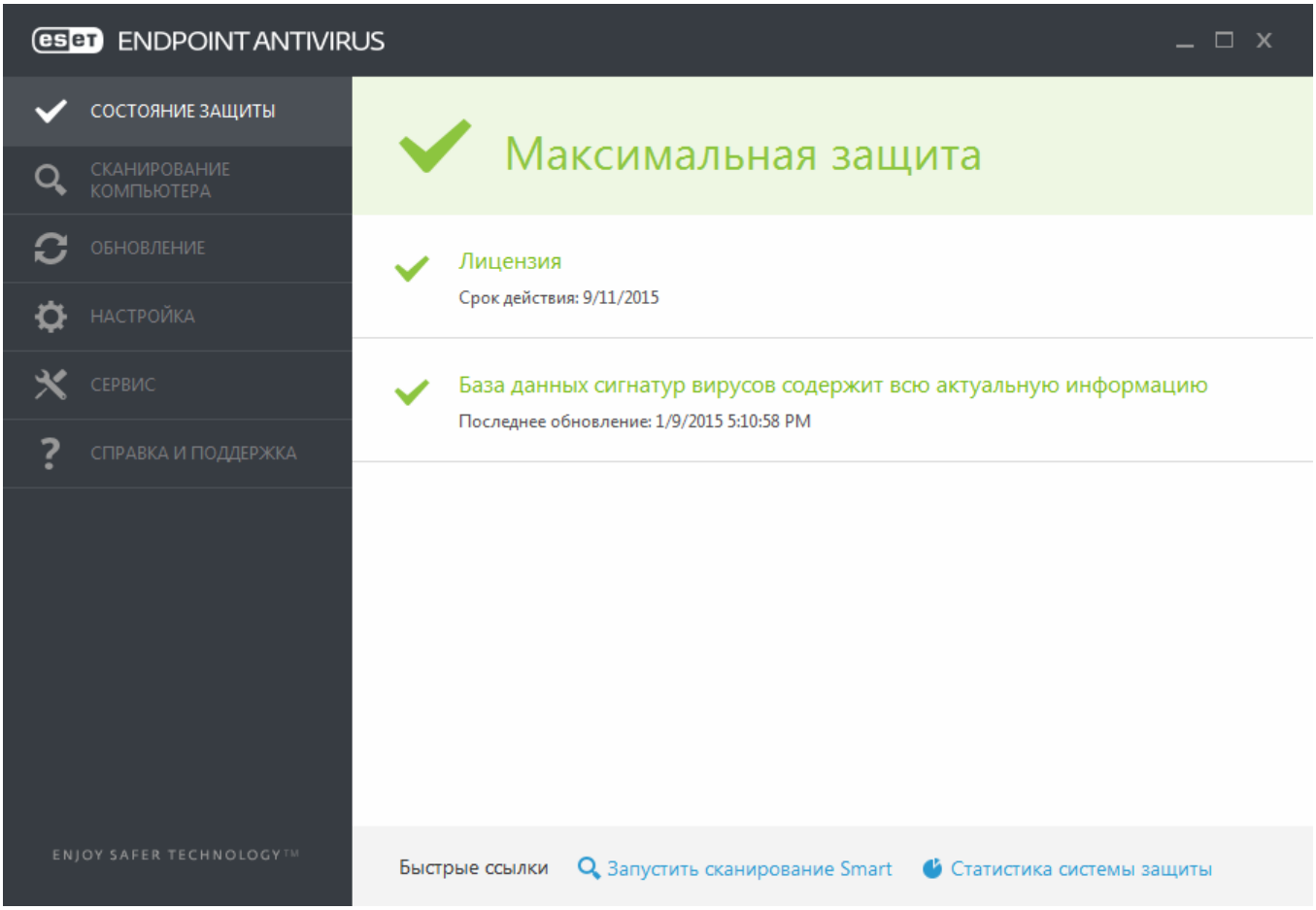
Сканирование компьютера - этот параметр позволяет настроить и запустить сканирование Smart, выборочное сканирование и сканирование съемных носителей. Также можно повторно запустить последнюю операцию сканирования.

Обновление - отображение информации о базе данных сигнатур вирусов.

Настройка - настройка параметров безопасности компьютера Интернета и электронной почты.

Служебные программы - доступ к файлам журнала, статистике защиты, программам мониторинга, запущенным процессам, планировщику, карантину , ESET SysInspector и ESET SysRescue для создания компакт-диска аварийного восстановления. Также можно отправить образец на анализ.

Справка и поддержка: доступ к файлам справки, базе знаний ESET и веб-сайту компании ESET. Также доступны ссылки на форму запроса в службу поддержки клиентов, средства поддержки и информацию об активации продукта.

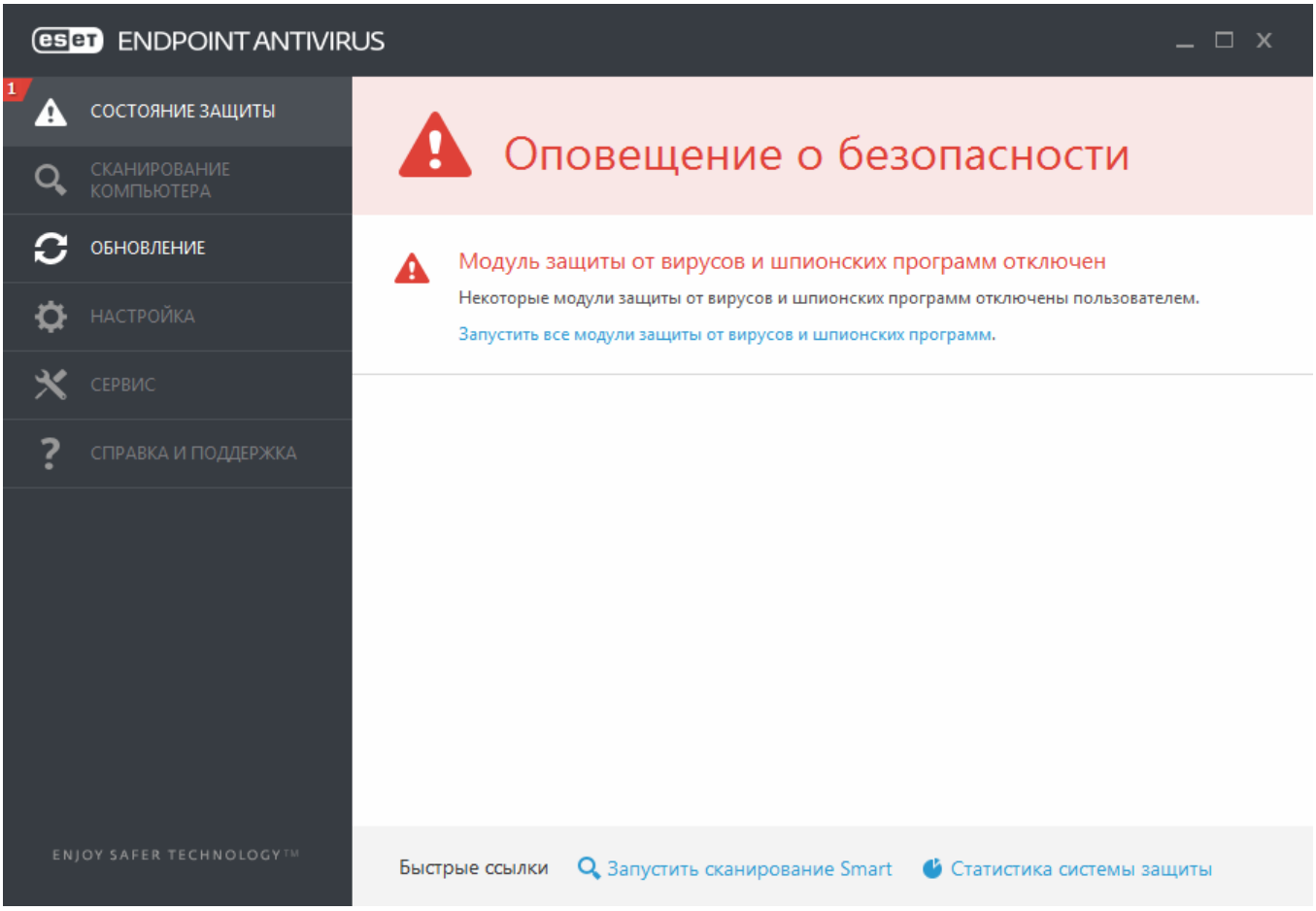


Окно **Состояние защиты** информирует пользователя об уровне безопасности и текущем уровне защиты компьютера. Зеленый значок **Максимальная защита** означает, что обеспечивается максимальная степень защиты.

В окне состояния также отображаются ссылки на часто используемые функции программы ESET Endpoint Antivirus, а также информация о последнем обновлении.

Действия, которые следует выполнить, если программа не работает надлежащим образом

Зеленая галочка отображается рядом со всеми программными модулями, которые полноценно функционируют. Красный восклицательный знак или оранжевый значок уведомления отображается, если модуль требует внимания. В верхней части окна выводятся дополнительные сведения о модуле, включая нашу рекомендацию о том, как восстановить полную функциональность. Для того чтобы изменить состояние модуля, выберите в главном меню пункт **Настройка** и щелкните нужный модуль.



 Красный восклицательный знак (!) указывает, что максимальная степень защиты компьютера не обеспечивается. Этот тип уведомления может наблюдаться в следующих сценариях:

- **Защита от вирусов и шпионских программ приостановлена**: щелкните **Запустить все модули защиты от вирусов и шпионских программ**, чтобы повторно включить защиту от вирусов и шпионских программ на панели **Состояние защиты** или **Включить защиту от вирусов и шпионских программ** на панели **Настройка** в главном окне программы.
- **Защита от вирусов не работает**: ошибка инициализации модуля сканирования на наличие вирусов. Большинство модулей ESET Endpoint Antivirus не будут функционировать должным образом.
- **Защита от фишинга не работает**: эта функция не работает, так как не активны другие нужные модули программы.
- **База данных сигнатур вирусов устарела**: программа использует устаревшую базу данных сигнатур вирусов. Обновите базу данных сигнатур вирусов.
- **Продукт не активирован** или **Срок действия лицензии истек**: об этих проблемах свидетельствует красный значок состояния защиты. С этого момента программа больше не сможет выполнять обновления. Чтобы продлить лицензию, рекомендуется выполнить инструкции в окне предупреждения.
- **Система предотвращения вторжений на узел (HIPS) отключена**: эта проблема указывается, если система HIPS отключена в разделе «Дополнительные настройки». Компьютер не защищен от некоторых типов угроз, и следует немедленно повторно включить защиту, нажав **Включить систему HIPS**.
- **Функция ESET Live Grid отключена**: эта проблема указывается, если функция ESET Live Grid отключена в разделе «Дополнительные настройки».
- **Регулярные обновления не запланированы**: ESET Endpoint Antivirus не будет проверять наличие важных обновлений и получать их, если не запланировать задачу обновления.
- **Защита Anti-Stealth отключена**: нажмите **Включить защиту Anti-Stealth**, чтобы повторно включить эту функцию.
- **Защита файловой системы в режиме реального времени приостановлена**: защита в режиме реального времени была отключена пользователем. Компьютер не защищен от угроз. Нажмите **Включить защиту в режиме реального времени**, чтобы повторно включить эту функцию.

 Оранжевый знак «i» указывает на то, что продукт ESET требует вашего внимания в связи с некритичной проблемой. Ниже указаны возможные причины.

- **Защита доступа в Интернет отключена**: щелкните уведомление о защите, чтобы повторно включить защиту доступа в Интернет, а затем щелкните **Включить защиту доступа в Интернет**.
- **Срок действия лицензии скоро закончится**: об этой проблеме свидетельствует появление восклицательного знака на значке состояния защиты. После окончания срока действия лицензии программа больше не сможет выполнять обновления, а значок состояния защиты станет красным.
- **Защита от спама приостановлена**: щелкните **Включить защиту от спама**, чтобы повторно включить эту функцию.
- **Контроль доступа в Интернет приостановлен**: щелкните **Включить контроль доступа в Интернет**, чтобы повторно включить эту функцию.
- **Действует переопределение политики**: конфигурация, заданная политикой, временно переопределена, возможно до завершения устранения неполадок. Параметры политики может переопределить только авторизованный пользователь. Дополнительные сведения см. в разделе Использование режима переопределения.
- **Контроль устройств приостановлен**: щелкните **Включить контроль устройств**, чтобы повторно включить эту функцию.

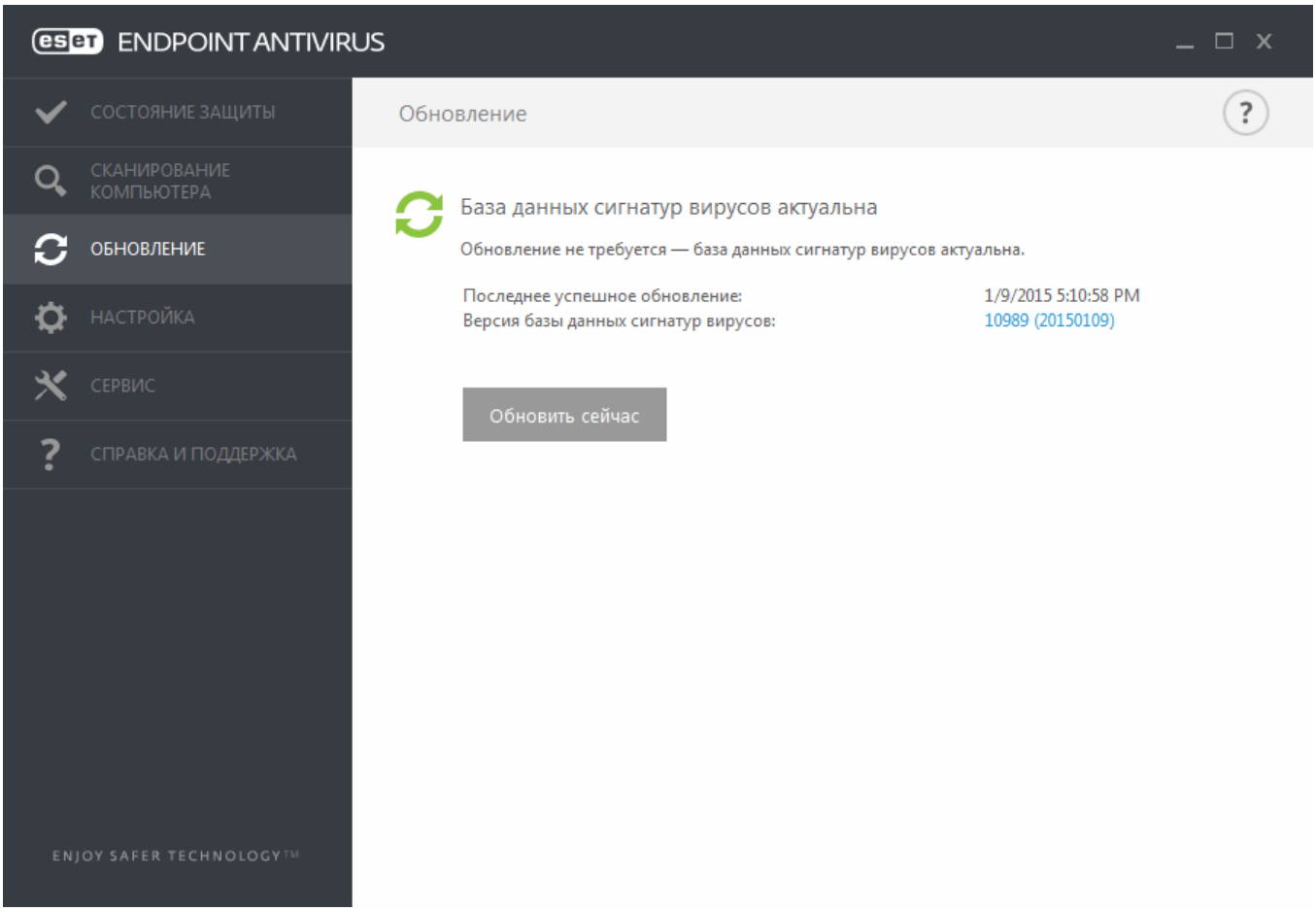
Если предложенные решения не позволяют устранить проблему, выберите пункт **Справка и поддержка** и просмотрите файлы справки или поищите нужную информацию в базе знаний ESET. Если вам по-прежнему нужна помощь, отправьте свой запрос в службу поддержки клиентов ESET. Ее специалисты оперативно ответят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

ПРИМЕЧАНИЕ.
Если состояние относится к функции, заблокированной политикой ERA, ссылка будет неактивна.

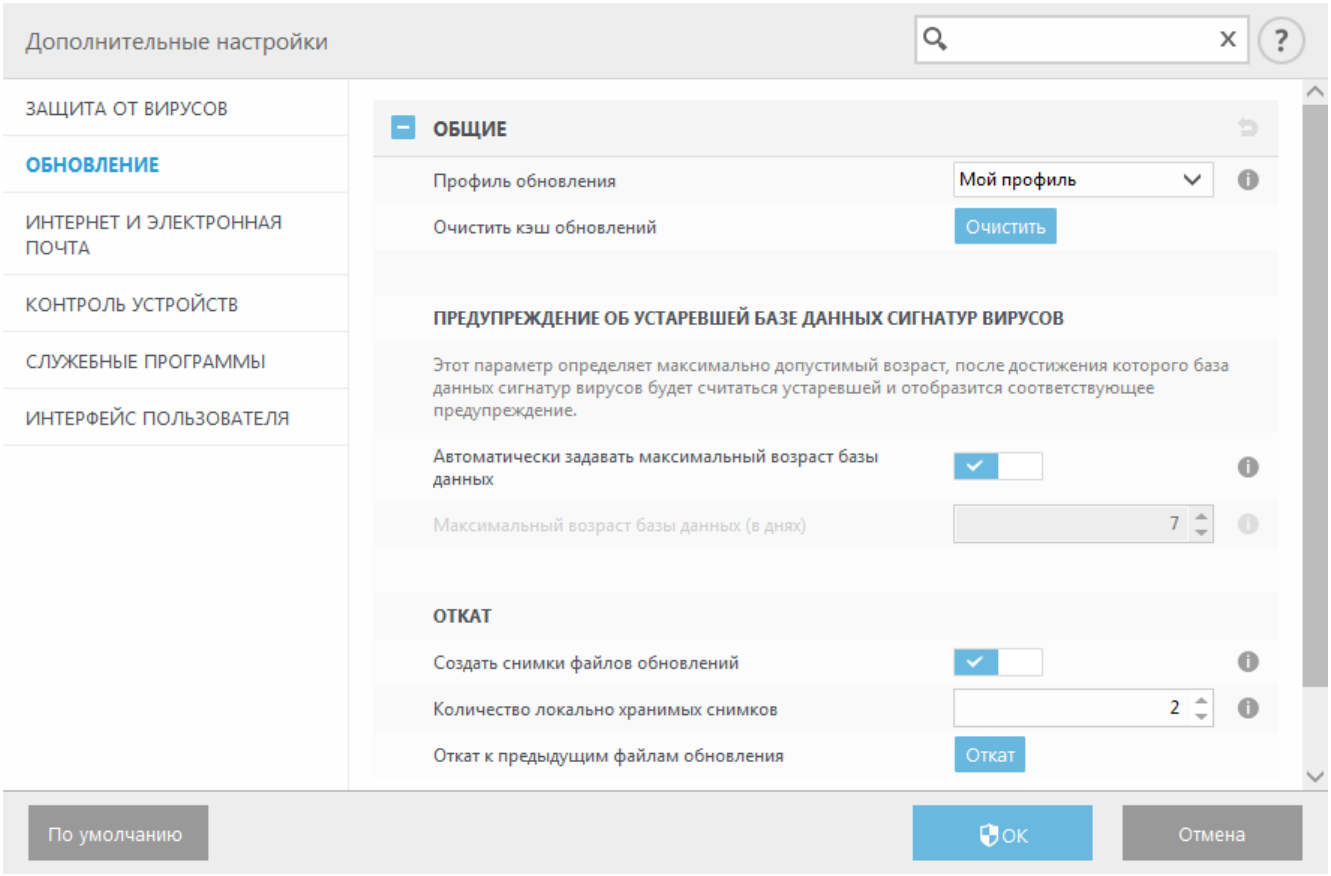
3.7.2 Настройка обновлений

Обновление базы данных сигнатур вирусов и компонентов программы является важнейшей частью обеспечения полной защиты компьютера от вредоносного кода. Уделите особенное внимание изучению конфигурации и работы этого процесса. В главном меню выберите **Обновление** > **Обновить**, чтобы проверить наличие обновлений базы данных.

Если **Лицензионный ключ** не был введен, обновление будет невозможно. Взамен вам будет предложено активировать продукт.



В окне «Дополнительные настройки» (в главном меню выберите **Настройка** > **Дополнительные настройки** или нажмите **F5** на клавиатуре) содержатся расширенные параметры обновления. Чтобы настроить расширенные параметры обновления, такие как режим обновления, доступ через прокси-сервер, подключения к локальной сети и настройки создания копий сигнатур вирусов, щелкните в дереве расширенных параметров пункт **Обновление**. При возникновении проблем с обновлением нажмите кнопку **Очистить**, чтобы удалить из кэша временные файлы обновления. По умолчанию в меню **Сервер обновлений** выбран параметр **Автоматический выбор**. При использовании сервера ESET рекомендуется активировать параметр **Выбирать автоматически**. Чтобы отключить отображение уведомлений на панели задач в правом нижнем углу экрана, выберите элемент **Отключить уведомления о завершении обновления**.



Для того чтобы использовать программу наилучшим образом, необходимо включить ее автоматическое обновление. Это возможно только в случае, если в разделе **Справка и поддержка** > **Активировать продукт** указан правильный **Лицензионный ключ**.

Вы можете ввести **лицензионный ключ** сразу после установки или в любое другое время. Дополнительные сведения об активации см. в статье Активация ESET Endpoint Antivirus. Учетные данные, полученные вместе с продуктом ESET для обеспечения безопасности, необходимо ввести в окне **Сведения о лицензии**.

3.8 Часто задаваемые вопросы

Эта глава содержит ответы на некоторые из наиболее часто задаваемых вопросов и решения проблем пользователей. Щелкните ссылку на тему, которая соответствует вашей проблеме.

Обновление ESET Endpoint Antivirus
Активация ESET Endpoint Antivirus
Активация нового продукта с использованием текущих учетных данных
Удаление вируса с компьютера
Создание задачи в планировщике
Планирование задачи сканирования (каждые 24 часа)
Подключение продукта к ESET Remote Administrator
Настройка зеркала

Если перечисленные выше разделы справки не дали ответа на ваш вопрос, попробуйте поискать по ключевым

словам или фразе, которые описывают проблему, в разделах справки ESET Endpoint Antivirus.

Если с помощью справки не удалось решить проблему или вопрос, посетите базу знаний ESET, в которой есть ответы и решения для самых распространенных ситуаций.

Удаление троянской программы Sirefef (ZeroAccess)?
Контрольный список для устранения проблем при обновлении с зеркала
Адреса и порты, которые необходимо открыть в стороннем файерволе для обеспечения полноценной работы продуктов ESET

При необходимости направьте свои вопросы в нашу онлайн-службу технической поддержки. К ссылке на контактную веб-форму можно получить на панели **Справка и поддержка** в главном окне программы.

3.8.1 Обновление программы ESET Endpoint Antivirus

Обновлять ESET Endpoint Antivirus можно вручную или автоматически. Чтобы запустить обновление, выберите команду **Обновить сейчас** в разделе **Обновление**.

При установке программы с параметрами по умолчанию создается задача автоматического обновления. Она запускается каждый час. Чтобы изменить интервал, последовательно выберите **Сервис** > **Планировщик** (дополнительную информацию о планировщике см. здесь).

3.8.2 Активация ESET Endpoint Antivirus

После завершения установки вам будет предложено активировать установленный продукт.

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

Чтобы активировать ESET Endpoint Antivirus непосредственно из программы, щелкните в области уведомлений значок и выберите в меню пункт **Активируйте лицензию на программный продукт**. Активацию продукта также можно выполнить, последовательно щелкнув в главном меню элементы **Справка и поддержка** > **Активировать продукт** или **Состояние защиты** > **Активировать продукт**.

Для активации ESET Endpoint Antivirus можно воспользоваться любым из перечисленных ниже методов.

- **Лицензионный ключ**: уникальная строка в формате XXXX-XXXX-XXXX-XXXX-XXXX, которая используется для идентификации владельца и активации лицензии.
- **Учетная запись администратора безопасности** - учетная запись, созданная на портале ESET License Administrator с использованием учетных данных (адрес электронной почты и пароль). Этот метод позволяет централизовано управлять несколькими лицензиями.
- **Офлайн-лицензии** - автоматически созданный файл со сведениями о лицензии, который передается в продукт ESET. Если лицензия позволяет загрузить автономный файл лицензии (.lf), его можно использовать для автономной активации. Количество офлайн-лицензий будет вычтено из общего количества доступных лицензий. Дополнительные сведения о создании автономного файла см. в руководстве пользователя ESET License Administrator.

Щелкните элемент **Активировать позже**, если компьютер является участником управляемой сети и администратор выполнит удаленную активацию через программу ESET Remote Administrator. Этот параметр можно использовать и в тех случаях, когда нужно активировать клиент позже.

Если у вас есть имя пользователя и пароль, но вы не знаете, как активировать ESET Endpoint Antivirus, щелкните **У меня есть имя пользователя и пароль. Что мне делать?** Отобразится экран ESET License Administrator. Здесь вы сможете преобразовать учетные данные в лицензионный ключ.

Изменить лицензию на продукт можно в любое время. Для этого щелкните **Справка и поддержка** > **Управление лицензией** в главном окне программы. Отобразится открытый идентификатор лицензии, предназначенный для ее идентификации в службе поддержки ESET. Имя пользователя, под которым зарегистрирован компьютер, можно найти в разделе **О программе** (на панели задач щелкните значок правой кнопкой мыши).

ПРИМЕЧАНИЕ.
Приложение ESET Remote Administrator может активировать клиентские компьютеры в автоматическом режиме, используя предоставленные администратором лицензии. Инструкции см. в руководстве пользователя по ESET Remote Administrator.

3.8.3 Активация нового продукта с использованием текущих учетных данных

Если у вас уже есть имя пользователя и пароль и вы желаете получить лицензионный ключ, посетите портал ESET License Administrator. На портале учетные данные можно преобразовать в лицензионный ключ.

3.8.4 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. Нажмите **Сканирование Smart**, чтобы запустить сканирование компьютера.
3. После завершения сканирования просмотрите журнал на предмет количества проверенных, зараженных и очищенных файлов.
4. Если необходимо проверить только определенную часть диска, щелкните элемент **Выборочное сканирование** и укажите объекты, которые следует просканировать на наличие вирусов.

Дополнительные сведения см. в нашей регулярно обновляемой статье базы знаний ESET.

3.8.5 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.
- **Первое сканирование** - по умолчанию через 20 минут после установки или перезагрузки выполняется сканирование компьютера как задание с низким приоритетом.
- **Обновление** - планирование задачи обновления, в рамках которой обновляется база данных сигнатур вирусов и программные модули.

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 указанные ниже 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**).

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.

3.8.6 Планирование задачи сканирования (каждые 24 часа)

Чтобы запланировать регулярную задачу, откройте главное окно программы и выберите **Служебные программы** > **Планировщик**. Ниже приведено краткое описание процедуры планирования задачи, которая будет сканировать локальные диски каждые 24 часа.

Для того чтобы запланировать задачу сканирования, выполните следующие действия.

1. В главном окне планировщика нажмите **Добавить**.
2. В раскрывающемся меню выберите **Сканирование компьютера по требованию**.
3. Введите имя задачи и выберите **Многократно**.
4. Укажите, что задача должна выполняться каждые 24 часа.
5. Выберите действие, которое будет выполняться, если по какой-либо причине не удается выполнить запланированную задачу.
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.

3.8.7 Подключение ESET Endpoint Antivirus к ESET Remote Administrator

Если после установки ESET Endpoint Antivirus на компьютер вы хотите подключиться через ESET Remote Administrator, убедитесь, что на клиентской рабочей станции также установлен агент ERA. Агент ERA — важная составляющая каждого клиентского решения, которое подключается к серверу ERA. Для поиска компьютеров в сети ESET Remote Administrator использует компонент RD Sensor. Каждый компьютер в сети, найденный с помощью компонента RD Sensor, отображается в веб-консоли.

После развертывания агента вы можете удаленно устанавливать на клиентских компьютерах другие решения безопасности ESET. Подробное описание удаленной установки приведено в руководстве пользователя ESET Remote Administrator.

3.8.8 Настройка зеркала

ESET Endpoint Antivirus сконфигурирован для хранения копий файлов обновлений сигнатур вирусов и передачи обновлений на другие рабочие станции, использующее ESET Endpoint Security или ESET Endpoint Antivirus.

Настройка ESET Endpoint Antivirus для работы в качестве сервера зеркала для передачи обновлений через внутренний HTTP-сервер

Нажмите клавишу **F5**, чтобы получить доступ к дополнительным настройкам, и последовательно щелкните элементы **Обновление** > **Основные сведение**. Убедитесь, что для **Сервера обновлений** включен параметр **Автоматический выбор**. Выберите **Создать зеркало обновления** и **Передавать файлы обновления через внутренний HTTP-сервер** в **Дополнительные настройки** > **Обычная** > **Зеркало**.

Настройка сервера зеркала для передачи обновлений через общую сетевую папку

Создайте общую папку на локальном или сетевом устройстве. Папка должна быть открыта для чтения всеми пользователями решений для обеспечения безопасности ESET и для записи из локальной учетной записи системы. Активируйте элемент **Создать зеркало обновления**. Чтобы получить к нему доступ, последовательно щелкните элементы **Дополнительные настройки** > **Основные сведения** > **Зеркало**. Найдите и откройте созданную общую папку.

ПРИМЕЧАНИЕ
Если через внутренний HTTP-сервер обновления выполнять не нужно, снимите флажок **Передавать файлы обновления с помощью внутреннего сервера HTTP**.

3.8.9 Как мне обновить свою систему до Windows 10, если у меня установлен продукт ESET Endpoint Antivirus?

ВНИМАНИЕ!
Прежде чем выполнять обновление до Windows 10, настоятельно рекомендуется обновить продукт ESET до последней версии, а затем загрузить последнюю базу данных сигнатур вирусов. Во время обновления до Windows 10 это обеспечит максимальную защиту, а также сохранение настроек программы и сведений о лицензии.

Версия 6.x и более поздние версии:

Чтобы подготовиться к обновлению до Windows 10, загрузите и установите последнюю версию продукта, щелкнув соответствующую ссылку ниже.

Загрузить ESET Endpoint Security 6 (32-разрядная версия) Загрузить ESET Endpoint Antivirus 6 (32-разрядная версия)

Загрузить ESET Endpoint Security 6 (64-разрядная версия) Загрузить ESET Endpoint Antivirus 6 (64-разрядная версия)

Версия 5.x и более ранние версии:

Чтобы подготовиться к обновлению до Windows 10, загрузите и установите последнюю версию продукта, щелкнув соответствующую ссылку ниже.

Загрузить ESET Endpoint Security 5 (32-разрядная версия) Загрузить ESET Endpoint Antivirus 5 (32-разрядная версия)

Загрузить ESET Endpoint Security 5 (64-разрядная версия) Загрузить ESET Endpoint Antivirus 5 (64-разрядная версия)

Версии на других языках:

Если вы ищете версию продукта ESET для конечных точек на другом языке, посетите нашу страницу загрузок.

ПРИМЕЧАНИЕ.
Дополнительные сведения о совместимости продуктов ESET с Windows 10.

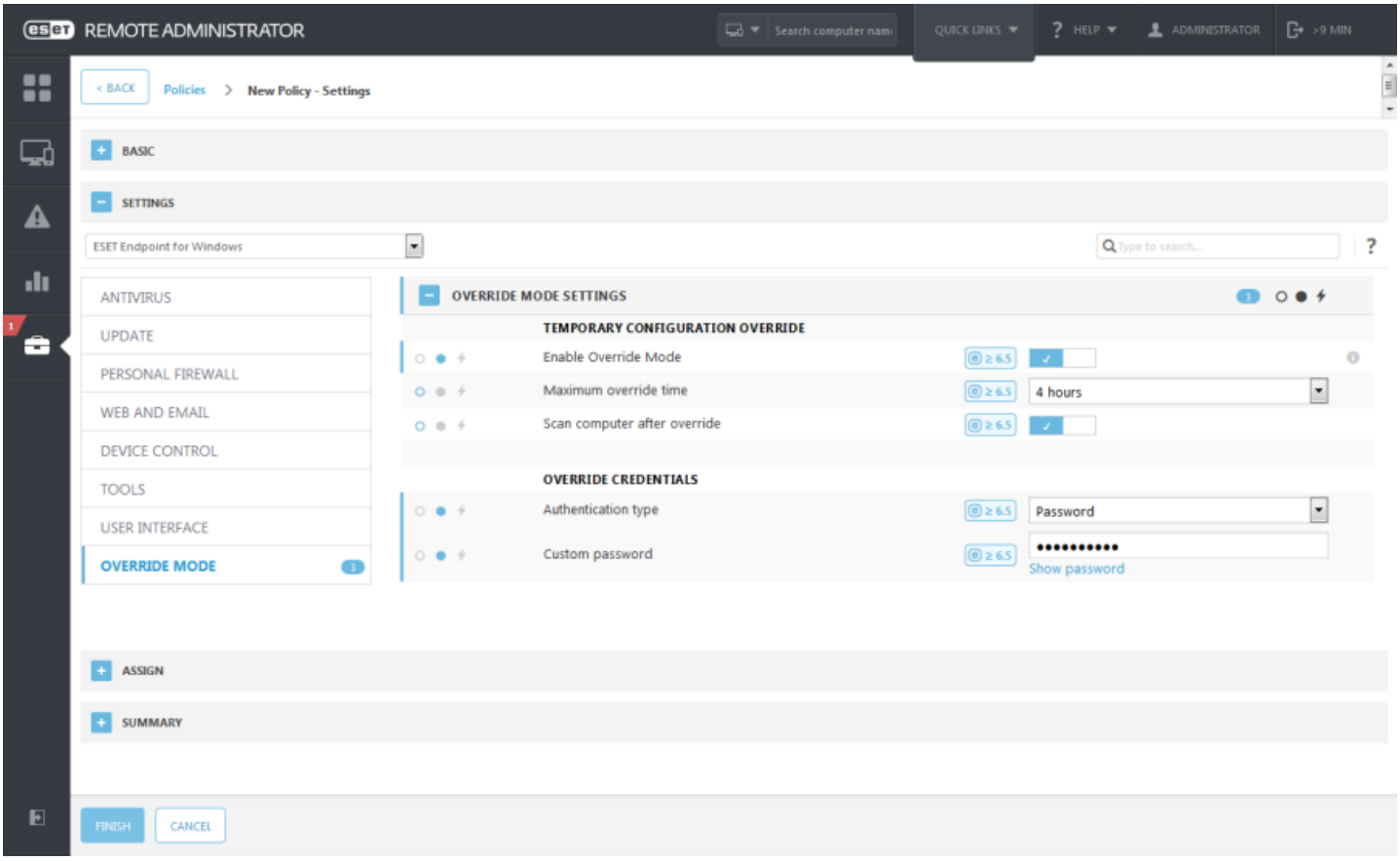
3.8.10 Использование режима переопределения

Пользователи, на компьютерах которых установлены продукты ESET Endpoint (версии 6.5 и выше) для Windows, могут воспользоваться функцией переопределения. Режим переопределения позволяет пользователям на уровне клиентского компьютера изменять настройки установленного продукта ESET, даже если поверх этих настроек применена та или иная политика. Режим переопределения можно включить для определенных пользователей AD или же защитить паролем. Эта функция не может быть включена более четырех часов подряд.

ВНИМАНИЕ!
Режим переопределения нельзя остановить из веб-консоли ERA после того, как он был включен. Переопределение отключается только по истечении времени переопределения или же после отключения на самом клиенте.

Чтобы задать **режим переопределения**, выполните следующие действия:

1. Перейдите в меню **Администратор** > **Политики** > **Создать политику**.
2. В разделе **Основная информация** введите **имя** и **описание** этой политики.
3. В разделе **Параметры** выберите **ESET Endpoint для Windows**.
4. Нажмите **Режим переопределения** и настройте правила этого режима.
5. В разделе **Назначить** выберите компьютер или группу компьютеров, к которым будет применена данная политика.
6. Проверьте настройки в режиме **Сводка** и нажмите кнопку **Готово**, чтобы применить политику.



ПОДСКАЗКА
Если у *Ивана* наблюдается проблема с параметрами конечной точки, блокирующими какую-либо важную функцию или доступ к Интернету на его компьютере, администратор может разрешить *Ивану* переопределить существующую политику конечной точки и настроить параметры вручную на своем компьютере. Впоследствии новые параметры могут быть запрошены системой ERA, чтобы администратор

мог создать на их основе новую политику.

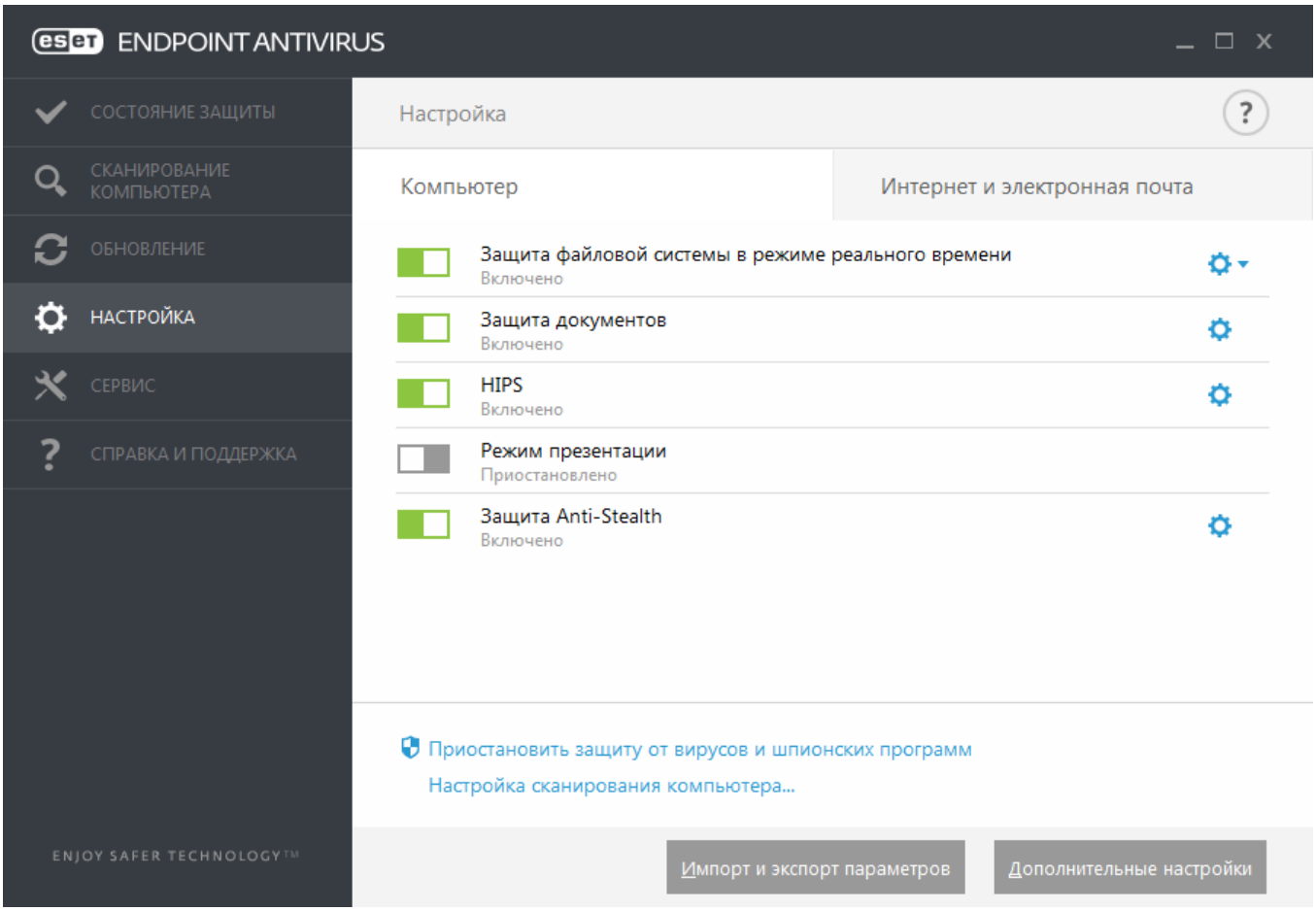
Для этого выполните следующие действия:

1. Перейдите в меню **Администратор** > **Политики** > **Создать политику**.
2. Заполните поля **Имя** и **Описание**. В разделе **Параметры** выберите **ESET Endpoint для Windows**.
3. Нажмите **Режим переопределения**, включите режим переопределения на один час и выберите пользователя AD *Иван*.
4. Назначьте политику *компьютеру Ивана* и нажмите кнопку **Готово**, чтобы сохранить политику.
5. *Иван* должен включить **режим переопределения** на своей конечной точке ESET и изменить параметры вручную на своем компьютере.
6. В веб-консоли ERA перейдите в раздел **Компьютеры**, выберите *Компьютер Ивана* и нажмите **Показать подробности**.
7. В разделе **Конфигурация** нажмите **Запросить конфигурацию**, чтобы запланировать клиентскую задачу для получения конфигурации от клиента как можно скорее.
8. Вскоре появится новая конфигурация. Щелкните продукт, параметры которого необходимо сохранить, а затем нажмите **Открыть конфигурацию**.
9. Можно просмотреть параметры, а затем нажать кнопку **Преобразовать в политику**.
10. Заполните поля **Имя** и **Описание**.
11. В разделе **Параметры** при необходимости можно изменить параметры.
12. В разделе **Назначить** можно назначить данную политику *компьютеру Ивана* (или другим).
13. Нажмите кнопку **Готово**, чтобы сохранить параметры.
14. Не забудьте удалить политику переопределения после того, как необходимость в ней исчезнет.

3.9 Работа с ESET Endpoint Antivirus

Параметры ESET Endpoint Antivirus дают пользователю возможность настраивать уровень защиты для компьютера, Интернета и электронной почты.

ПРИМЕЧАНИЕ.
При создании политики из веб-консоли ESET Remote Administrator можно выбрать флаг для каждого параметра. Параметры с флагом «Принудительно применить» имеют приоритет и не могут быть переопределены последующей политикой (даже если в ней установлен этот флажок). Это гарантирует, что данный параметр не будет изменен (например, пользователем или последующими политиками в ходе объединения). Дополнительные сведения см. в справке о флагах в ERA в Интернете.



Меню **Настройка** содержит следующие разделы.

- **Компьютер**
- **Интернет и электронная почта**

В настройках защиты **Компьютер** можно включать и отключать следующие компоненты:

- **Защита файловой системы в режиме реального времени**: все файлы сканируются на наличие злонамеренного кода во время их открытия, создания или запуска.
- **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.
- **HIPS**: система HIPS отслеживает события, происходящие в операционной системе, и реагирует на них в соответствии с настраиваемым набором правил.
- **Режим презентации**: функция для пользователей, которым необходимо отсутствие каких-либо перерывов при использовании программного обеспечения и отвлекающих внимание всплывающих окон, а также требуется свести к минимуму потребление ресурсов процессора. После включения Режима презентации на экран будет выведено предупреждение (о потенциальной угрозе безопасности), а для оформления главного окна будет применен оранжевый цвет.
- **Защита Anti-Stealth**: обеспечивает обнаружение опасных программ, например руткитов, способных скрывать свое присутствие от операционной системы. Это значит, что такие программы невозможно обнаружить с помощью обычных методов проверки.

В настройках защиты **Интернет и электронная почта** можно включать и отключать следующие компоненты:

- **Защита доступа в Интернет**: если этот параметр включен, весь трафик по протоколам HTTP и HTTPS сканируется на наличие вредоносных программ.
- **Защита почтового клиента**: обеспечивает контроль обмена данными по протоколам POP3 и IMAP.
- **Защита от фишинга**: защита от попыток получения паролей, банковских данных и прочей конфиденциальной информации незаконными веб-сайтами, выдающими себя за законные.

Чтобы временно отключить отдельный модуль, щелкните зеленый переключатель возле нужного

модуля. Обратите внимание, что при этом будет ослаблена защита вашего компьютера.

Чтобы возобновить защиту отключенного компонента безопасности, щелкните красный переключатель — и компонент снова будет включен.

При применении политики ERA будет отображаться значок блокировки рядом с определенным компонентом. Политика, примененная решением ESET Remote Administrator, может быть переопределена локально после проверки подлинности пользователя, вошедшего в систему (например, администратора). Дополнительные сведения см. в справке о решении ESET Remote Administrator в Интернете.

ПРИМЕЧАНИЕ.
Все средства защиты, отключенные таким способом, будут повторно включены после перезагрузки компьютера.

Чтобы открыть подробные настройки компонента безопасности, щелкните значок шестеренки . возле соответствующего компонента**.**

В нижней части окна настройки есть дополнительные 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**. Для получения дополнительных сведений см. раздел Импорт и экспорт параметров.

Чтобы открыть дополнительные параметры, щелкните элемент **Дополнительные настройки** или нажмите клавишу **F5**.

3.9.1 Компьютер

Доступ к модулю **Компьютер** можно получить, выбрав **Настройка** > **Компьютер**. В нем отображается общая информация о модулях защиты, описанных в предыдущей главе. В данном разделе доступны следующие настройки:

Щелкните значок шестеренки рядом с элементом **Защита файловой системы в режиме реального времени**, затем щелкните **Изменить исключения**, после чего откроется окно настроек Исключения, в котором можно исключить файлы и папки из сканирования.

ПРИМЕЧАНИЕ.
Информация о состоянии защиты документа может быть недоступной, пока не будет активирована в меню **Дополнительные настройки** (F5) > **Защита от вирусов** > **Защита документов**. После активации перезагрузите компьютер. Для этого в области «Настройки» перейдите к разделу «Компьютер» и выберите в меню «Контроль устройств» команду **Перезапустить**. Или же перейдите к области состояний «Защита» и нажмите кнопку **Перезапустить компьютер**.

Приостановить защиту от вирусов и шпионских программ: при каждом временном отключении защиты от вирусов и шпионских программ можно, воспользовавшись раскрывающимся меню, выбрать период времени, на протяжении которого будет отключен выбранный компонент, после чего следует нажать кнопку **Применить**, чтобы отключить компонент безопасности. Чтобы вновь активировать защиту, нажмите кнопку **Включить защиту от вирусов и шпионских программ**.

Настройка сканирования компьютера...: настройка параметров сканирования компьютера (сканирования, запускаемого вручную).

3.9.1.1 Защита от вирусов

Защита от вирусов предотвращает вредоносные атаки на компьютер путем контроля файлов, электронной почты и связи через Интернет. Если обнаруживается угроза, модуль защиты от вирусов может обезвредить ее, сначала заблокировав, а затем очистив, удалив или переместив на карантин.

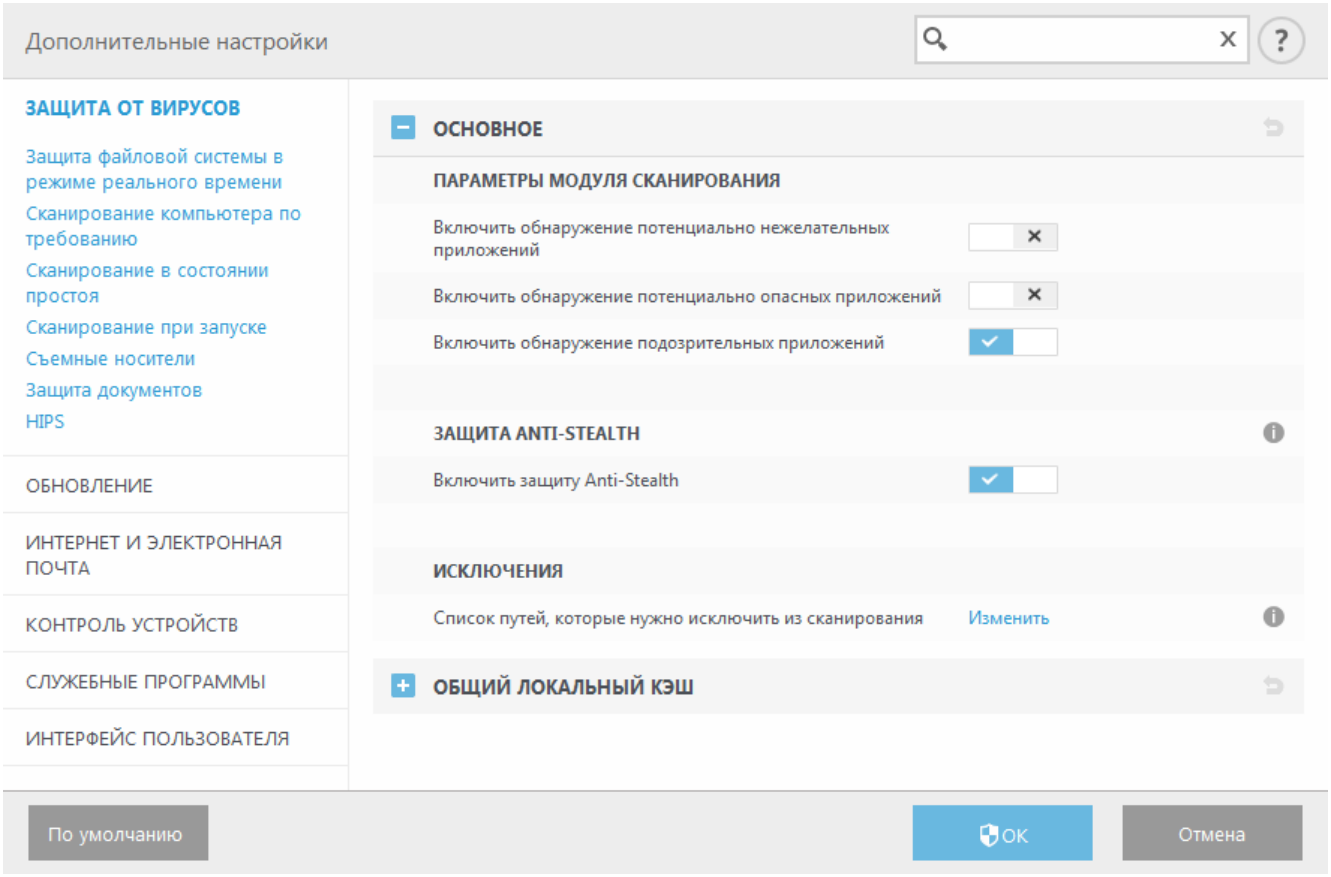
Для настройки параметров модуля защиты от вирусов щелкните элемент **Дополнительные настройки** или нажмите клавишу **F5**.

Параметры модуля сканирования во всех модулях защиты (защиты файловой системы в реальном времени, защиты доступа в Интернет и т. д.) позволяют включать и отключать обнаружение приведенных ниже элементов.

- **Потенциально нежелательные приложения** не всегда являются вредоносными, однако могут негативно повлиять на производительность компьютера.
  Дополнительную информацию о приложениях этого типа см. в глоссарии.
- **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). По умолчанию этот параметр отключен.
  Дополнительную информацию о приложениях этого типа см. в глоссарии.
- **Подозрительные приложения**: к ним относятся программы, сжатые при помощи упаковщиков или средств защиты. Злоумышленники часто используют программы этого типа, чтобы избежать обнаружения.

Технология Anti-Stealth является сложной системой, обеспечивающей обнаружение опасных программ, таких как руткиты, которые могут скрываться от операционной системы. Это значит, что такие программы невозможно обнаружить с помощью обычных методов проверки.

Исключения позволяют исключить файлы и папки из сканирования. Чтобы обеспечить сканирование всех объектов на наличие угроз, рекомендуется создавать исключения только в случае крайней необходимости. Однако в некоторых случаях все же необходимо исключать объекты, например большие базы данных, которые замедляют работу компьютера при сканировании, или программы, конфликтующие с процессом сканирования. Сведения об исключении объекта из области сканирования см. в разделе Исключения.



3.9.1.1.1 Действия при обнаружении заражения

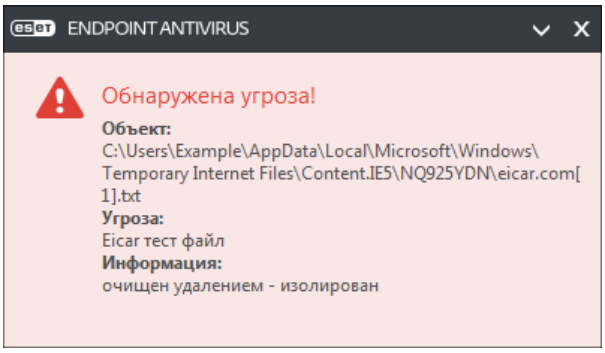
Заражения могут попасть на компьютер из различных источников, таких как веб-сайты, общие папки, электронная почта или съемные носители (накопители USB, внешние диски, компакт- или DVD-диски, дискеты и т. д.).

Стандартное поведение

Обычно ESET Endpoint Antivirus обнаруживает заражения с помощью перечисленных ниже модулей.

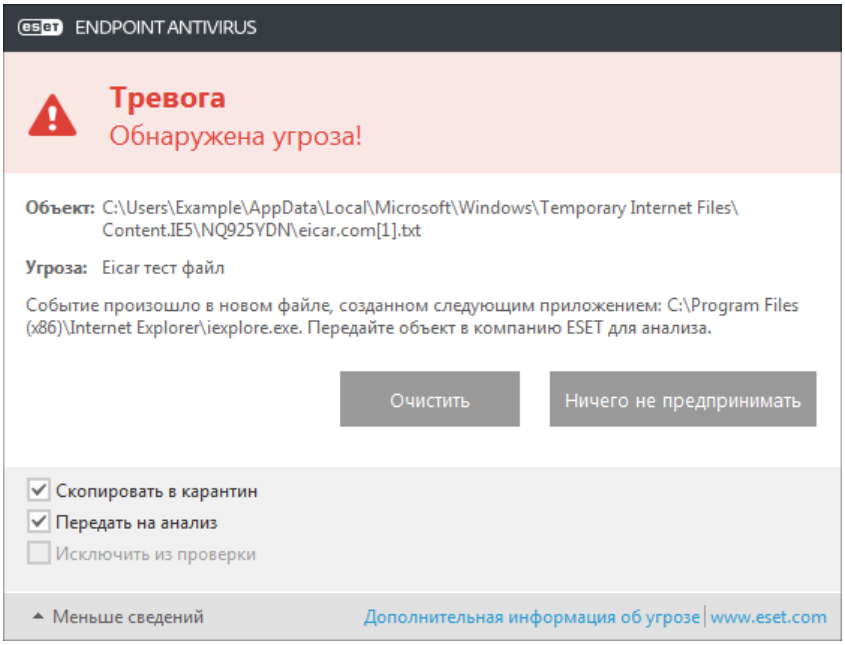
- Защита файловой системы в режиме реального времени
- Защита доступа в Интернет
- Защита почтового клиента
- Сканирование компьютера по требованию

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. Дополнительные сведения об уровнях очистки и поведении см. в разделе Очистка.



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, он будет удален.

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

Множественные угрозы

Если какие-либо зараженные файлы при сканировании компьютера не были очищены (или был выбран уровень очистки **Без очистки**), на экран будет выведено окно предупреждения, в котором пользователю предлагается выбрать действие для таких файлов.

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.

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

- Откройте ESET Endpoint Antivirus и выберите команду «Сканирование компьютера».
- Выберите вариант **Сканирование Smart** (дополнительную информацию см. в разделе Сканирование компьютера).
- После окончания сканирования проверьте в журнале количество просканированных, 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.

3.9.1.2 Общий локальный кэш

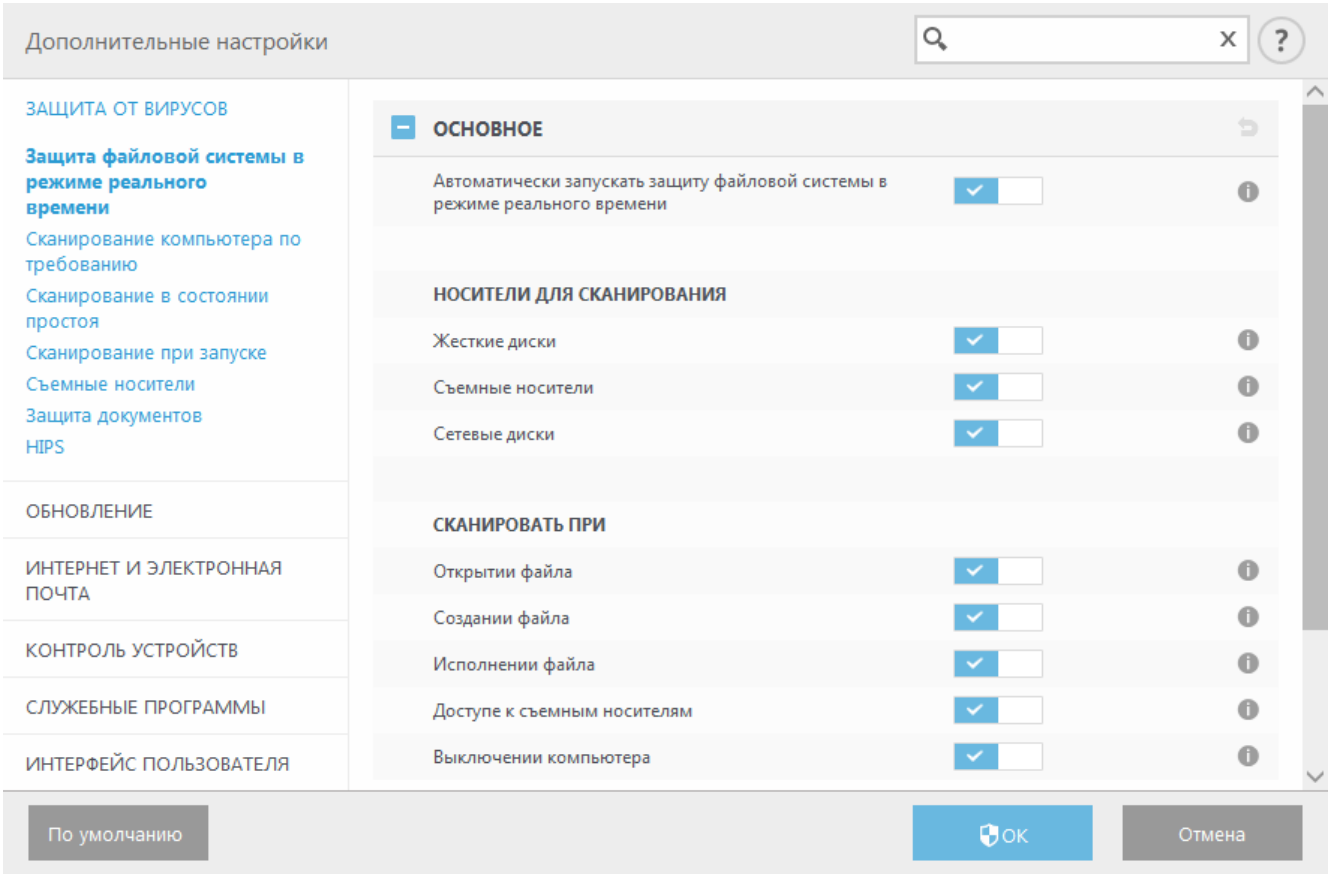
Общий локальный кэш повышает производительность в виртуализированных средах, запрещая повторяющееся сканирование в сети. Благодаря этому каждый файл сканируется только один раз, а затем сохраняется в общем кэше. Включите элемент **Параметры кэширования**, чтобы сохранять данные о сканировании файлов и папок в сети в локальный кэш. При следующем сканировании продукт ESET Endpoint Antivirus будет искать сканируемые файлы в кэше. Если файлы совпадают, они будут исключены из сканирования.

При настройке **сервера кэширования** нужно работать с указанными ниже элементами**.**

- **Имя хоста**: имя или IP-адрес компьютера, на котором расположен кэш.
- **Порт**: номер порта, используемого для передачи данных (тот же, что указан для общего локального кэша).
- **Пароль**: укажите пароль общего локального кэша, если необходимо.

3.9.1.3 Защита файловой системы в режиме реального времени

Функция защиты файловой системы в режиме реального времени контролирует все события в системе, относящиеся к защите от вирусов. Все файлы сканируются на наличие вредоносного кода во время их открытия, создания или запуска. Защита файловой системы в режиме реального времени запускается при загрузке операционной системы.



По умолчанию функция защиты файловой системы в режиме реального времени запускается при загрузке системы и обеспечивает постоянное сканирование. В особых случаях (например, при возникновении конфликта с другим модулем сканирования в режиме реального времени) защиту файловой системы в режиме реального времени можно отключить. Для этого нужно снять флажок **Автоматически запускать защиту файловой системы в режиме реального времени** в разделе **Защита файловой системы в реальном времени** > **Основные сведения**, который входит в меню **Дополнительные настройки**.

Носители для сканирования

По умолчанию все типы носителей сканируются на наличие возможных угроз.

Локальные диски: контролируются все жесткие диски, существующие в системе.
Съемные носители: контролируются компакт-/DVD-диски, USB-устройства хранения, Bluetooth-устройства и т. п.
Сетевые диски: сканируются все подключенные сетевые диски.

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 исполнении. Рекомендуется не изменять настройки по умолчанию, поскольку они обеспечивают максимальную защиту компьютера в режиме реального времени.

- **Открытие файла**: включение и отключение сканирования при открытии файлов.
- **Создание файла**: включение и отключение сканирования при создании файлов.
- **Исполнение файла**: включение и отключение сканирования при запуске файлов.
- **Доступ к съемным носителям**: включение и отключение сканирования при доступе к конкретному съемному носителю, на котором могут храниться данные.
- **Выключение компьютера**: включение и отключение сканирования при выключении компьютера.

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 Настройка параметров модуля 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.

Для снижения влияния на производительность компьютера при использовании защиты в режиме реального времени файлы, которые уже сканировались, не сканируются повторно, пока не будут изменены. Файлы сканируются повторно сразу после каждого обновления базы данных сигнатур вирусов. Такое поведение контролируется с использованием **оптимизации Smart**. Если **оптимизация Smart** отключена, все файлы сканируются каждый раз при доступе к ним. Для изменения этого параметра нажмите **F5**, чтобы открыть окно «Дополнительные настройки», и перейдите к разделу **Защита от вирусов** > **Защита файловой системы в режиме реального времени**. Последовательно щелкните элементы **Настройка параметров модуля ThreatSense** > **Другое** и снимите или установите флажок **Включить интеллектуальную оптимизацию**.

3.9.1.3.1 Дополнительные параметры ThreatSense

Дополнительные параметры модуля ThreatSense для новых и измененных файлов: вероятность заражения вновь созданных или измененных файлов выше по сравнению с аналогичным показателем для существующих файлов. Именно поэтому программа проверяет эти файлы с дополнительными параметрами сканирования. Вместе с обычными методами сканирования, основанными на сигнатурах, применяется расширенная эвристика, что делает возможным обнаружение новых угроз еще до выпуска обновлений базы данных сигнатур вирусов. В дополнение ко вновь созданным файлам выполняется также сканирование самораспаковывающихся файлов (.sfx) и упаковщиков (исполняемых файлов с внутренним сжатием). По умолчанию проверяются архивы с глубиной вложенности до 10 независимо от их фактического размера. Для изменения параметров сканирования архивов снимите флажок **Параметры сканирования архива по умолчанию**.

Дополнительную информацию об **упаковщиках**, **самораспаковывающихся архивах** и **расширенном эвристическом анализе** см. в разделе о настройках параметров модуля ThreatSense.

Дополнительные параметры модуля ThreatSense для исполняемых файлов: по умолчанию расширенная эвристика не применяется при исполнении файлов. Если этот параметр включен, настоятельно рекомендуется включить оптимизацию Smart и ESET Live Grid, чтобы уменьшить воздействие на производительность системы.

3.9.1.3.2 Уровни очистки

Защита в режиме реального времени предусматривает три уровня очистки (для доступа к ним щелкните **Настройка параметров модуля ThreatSense** в разделе **Защита файловой системы в режиме реального времени**, а затем щелкните **Очистка**).

Без очистки: зараженные файлы не будут очищаться автоматически. Программа выводит на экран окно предупреждения и предлагает пользователю выбрать действие. Этот уровень предназначен для более опытных пользователей, которые знают о действиях, которые следует предпринимать в случае заражения.

Стандартная очистка: программа пытается автоматически очистить или удалить зараженный файл на основе предварительно определенного действия (в зависимости от типа заражения). Обнаружение и удаление зараженных файлов сопровождается уведомлением, отображающимся в правом нижнем углу экрана. Если невозможно выбрать правильное действие автоматически, программа предложит выбрать другое действие. То же самое произойдет в том случае, если предварительно определенное действие невозможно выполнить.

Тщательная очистка: программа очищает или удаляет все зараженные файлы. Исключение составляют только системные файлы. Если очистка невозможна, на экран выводится окно предупреждения, в котором пользователю предлагается выполнить определенное действие.

ВНИМАНИЕ!
Если в архиве содержатся зараженные файлы, существует два варианта обработки архива. В стандартном режиме (при стандартной очистке) целиком удаляется архив, все файлы в котором заражены. В режиме **Тщательная очистка** удаляется архив, в котором заражен хотя бы один файл, независимо от состояния остальных файлов.

3.9.1.3.3 Проверка модуля защиты в режиме реального времени

Чтобы убедиться, что защита в режиме реального времени работает и обнаруживает вирусы, используйте проверочный файл eicar.com. Этот тестовый файл является безвредным, и его обнаруживают все программы защиты от вирусов. Файл создан компанией EICAR (Европейский институт антивирусных компьютерных исследований) для проверки функционирования программ защиты от вирусов. Файл доступен для загрузки с веб-сайта http://www.eicar.org/download/eicar.com.

3.9.1.3.4 Момент изменения конфигурации защиты в режиме реального времени

Защита файловой системы 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 Endpoint Antivirus все параметры оптимизированы для максимальной защиты системы. Для восстановления настроек по умолчанию щелкните возле каждой вкладки в окне (**Дополнительные настройки** > **Антивирус** > **Защита файловой системы в режиме реального времени**).

3.9.1.3.5 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 защита файловой системы в режиме реального времени непреднамеренно была отключена пользователем, ее нужно включить. Для повторной активации защиты в режиме реального времени перейдите в раздел **Настройка** и в главном окне программы нажмите **Защита файловой системы в режиме реального времени**.

Если защита файловой системы в режиме реального времени не запускается при загрузке операционной системы, обычно это связано с тем, что отключен параметр **Автоматический запуск защиты файловой системы в режиме реального времени**. Чтобы включить этот параметр, перейдите к разделу **Дополнительные**

настройки (**F5**) и последовательно щелкните элементы **Антивирус** > **Защита в режиме реального времени**> **Основные сведения**. Обязательно установите флажок **Автоматически запускать защиту файловой системы в режиме реального 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. При одновременной работе двух систем защиты от вирусов могут возникнуть конфликты. Перед установкой ESET рекомендуется удалить с компьютера все прочие программы защиты от вирусов.

Защита файловой системы в режиме реального времени на запускается

Если защита не запускается при загрузке системы, но функция **Автоматический запуск защиты файловой системы в режиме реального времени** включена, возможно, возник конфликт с другими приложениями. Чтобы получить помощь для решения этой проблемы, обратитесь в службу поддержки клиентов ESET.

3.9.1.4 Сканирование компьютера по требованию

Модуль сканирования по требованию является важной частью ESET Endpoint Antivirus. 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. Рекомендуется выполнять регулярные (например, раз в месяц) операции детального сканирования системы на предмет обнаружения вирусов, которые не были обнаружены при помощи функции защиты файловой системы в режиме реального времени. Это может произойти, если в определенный момент защита файловой системы в режиме реального времени была отключена, база данных вирусов была устаревшей или файл не был распознан как вирус при сохранении на диск.

Доступно два типа **сканирования компьютера**. **Сканирование Smart** позволяет быстро просканировать систему без необходимости дополнительной настройки параметров сканирования. **Выборочное сканирование** позволяет выбрать предопределенный профиль сканирования и указать объекты, которые нужно просканировать.

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

Сканирование Smart

Сканирование Smart позволяет быстро запустить сканирование компьютера и очистить зараженные файлы без вмешательства пользователя. Преимущество сканирования Smart заключается в том, что оно удобно в выполнении и не требует тщательной настройки сканирования. При сканировании Smart проверяются все файлы на локальных дисках, а также автоматически очищаются или удаляются обнаруженные заражения. Для уровня очистки автоматически выбрано значение по умолчанию. Дополнительную информацию о типах очистки см. в разделе Очистка.

Выборочное сканирование

Выборочное сканирование является оптимальным решением в том случае, когда нужно указать параметры сканирования, такие как объекты и методы сканирования. Преимуществом выборочного сканирования является возможность подробной настройки параметров. Конфигурации можно сохранять в пользовательских профилях сканирования, которые удобно применять, если регулярно выполняется сканирование с одними и теми же параметрами.

Для выбора объектов сканирования щелкните **Сканирование компьютера** > **Выборочное сканирование** и выберите один из вариантов из раскрывающегося меню **Объекты сканирования** или конкретные объекты сканирования в древовидной структуре. Объекты сканирования также можно задать, указав пути к папкам и файлам, которые нужно сканировать. Если нужно только выполнить сканирование системы без дополнительных действий по очистке, выберите параметр **Сканировать без очистки**. При выполнении сканирования можно выбрать один из трех уровней очистки, последовательно щелкнув элементы **Настройка** > **Параметры ThreatSense** > **Очистка**.

Пользователям, не имеющим достаточного опыта работы с антивирусными программами, не рекомендуется выполнять выборочное сканирование.

Сканирование съемных носителей

Подобно сканированию Smart данная функция быстро запускает сканирование съемных носителей (таких как компакт-диски, DVD-диски, накопители USB), 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**.

В раскрывающемся списке **Действие после сканирования** можно выбрать действие (бездействие, выключение или перезагрузка), которое нужно выполнить после сканирования.

Выключить после сканирования: разрешает запланированное завершение работы после окончания сканирования компьютера по требованию. На экран будет выведено диалоговое окно подтверждения, которое будет активно в течение 60 секунд. Нажмите кнопку **Отмена**, если нужно отменить завершение работы.

ПРИМЕЧАНИЕ.
Рекомендуется запускать сканирование компьютера не реже одного раза в месяц. Можно настроить сканирование как запланированную задачу в меню **Сервис** > **Планировщик**.

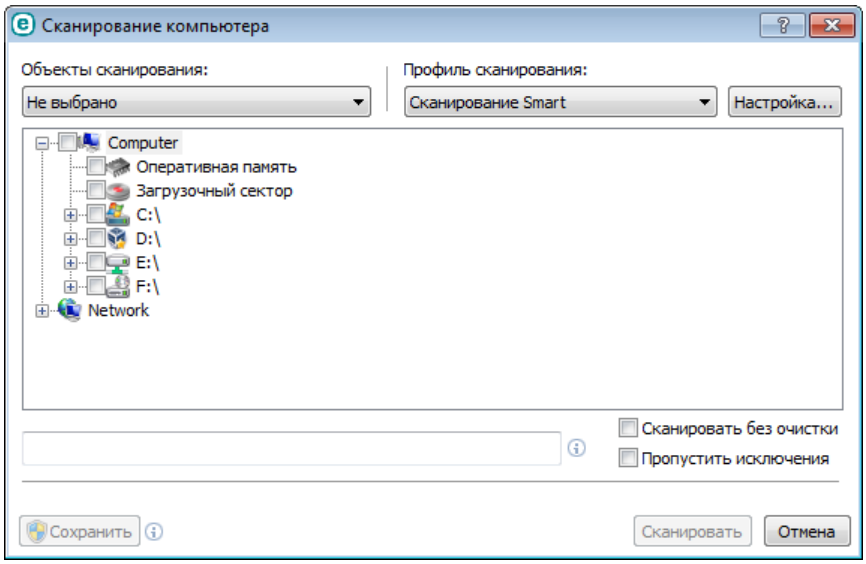
3.9.1.4.1 Средство запуска выборочного сканирования

Если необходимо просканировать определенный объект, можно использовать выборочное сканирование. Для этого необходимо выбрать **Сканирование компьютера** > **Выборочное сканирование**, а затем выбрать необходимый вариант в раскрывающемся меню **Объекты сканирования** или же указать нужные объекты в дереве папок.

В окне объектов сканирования можно определить, какие объекты (оперативная память, жесткие диски, секторы, файлы и папки) будут сканироваться на предмет выявления заражений. Выберите объекты сканирования в древовидной структуре, содержащей все доступные на компьютере устройства. В раскрывающемся меню **Объекты сканирования** можно выбрать предварительно определенные объекты сканирования.

- **Используя Настройки профиля**: выбираются объекты, указанные в выделенном профиле сканирования.
- **Сменные носители**: выбираются дискеты, USB-устройства хранения, компакт- и DVD-диски.
- **Локальные диски**: выбираются все жесткие диски, существующие в системе.
- **Сетевые диски**: выбираются все подключенные сетевые диски.
- **Не выбрано**: отменяется выбор объектов.

Для быстрого перехода к какому-либо объекту сканирования (папкам или файлам) или для его непосредственного добавления укажите нужный объект в пустом поле под списком папок. Это возможно только в том случае, если в древовидной структуре не выбраны никакие объекты, а в меню **Объекты сканирования** выбран пункт **Не выбрано**.



Зараженные элементы не очищаются автоматически. Сканирование без очистки можно использовать для получения общих сведений о текущем состоянии защиты. Если нужно только выполнить сканирование системы без дополнительных действий по очистке, выберите параметр **Сканировать без очистки**. Кроме того, можно выбрать один из трех уровней очистки, последовательно щелкнув элементы **Настройки** > **Параметры ThreatSense** > **Очистка**. Информация о сканировании сохраняется в журнале сканирования.

В раскрывающемся меню **Профиль сканирования** можно выбрать профиль, который будет использован для сканирования выбранных объектов. По умолчанию используется профиль **Сканирование Smart**. Существует еще два предварительно заданных профиля сканирования под названием **Детальное сканирование** и **Сканирование через контекстное меню**. В этих профилях сканирования используются другие параметры модуля ThreatSense. Нажмите кнопку **Настройки...**, чтобы детально настроить выбранный профиль сканирования в меню профиля сканирования. Доступные параметры описаны в разделе **Другое** при настройке параметров модуля ThreatSense.

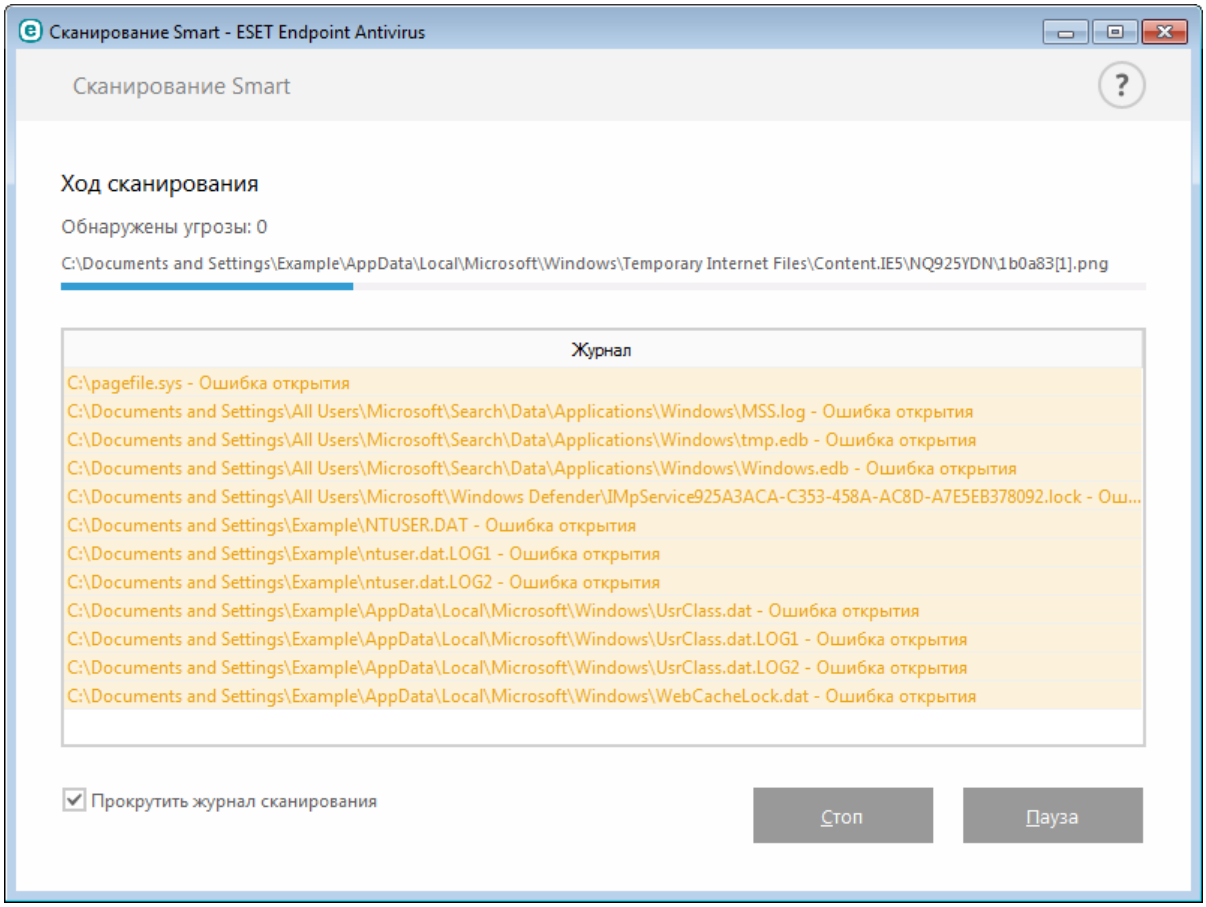
Нажмите кнопку **Сохранить**, чтобы сохранить изменения в выборе объектов сканирования, в том числе объектов, выбранных в дереве каталогов.

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 текущая учетная запись пользователя не имеет достаточных прав на доступ к файлам, которые следует сканировать. Обратите внимание, что данная кнопка недоступна, если текущий пользователь не может вызывать операции контроля учетных записей в качестве администратора.

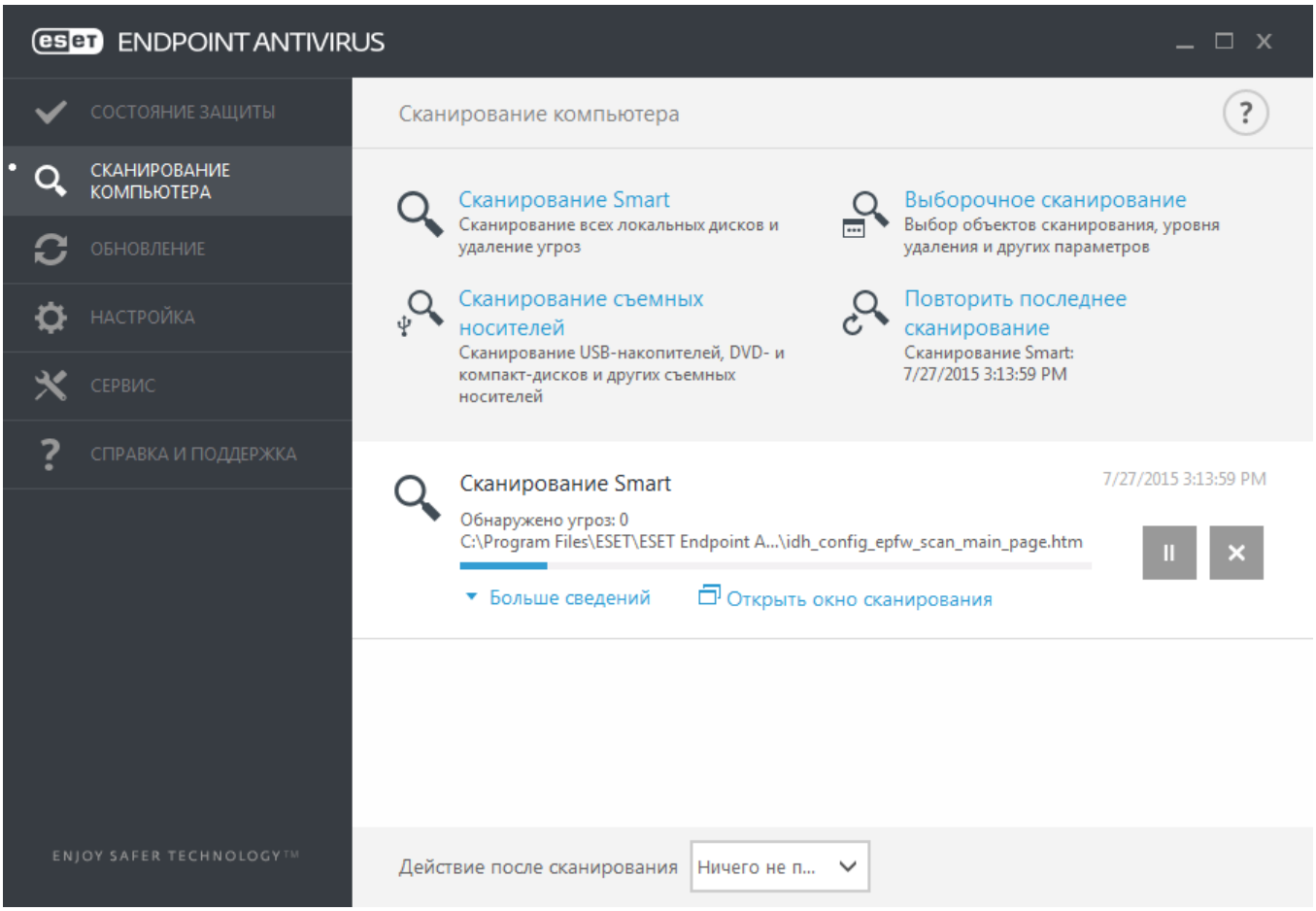
3.9.1.4.2 Ход сканирования

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



ПРИМЕЧАНИЕ.
Нормально, что некоторые файлы, такие как защищенные паролем файлы или файлы, используемые исключительно операционной системой (обычно *pagefile.sys* и некоторые файлы журналов), не могут сканироваться.

Ход сканирования: индикатор выполнения показывает состояние уже просканированных объектов по сравнению с оставшимися. Состояние выполнения сканирования формируется на основе общего количества объектов, включенных в сканирование.
Объект: имя объекта, который сканируется в настоящий момент, и его расположение.
Обнаружено угроз: общее количество угроз, обнаруженных при сканировании.
Пауза: приостановка сканирования.
Продолжить: эта возможность становится доступна после приостановки выполнения сканирования. Нажмите **Возобновить**, чтобы возобновить сканирование.
Остановить: прекращение сканирования.
Прокрутить журнал сканирования: если этот параметр активирован, журнал сканирования будет прокручиваться автоматически при добавлении новых записей, чтобы были видны самые свежие элементы.



3.9.1.5 Контроль устройств

ESET Endpoint Antivirus обеспечивает автоматическое управление устройствами (компакт- и DVD-дисками, USB-устройствами и т. п.). 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
- USB-принтеры
- FireWire-хранилище
- Устройство Bluetooth
- Устройство чтения смарт-карт
- Устройство обработки изображений
- Модемы
- LPT/COM-порты
- Переносное устройство
- Все типы устройств

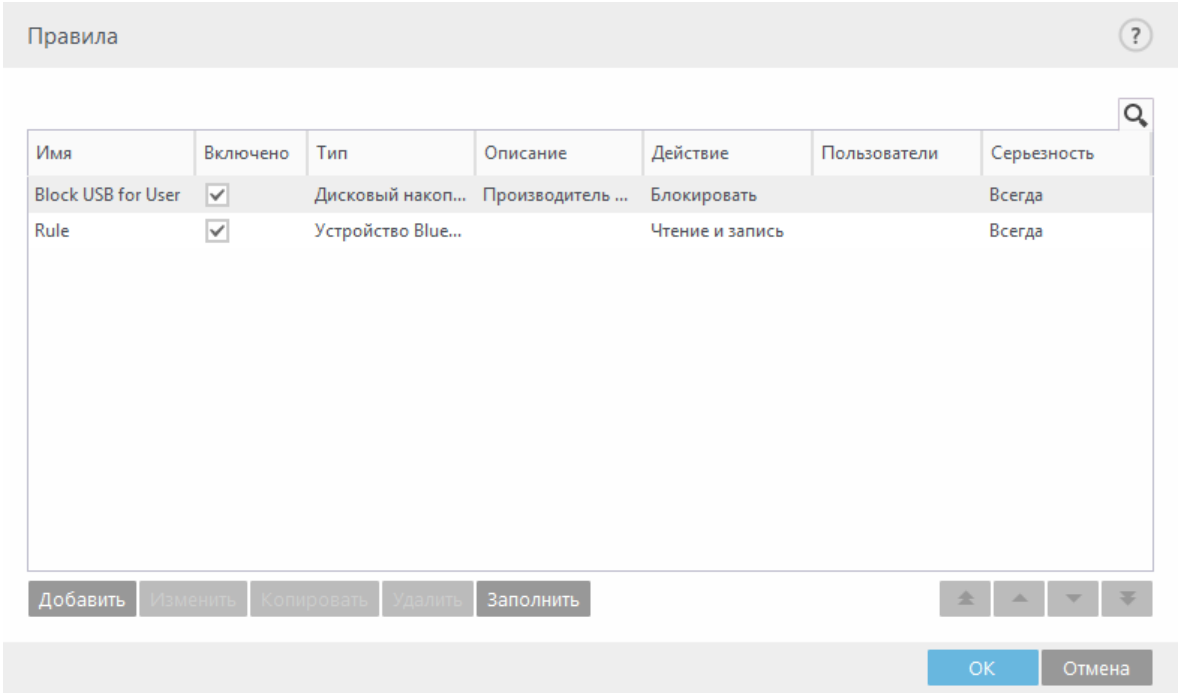
Параметры контроля устройств можно изменить в разделе **Дополнительные настройки** (F5) > **Контроль устройств**.

Если активировать переключатель **Интеграция с системой**, в программе ESET Endpoint Antivirus будет включена функция контроля устройств. Чтобы это изменение вступило в силу, необходимо перезагрузить компьютер. После включения контроля устройств кнопка **Редактор правил** станет активной и вы сможете использовать редактор правил.

При подключении устройства, заблокированного существующим правилом, отобразится окно уведомления, и доступ к устройству будет заблокирован.

3.9.1.5.1 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.



Некоторые устройства можно разрешить или заблокировать на основании сведений об их пользователе, группе пользователя или в соответствии с несколькими 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.

Для управления правилом используйте кнопки **Добавить** или **Изменить**. Снимите флажок **Включено** возле правила, чтобы отключить его до тех пор, пока оно не понадобится снова. Чтобы удалить правило, выделите его и выберите команду **Удалить**.

Чтобы создать правило с использованием заранее заданных параметров из другого правила, нажмите кнопку **Копировать**.

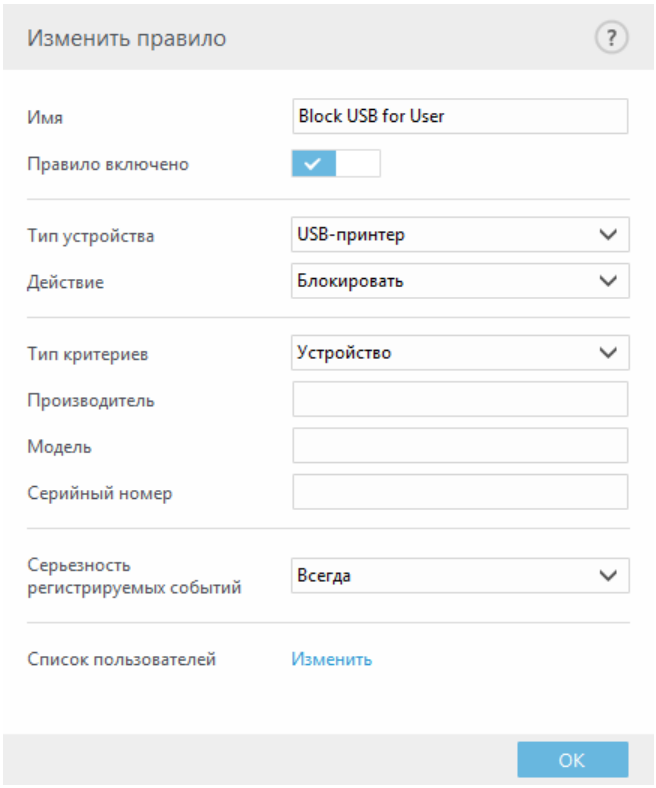
Щелкните **Заполнить**, чтобы выполнить автоматическое заполнение параметров для съемных носителей, подключенных к компьютеру.

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**.

В журнал контроля устройств записываются все случаи, когда срабатывает функция контроля устройств. Записи журнала можно просмотреть в главном окне программы ESET Endpoint Antivirus в разделе **Служебные программы** > **Файлы журнала**.

3.9.1.5.2 Добавление правил контроля устройств

Правило контроля устройств определяет 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 переключатель 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 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.

ПРИМЕЧАНИЕ.
Функция списка пользователей недоступна для модемов. Правило применяется ко всем пользователям, а текущий список пользователей удаляется.

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.

- **Чтение и запись**: будет разрешен полный доступ к устройству.
- **Блокировать**: доступ к устройству будет заблокирован.
- **Только чтение**: будет разрешено только чтение данных с устройства.
- **Предупредить**: при каждом подключении устройства пользователь получает уведомление, разрешено 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 (прав) 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 **Только чтение** 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 и изменять правила для конкретных устройств. Все параметры не зависят от регистра.

- **Производитель**: фильтрация по имени или идентификатору производителя.
- **Модель**: наименование устройства.
- **Серийный номер**: у внешних устройств обычно есть серийные номера. Когда речь идет о компакт- или DVD-диске, то это серийный номер конкретного носителя, а не дисковода компакт-дисков.

ПРИМЕЧАНИЕ.
Если для этих параметров не заданы значения, во время сопоставления правило игнорирует эти поля. Для параметров фильтрации во всех текстовых полях не учитывается регистр и не поддерживаются подстановочные знаки (*, ?).

ПОДСКАЗКА
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

- **Всегда** : записываются все события.
- **Диагностика** — регистрируется информация, необходимая для тщательной настройки программы.
- **Информация**: записываются 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.

Правила можно назначать только для некоторых пользователей или их групп, добавленных в **список пользователей**.

- **Добавить**: открывается диалоговое окно **Типы объектов: пользователи и группы**, в котором можно выбрать нужных пользователей.
- **Удалить**: выбранный пользователь удаляется из фильтра.

ПРИМЕЧАНИЕ.
Не все устройства можно фильтровать по пользовательским правилам (например, устройства обработки изображений предоставляют информацию только о действиях, но не о пользователях).

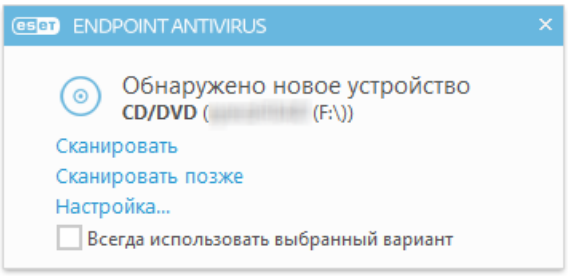
3.9.1.6 Съемные носители

ESET Endpoint Antivirus обеспечивает автоматическое сканирование съемных носителей (компакт- и DVD-дисков, USB-устройств и т. п.). Данный модуль позволяет сканировать вставленный носитель. Это может быть удобно, если администратор компьютера хочет предотвратить подключение пользователями съемных носителей с нежелательным содержимым.

Действие, которое следует предпринять после подключения съемного носителя — выбор действия по умолчанию, которое будет выполняться при подключении съемного носителя (компакт-диска, DVD-диска, USB-устройства) к компьютеру. Если выбран вариант **Показать параметры сканирования**, на экран будет выведено уведомление, с помощью которого можно выбрать нужное действие.

- **Не сканировать**: не будет выполнено никаких действий, а окно **Обнаружено новое устройство** будет закрыто.
- **Автоматическое сканирование устройств**: выполняется сканирование подключенного съемного носителя по требованию.
- **Показать параметры сканирования**: переход в раздел настройки работы со съемными носителями.

Когда вставляется съемный носитель, отображается следующее диалоговое окно:



Сканировать сейчас: начнется сканирование съемного носителя.

Сканировать позже: сканирование съемного носителя будет отложено.

Настройки: вызов дополнительных параметров.

Всегда использовать выбранный вариант: если установить этот флажок, выбранное действие будет выполняться каждый раз, когда вставляется съемный носитель.

Кроме того, в ESET Endpoint Antivirus есть модуль контроля устройств, дающий возможность задавать правила использования внешних устройств на указанном компьютере. Дополнительные сведения об этом модуле см. в разделе Контроль устройств.

3.9.1.7 Сканирование в состоянии простоя

Вы можете разрешить сканирование в состоянии простоя, выбрав **Дополнительные настройки** в меню **Антивирус** > **Сканирование в состоянии простоя** > **Основное**. Установите переключатель **Разрешить сканирование в состоянии простоя** в положение **Вкл.**, чтобы разрешить использование этой функции. Когда компьютер находится в состоянии простоя, автоматически выполняется сканирование всех локальных дисков. Полный список условий для запуска сканирования в состоянии простоя см. в Условиях запуска обнаружения в состоянии простоя..

По умолчанию в состоянии простоя сканирование не работает, если компьютер (ноутбук) работает от батареи. Этот параметр можно изменить, щелкнув переключатель **Сканировать даже в случае работы компьютера от аккумулятора** в разделе «Дополнительные настройки».

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**).

Обнаружение в состоянии простоя будет запущено в случае пребывания компьютера в одном из следующих режимов.

- выключенный экран или заставка;
- блокировка компьютера;
- выход пользователя.

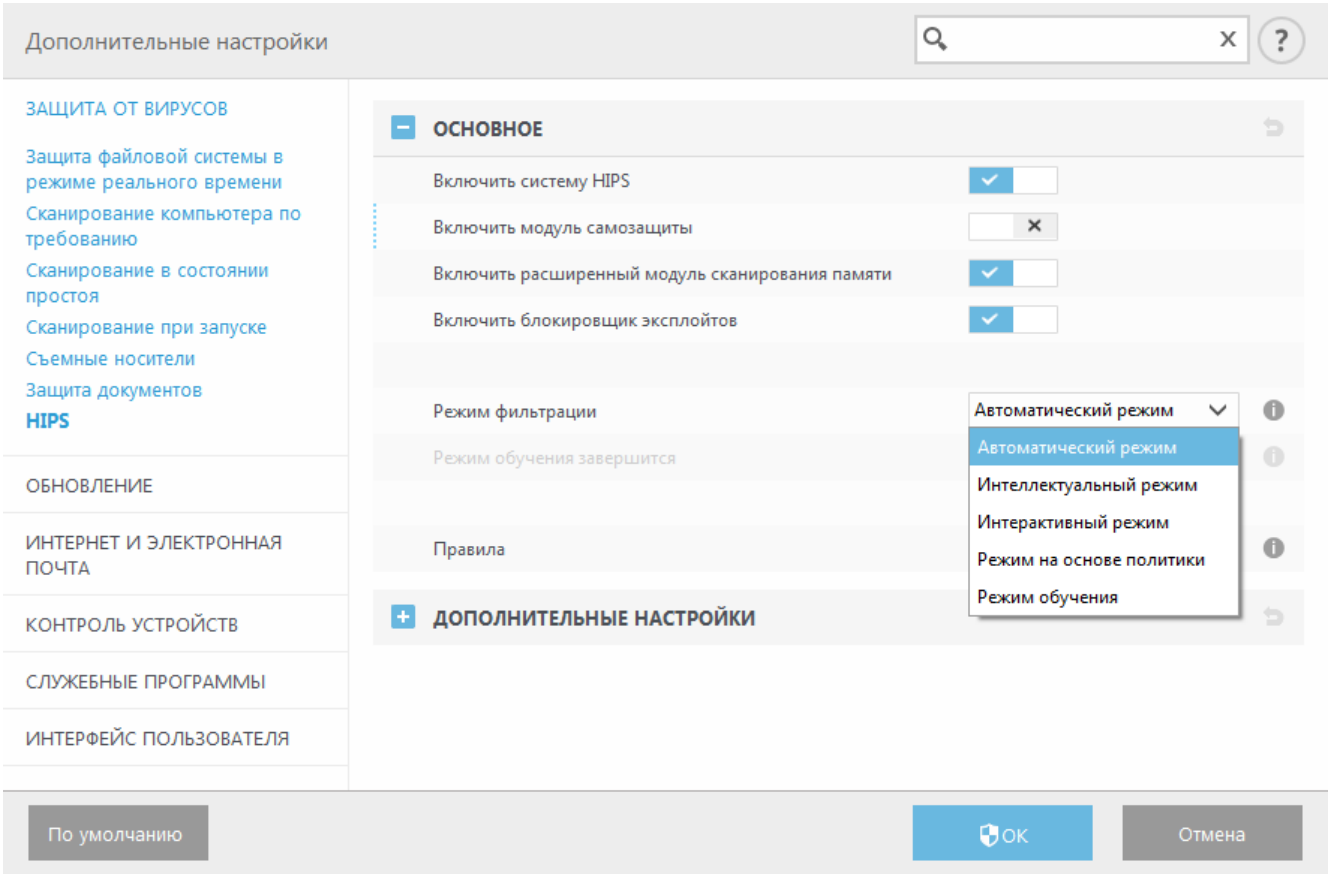
Выберите Настройка параметров модуля ThreatSense для изменения параметров сканирования (например, методов обнаружения) для сканирования в состоянии простоя.

3.9.1.8 Система предотвращения вторжений на узел

ВНИМАНИЕ!
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 HIPS доступны в разделе **Дополнительные настройки** (F5) > **Антивирус** > **Система предотвращения вторжений на узел** > **Основные сведения**. Состояние HIPS (включено/отключено) отображается в главном окне программы ESET Endpoint Antivirus, в разделе **Установка** > **Компьютер**.



В ESET Endpoint Antivirus есть встроенная технология самозащиты, которая не позволяет вредоносным программам повреждать или отключать защиту от вирусов и шпионских программ. Благодаря этому пользователь всегда уверен в защищенности компьютера. Чтобы отключить систему HIPS или функцию самозащиты, требуется перезагрузить Windows.

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.

Доступны четыре режима фильтрации.

Автоматический режим: включены все операции за исключением тех, которые заблокированы предварительно заданными правилами, защищающими компьютер.

Интерактивный режим: пользователю будет предлагаться подтверждать операции.

Режим на основе политики: операции блокируются.

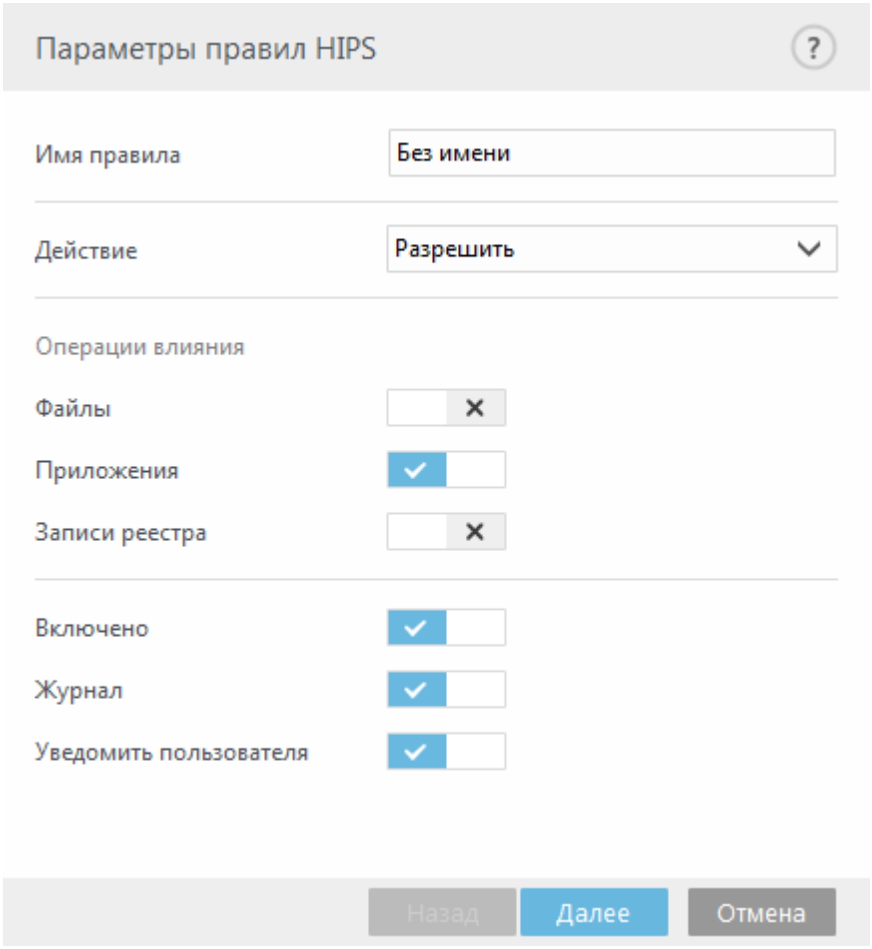
Режим обучения: операции включены, после каждой операции создается правило. Правила, создаваемые в таком режиме, можно просмотреть в редакторе правил, но их приоритет ниже, чем у правил, создаваемых вручную или в автоматическом режиме. При выборе режима обучения в раскрывающемся меню режимов фильтрации HIPS 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.

Интеллектуальный режим: пользователь будет получать уведомления только об очень подозрительных событиях.

Система предотвращения вторжений на узел отслеживает события в операционной системе и реагирует на них соответствующим образом на основе правил, которые аналогичны правилам персонального файервола. Нажмите кнопку **Настроить**, чтобы открыть окно управления правилами системы HIPS. Здесь можно выбирать, создавать, изменять и удалять правила.

В следующем примере будет показано, как ограничить нежелательное поведение приложений.

1. Присвойте правилу имя и выберите **Блокировать** в раскрывающемся меню **Действие**.
2. Активируйте переключатель **Уведомить пользователя**, чтобы уведомление отображалось при каждом применении правила.
3. Выберите хотя бы одну операции, к которой будет применяться правило. В окне **Исходные приложения** выберите в раскрывающемся списке вариант **Все приложения**. Новое правило будет применяться ко всем приложениям, которые будут пытаться выполнить любое из выбранных действий по отношению к указанным приложениям.
4. Выберите **Изменить состояние другого приложения** (все операции описаны в справке продукта, которую можно открыть, нажав клавишу F1)..
5. Выберите в раскрывающемся списке вариант **Определенные приложения** и **добавьте** одно или несколько приложений, которые нужно защитить.
6. Нажмите кнопку **Готово**, чтобы сохранить новое правило.



3.9.1.8.1 Дополнительные настройки

Перечисленные далее параметры полезны для отладки и анализа поведения приложения.

Драйверы, загрузка которых разрешена всегда: загрузка выбранных драйверов разрешена всегда, вне зависимости от настроенного режима фильтрации, если они не заблокированы в явном виде правилом пользователя.

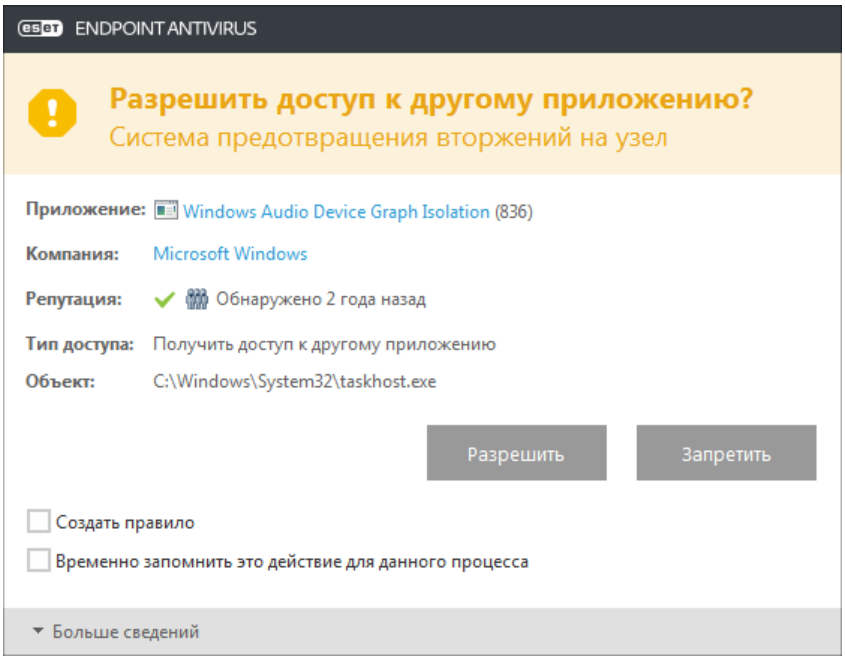
Регистрировать все заблокированные операции: все заблокированные операции будут записываться в журнал системы предотвращения вторжений на узел.

Сообщать об изменениях приложений, загружаемых при запуске системы: при добавлении или удалении приложения, загружаемого при запуске системы, на рабочем столе отображается уведомление.

Обновленную версию этой страницы справочной системы см. в статье базы знаний ESET.

3.9.1.8.2 Интерактивное окно HIPS

Если для правила по умолчанию установлено действие **Запрашивать**, 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.



В диалоговом окне можно создать правило на основе нового действия, обнаруживаемого системой HIPS, а затем определить условия, в соответствии с которыми это действие будет разрешено или запрещено. Отдельные параметры можно настроить, щелкнув элемент **Дополнительные сведения**. Правила, создаваемые таким способом, считаются равнозначными правилам, созданным вручную, поэтому правило, созданное в диалоговом окне, может быть менее подробным, чем правило, которое вызвало появление такого диалогового окна. Это значит, что после создания такого правила эта же операция может вызвать появление такого же окна.

Выбор параметра **Временно запомнить это действие для данного процесса** 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.

3.9.1.9 Режим презентации

Режим презентации — это функция для тех, кто стремится избежать перерывов в работе программного обеспечения и появления отвлекающих от дел всплывающих окон, а также желает свести к минимуму нагрузку на процессор. Его также можно использовать во время проведения презентаций, которые нельзя прерывать деятельностью модуля защиты от вирусов. Он блокирует появление всплывающих окон и выполнение запланированных задач. Защита системы по-прежнему работает в фоновом режиме, но не требует какого-либо вмешательства со стороны пользователя.

Выберите **Настройки** > **Компьютер** и затем щелкните переключатель напротив **Режима презентации** для его ручного включения. В окне **Дополнительные настройки** (F5) выберите **Служебные программы** > **Режим презентации** и затем щелкните переключатель **Автоматически включать режим презентации при выполнении приложений в полноэкранном режиме**, чтобы при запуске приложений в полноэкранном режиме продукт ESET Endpoint Antivirus автоматически переходил в режим презентации. Включая режим презентации вы подвергаете систему угрозе, поэтому значок состояния защиты на панели задач станет оранжевым, чтобы тем самым предупредить вас. Данное предупреждение также отобразится в главном окне программы: в нем вы увидите надпись **Режим презентации включен** оранжевого цвета.

Если установить флажок **Автоматически включать режим презентации при работе приложений в полноэкранном режиме**, режим презентации будет включаться при запуске любого приложения в

полноэкранном режиме и автоматически выключаться после выхода из этого приложения. Это особенно удобно для включения режима презентации непосредственно при запуске игры, полноэкранного приложения или презентации.

Вы также можете выбрать **Автоматически отключать режим презентации через** для указания времени в минутах, через которое режим презентации будет автоматически отключен.

3.9.1.10 Сканирование файлов, исполняемых при запуске системы

При загрузке компьютера и обновлении базы данных сигнатур вирусов 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 при запуске системы**. Чтобы изменить эти параметры, выберите **Служебные программы** > **Планировщик**, нажмите кнопку **Автоматическая проверка файлов при запуске системы**, а затем — кнопку **Изменить**. На последнем этапе отобразится диалоговое окно Автоматическая проверка файлов при запуске системы (дополнительные сведения см. в следующем разделе).

Более подробные инструкции по созданию задач в планировщике и управлению ими см. в разделе Создание новой задачи.

3.9.1.10.1 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, запускающиеся 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 подлежащих сканированию файлов являются фиксированными для каждой описанной выше группы.

Приоритет сканирования: уровень приоритетности, используемый для определения условий начала сканирования.

- **При бездействии**: задача будет выполняться только при бездействии системы.
- **Низкий**: минимальная нагрузка на систему.
- **Ниже среднего**: низкая нагрузка на систему.
- **Средний**: средняя нагрузка на систему.

3.9.1.11 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 режиме реального времени. Ее можно отключить, чтобы улучшить производительность систем, которые не содержат большое количество документов Microsoft Office.

Параметр **Интеграция с системой** активирует систему защиты. Для изменения этого параметра нажмите F5, чтобы открыть окно «Дополнительные настройки», и перейдите к разделу **Защита от вирусов** > **Защита документов** дерева расширенных параметров.

Эта функция активируется приложениями, в которых используется Microsoft Antivirus API (например, Microsoft Office 2000 и более поздние версии или Microsoft Internet Explorer 5.0 и более поздние версии).

3.9.1.12 Исключения

Исключения позволяют исключить файлы и папки из сканирования. 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 больших баз данных, которые замедляет работу или программ, конфликтующих с процессом сканирования (например, программное обеспечение для резервного копирования).

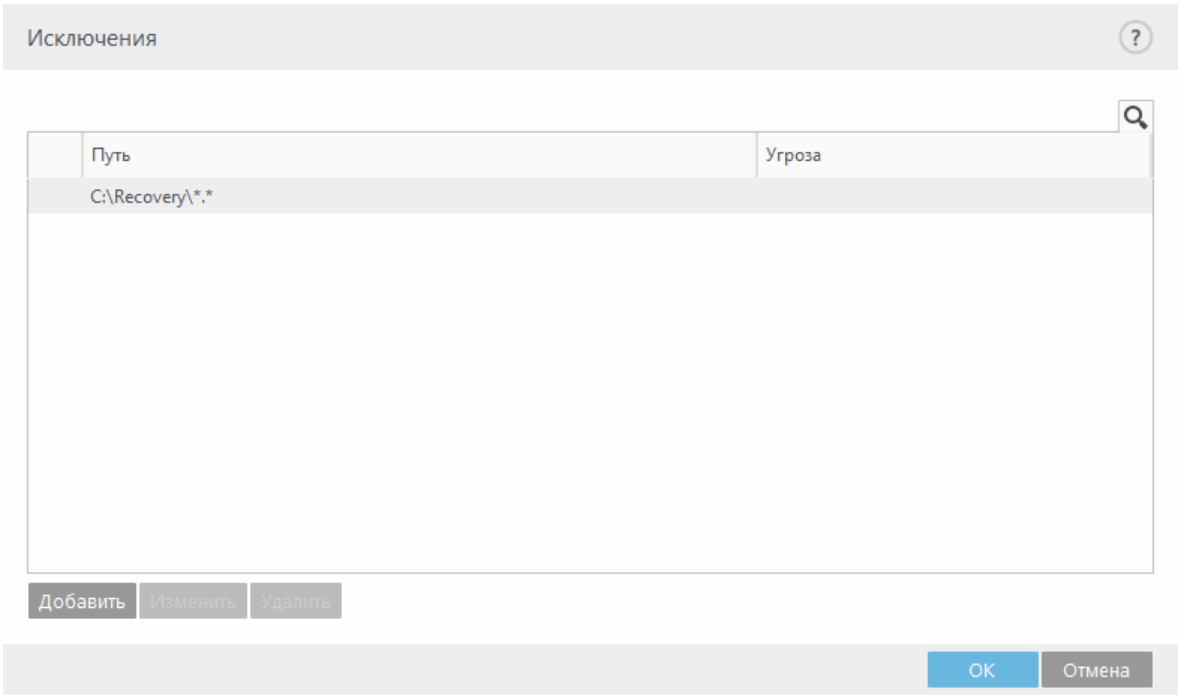
Для исключения объекта из сканирования выполните следующие действия.

1. Нажмите **Добавить**.
2. Введите путь к объекту или выделите его в древовидной структуре.

Для указания групп файлов можно использовать символы шаблона. Вопросительный знак (?) обозначает один любой символ, а звездочка (*) — любое количество символов.

Примеры

- Если нужно исключить все файлы в папке, следует ввести путь к папке и использовать маску «*.*».
- Для того чтобы исключить весь диск, в том числе все файлы и подпапки на нем, используйте маску «D:*».
- Если нужно исключить только файлы с расширением .doc, используйте маску «*.doc».
- Если имя исполняемого файла содержит определенное количество символов (и символы могут меняться), причем известна только первая буква имени (скажем, «D»), следует использовать следующий формат: «D????.exe». Вопросительные знаки замещают отсутствующие (неизвестные) символы.



ПРИМЕЧАНИЕ.
Угроза в файле не будет обнаружена модулем защиты файловой системы в режиме реального времени или модулем сканирования компьютера, если файл соответствует критериям для исключения из сканирования.

Столбцы

Путь — путь к исключаемым файлам и папкам.

Угроза— если рядом с исключаемым файлом указано имя угрозы, файл не сканируется только на наличие этой угрозы, а не исключается из сканирования полностью. Если этот файл позже окажется заражен другой вредоносной программой, модуль защиты от вирусов ее обнаружит. Этот тип исключений можно использовать только для определенных типов заражений. Создать такое исключение можно либо в окне предупреждения об угрозе, в котором сообщается о заражении (последовательно щелкните элементы **Показать расширенные параметры** > **Исключить из обнаружения**), либо в разделе **Сервис** > **Карантин**, щелкнув правой кнопкой мыши файл на карантине и выбрав в контекстном меню пункт **Восстановить и исключить из обнаружения**.

Элементы управления

Добавить — команда, исключающая объекты из сканирования.

Изменить — команда, изменяющая выделенные записи.

Удалить — команда, удаляющая выделенные записи..

3.9.1.13 Настройка параметров модуля 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, подлежащие сканированию;
- сочетание различных методов обнаружения угроз;
- уровни очистки и т. д.

Чтобы открыть окно параметров, щелкните **Настройка параметров модуля ThreatSense** в окне дополнительных настроек 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 файловой системы в режиме реального времени.
- Сканирование в состоянии простоя.
- Сканирование файлов, исполняемых при запуске системы.
- 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: выполняется сканирование на наличие угроз, которые атакуют оперативную память системы.

Загрузочные секторы: загрузочные секторы сканируются на наличие вирусов в основной загрузочной записи.

Почтовые файлы: программа поддерживает расширения DBX (Outlook Express) и EML.

Архивы: программа поддерживает расширения 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: самораспаковывающиеся архивы (файлы с расширением SFX) — это архивы, которым для распаковки не нужны специальные программы.

Упаковщики: в отличие от стандартных типов архивов упаковщики, будучи выполненными, распаковываются в память. Благодаря эмуляции кода модуль сканирования распознает не только стандартные статические упаковщики (UPX, yoda, ASPack, FGS и т. д.), но и множество других типов упаковщиков.

Параметры сканирования

Выберите способы сканирования системы на предмет заражений. Доступны указанные ниже варианты.

Эвристический анализ: анализ злонамеренной активности программ с помощью специального алгоритма. Главным достоинством этого метода является способность идентифицировать вредоносные программы, сведения о которых отсутствуют в существующей базе данных сигнатур вирусов. Недостатком же является вероятность (очень небольшая) ложных тревог.

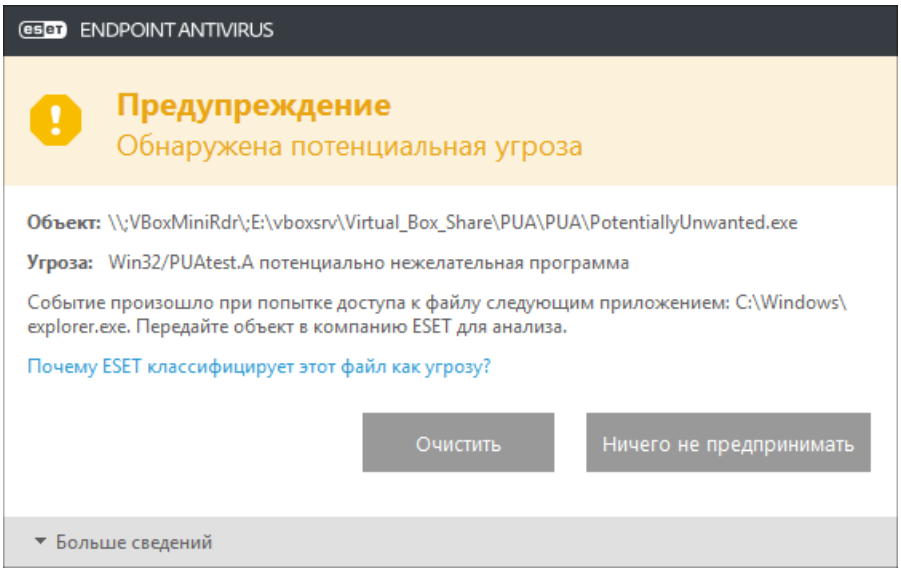
Расширенная эвристика/DNA/Сигнатуры Smart: метод расширенной эвристики базируется на уникальном эвристическом алгоритме, разработанном компанией ESET, оптимизированном для обнаружения компьютерных червей и троянских программ и написанном на языках программирования высокого уровня. Использование расширенной 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).

Потенциально нежелательное приложение содержит рекламу, устанавливает панели инструментов или выполняет другие неясные функции. В некоторых ситуациях может показаться, что преимущества такого приложения перевешивают риски. Поэтому компания ESET помещает эти приложения в категорию незначительного риска, в отличие от других вредоносных программ, например троянских программ или червей.

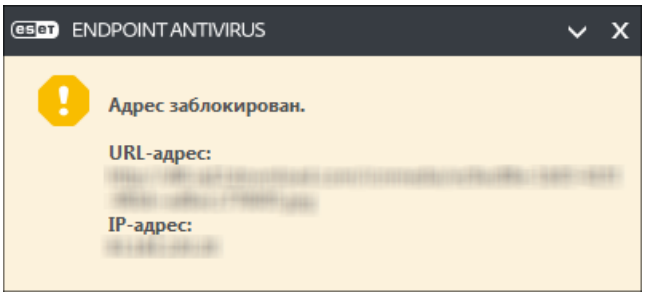
Предупреждение — обнаружена потенциальная угроза

Когда обнаруживается потенциально нежелательное приложение, вы можете самостоятельно решить, какое действие нужно выполнить.

1. **Очистить/отключить**: действие прекращается, и потенциальная угроза не попадает в систему.
2. **Ничего не предпринимать**: эта функция позволяет потенциальной угрозе проникнуть на компьютер.
3. Чтобы разрешить приложению и впредь работать на компьютере без прерываний, щелкните элемент **Дополнительные сведения/показать параметры** и установите флажок **Исключить из проверки**.

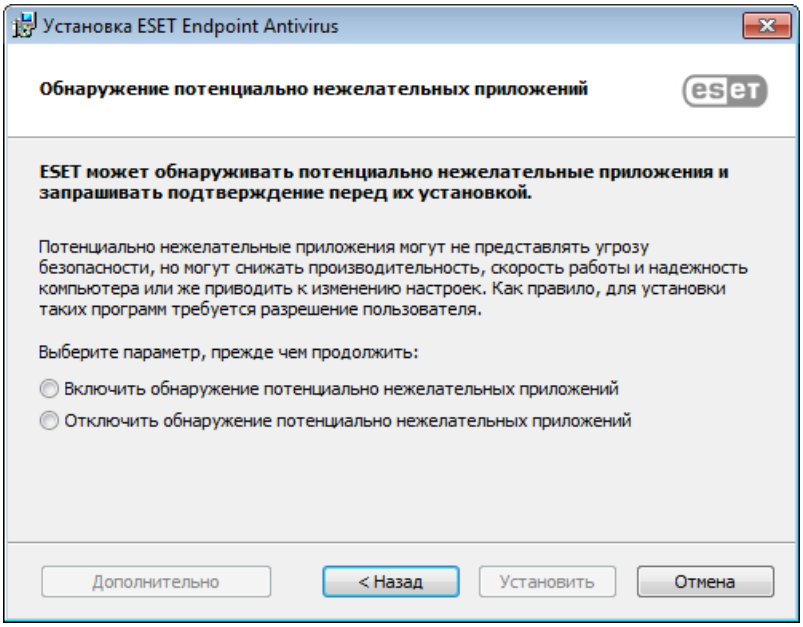


Если обнаружено потенциально нежелательное приложение и его невозможно очистить, в правом нижнем углу экрана отобразится окно уведомлений **Адрес заблокирован**. Дополнительные сведения об этом событии можно получить, последовательно щелкнув в главном меню элементы **Сервис** > **Файлы журнала** > **Отфильтрованные веб-сайты**.



Потенциально нежелательные приложения — параметры

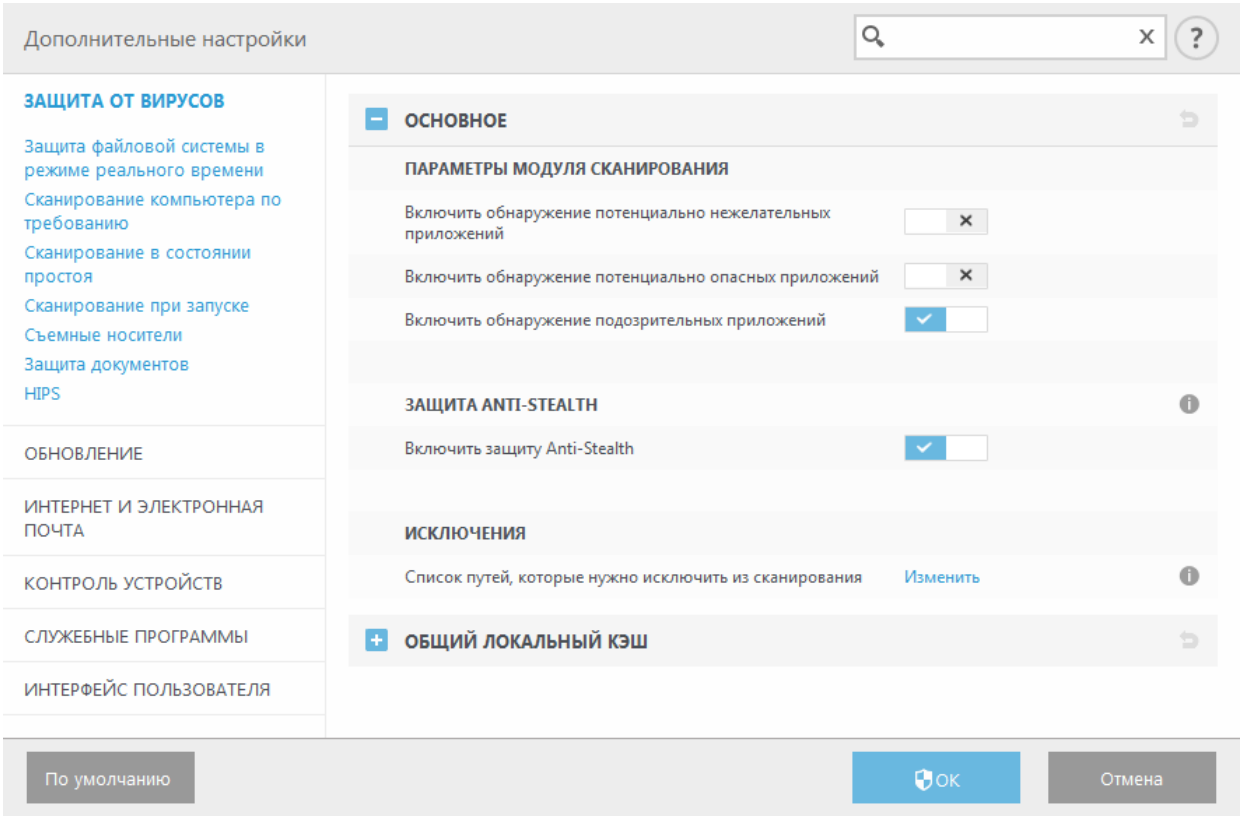
При установке программы ESET можно включить обнаружение потенциально нежелательных приложений (см. изображение ниже).



ВНИМАНИЕ!
Потенциально нежелательные приложения могут устанавливать рекламные программы и панели инструментов или содержать рекламу и другие нежелательные и небезопасные программные компоненты.

Эти параметры можно в любое время изменить в разделе параметров программы. Чтобы включить или отключить обнаружение потенциально нежелательных, небезопасных или подозрительных приложений, следуйте нижеприведенным инструкциям.

1. Откройте программу ESET. Как открыть мой продукт ESET?
2. Нажмите клавишу **F5**, чтобы перейти к разделу **Дополнительные настройки**.
3. Щелкните элемент **Антивирус** и на свое усмотрение включите или отключите параметры **Включить обнаружение потенциально нежелательных приложений**, **Включить обнаружение потенциально опасных приложений** и **Включить обнаружение подозрительных приложений**. Чтобы сохранить настройки, нажмите кнопку **ОК**.



Потенциально нежелательные приложения — оболочки

Оболочка — специальное приложение, используемое на некоторых файлообменных ресурсах. Это стороннее средство, устанавливающее программу, которую нужно загрузить, в комплекте с другим программным обеспечением, например панелью инструментов или рекламой, которые изменяют домашнюю страницу браузера или параметры поиска. При этом файлообменные ресурсы часто не уведомляют производителя программного обеспечения или пользователей о внесенных изменениях, а отказаться от этих изменений непросто. Именно поэтому компания ESET считает оболочки потенциально нежелательными приложениями и дает пользователям возможность отказаться от их загрузки.

Обновленную версию этой страницы справочной системы см. в этой статье базы знаний ESET.

Потенциально опасные приложения. Потенциально опасные приложения — это обозначение для законных коммерческих программ, таких как средства удаленного доступа, приложения для взлома паролей и клавиатурные шпионы (программы, записывающие каждое нажатие клавиши на клавиатуре). По умолчанию этот параметр отключен.

Очистка

Параметры очистки определяют поведение модуля сканирования при очистке зараженных файлов. Предусмотрено три уровня очистки.

Без очистки: зараженные файлы не будут очищаться автоматически. Программа выводит на экран окно предупреждения и предлагает пользователю выбрать действие. Этот уровень предназначен для более опытных пользователей, которые знают о действиях, которые следует предпринимать в случае заражения.

Стандартная очистка: программа пытается автоматически очистить или удалить зараженный файл на основе предварительно определенного действия (в зависимости от типа заражения). Обнаружение и удаление зараженных файлов сопровождается уведомлением, отображающимся в правом нижнем углу экрана. Если невозможно выбрать правильное действие автоматически, программа предложит выбрать другое действие. То же самое произойдет в том случае, если предварительно определенное действие невозможно выполнить.

Тщательная очистка: программа очищает или удаляет все зараженные файлы. Исключение составляют только системные файлы. Если очистка невозможна, на экран выводится окно предупреждения, в котором пользователю предлагается выполнить определенное действие.

ВНИМАНИЕ!
Если в архиве содержатся зараженные файлы, существует два варианта обработки архива. В стандартном режиме (при стандартной очистке) целиком удаляется архив, все файлы в котором заражены. В режиме **Тщательная очистка** удаляется архив, в котором заражен хотя бы один файл, независимо от состояния остальных файлов.

Исключения

Расширением называется часть имени файла, отделенная от основной части точкой. Оно определяет тип файла и его содержимое. Этот раздел параметров ThreatSense позволяет определить типы файлов, подлежащих сканированию.

Другое

При настройке модуля ThreatSense также доступны представленные ниже параметры 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.

Регистрировать все объекты: если этот флажок установлен, в файле журнала будет содержаться информация обо всех просканированных файлах, в том числе незараженных. Например, если в архиве найден вирус, в журнале также будут перечислены незараженные файлы из архива.

Включить интеллектуальную оптимизацию: при включенной интеллектуальной оптимизации 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 интеллектуальная оптимизация отключена, при сканировании используются только пользовательские настройки ядра ThreatSense каждого модуля.

Сохранить отметку о времени последнего доступа: установите этот флажок, чтобы сохранять исходную отметку о времени доступа к сканируемым файлам, не обновляя ее (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 объекта. Если пользователь укажет здесь собственное значение, модуль защиты от вирусов прекратит сканирование объекта по истечении указанного времени вне зависимости от того, было ли сканирование завершено. 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. Значение по умолчанию: *не ограничено*.

ПРИМЕЧАНИЕ.
Не рекомендуется изменять значения по умолчанию, так как обычно для этого нет особой причины.

3.9.1.13.1 Исключения

Расширением называется часть имени файла, отделенная от основной части точкой. Оно определяет тип файла и его содержимое. Этот раздел параметров ThreatSense позволяет определить типы файлов, подлежащих сканированию.

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.

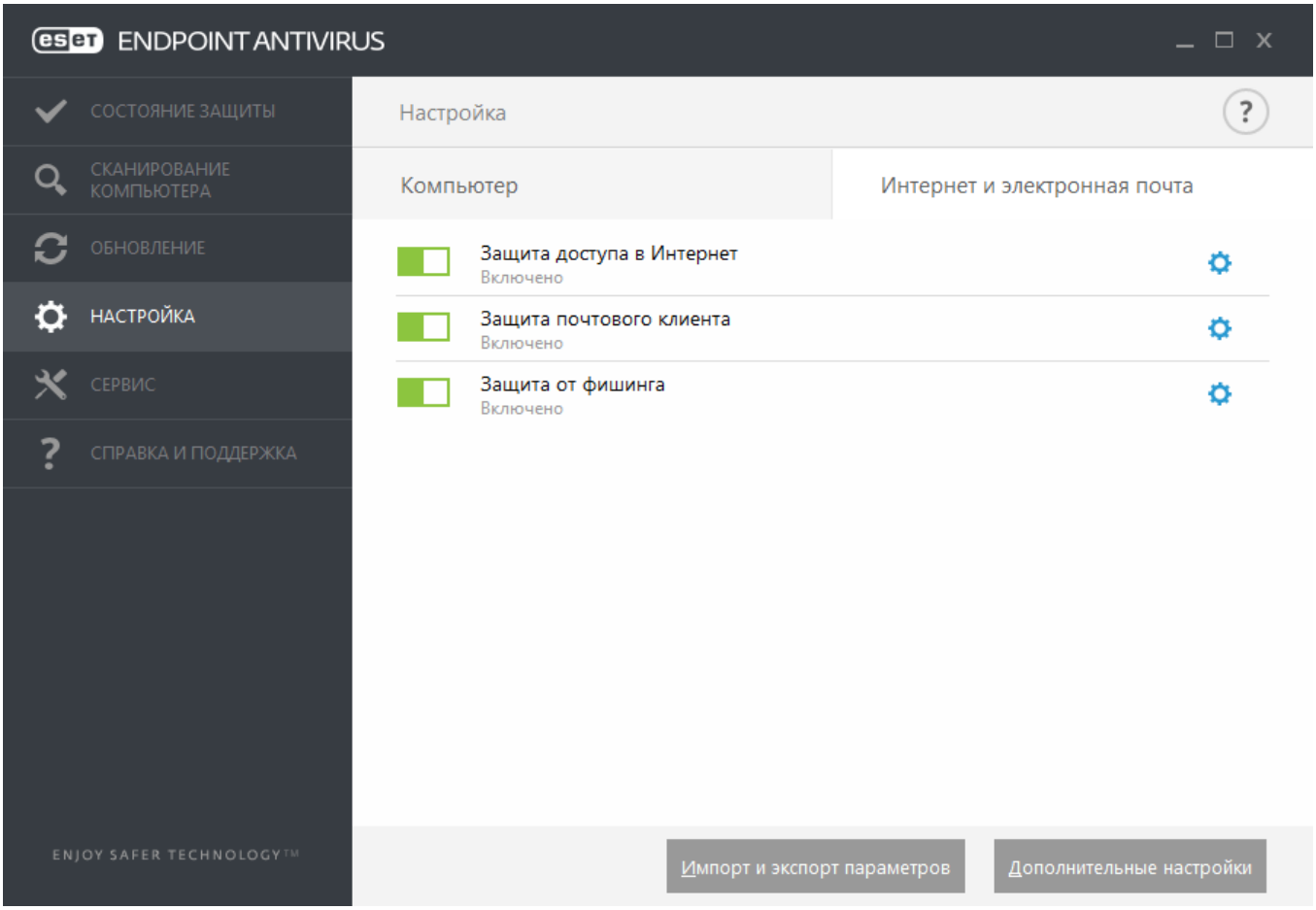
С помощью кнопок **Добавить** и **Удалить** можно изменять содержимое списка, разрешая или запрещая сканирование определенных расширений. Чтобы добавить в список новое расширение, щелкните **Добавить**, введите в пустое поле расширение и нажмите кнопку **ОК**. Выбрав **Введите несколько значений**, вы можете добавлять несколько расширений файлов, разделенных переводом строки, запятыми или точками с запятой. Если разрешен ввод нескольких значений, расширения будут отображаться в виде списка. Чтобы удалить расширение из списка, выберите его и нажмите кнопку **Удалить**. Для изменения выбранного расширения щелкните **Изменить**.

Возможно использование следующих специальных символов: ? (вопросительный знак). Звездочка вопросительный знак — любой отдельный символ.

ПРИМЕЧАНИЕ.
Чтобы расширение (тип файла) отображалось для всех файлов в операционной системе Windows, снимите флажок **Скрывать расширения для зарегистрированных типов файлов**, выбрав **Панель управления** > **Свойства папки** > **Вид**.

3.9.2 Интернет и электронная почта

Конфигурацию защиты доступа в Интернет и электронной почты можно найти, выбрав **Настройка** > **Интернет и электронная почта**. В этом окне предоставляется доступ к дополнительным параметрам программы.



Подключение к Интернету стало стандартной функцией персонального компьютера. К сожалению, Интернет стал также основной средой распространения вредоносного кода. Поэтому крайне важно уделить особое внимание **защите доступа в Интернет**.

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

Защита от фишинга представляет собой еще один уровень безопасности, который обеспечивает улучшенную защиту от незаконных веб-сайтов, пытающихся получить пароли и прочую конфиденциальную информацию. Функция защиты от фишинга доступна на панели **Настройка** в разделе **Интернет и электронная почта**. Для получения дополнительных сведений см. раздел Защита от фишинга.

Отключить: отключение защиты Интернета/электронной почты для веб-браузеров и почтовых клиентов  .

3.9.2.1 Фильтрация протоколов

Защита от вирусов протоколов приложений обеспечивается модулем сканирования ThreatSense, в котором объединены все современные методы сканирования для выявления вредоносных программ. Функция фильтрации протоколов работает автоматически вне зависимости от используемого веб-браузера и почтового клиента. Для редактирования настроек зашифрованных (SSL) соединений выберите элементы **Интернет и электронная почта** > **SSL**.

Включить фильтрацию содержимого, передаваемого по протоколам приложений: может использоваться для отключения фильтрации протоколов. Многие компоненты ESET Endpoint Antivirus (защита доступа в интернет, защита протоколов электронной почты, защита от фишинга и контроль доступа в Интернет) зависят от этого параметра и не смогут работать в случае его отключения.

Исключенные приложения: позволяет исключить указанные приложения из фильтрации протоколов. Полезно в случае, если фильтрация протоколов вызывает проблемы совместимости.

Исключенные IP-адреса: позволяет исключить указанные удаленные адреса из фильтрации протоколов. Полезно, если фильтрация протоколов вызывает проблемы совместимости.

Веб-клиенты и почтовые клиенты: (используется только в операционной системе Windows XP) позволяет выбрать приложения, трафик которых будет проходить фильтрацию протоколов вне зависимости от используемого порта.

3.9.2.1.1 Клиенты Интернета и электронной почты

ПРИМЕЧАНИЕ.
Начиная с ОС Windows Vista с пакетом обновления 1 и Windows Server 2008, для проверки сетевых соединений используется новая архитектура платформы фильтрации Windows (WFP). Так технология платформы фильтрации Windows использует особые методы отслеживания, раздел **Клиенты Интернета и электронной почты** недоступен.

В условиях перенасыщенности Интернета вредоносными программами безопасное посещение веб-страниц является важным аспектом защиты компьютера. Уязвимости веб-браузеров и мошеннические ссылки позволяют вредоносным программам незаметно проникать в систему. Именно поэтому в программном обеспечении ESET Endpoint Antivirus основное внимание уделяется обеспечению безопасности веб-браузеров. Каждое приложение, обращающееся к сети, может быть помечено как веб-браузер. Приложения, которые уже использовали протоколы для передачи данных или приложения, находящиеся по выбранному адресу, можно внести в список веб-клиентов и почтовых клиентов.

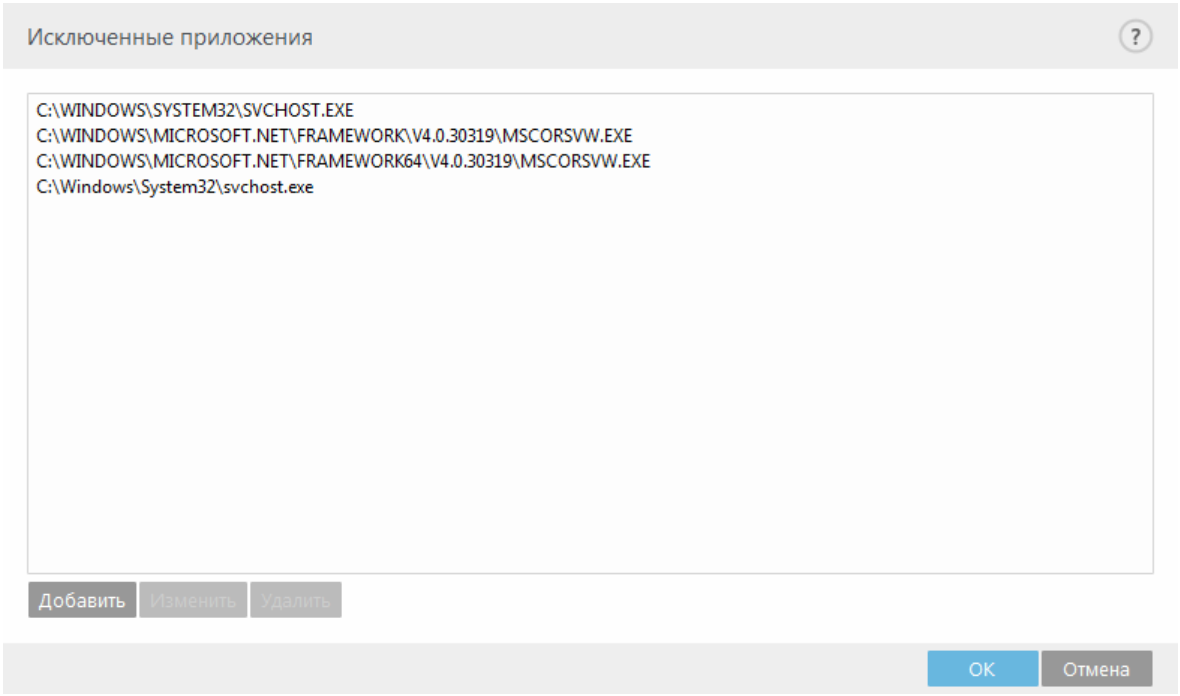
3.9.2.1.2 Исключенные приложения

Для исключения соединений определенных сетевых приложений из фильтрации протоколов добавьте их в список. Соединения выделенных приложений по протоколам HTTP/POP3/IMAP не будут проверяться на наличие угроз. Рекомендуется использовать этот метод, только если при включенной фильтрации протоколов приложения не функционируют надлежащим образом.

Чтобы приложения и службы, затронутые фильтрацией протоколов, начали автоматически отображаться, нажмите кнопку **Добавить**.

Изменить: изменение выбранных в списке записей.

Удалить: удаление выделенных записей из списка.



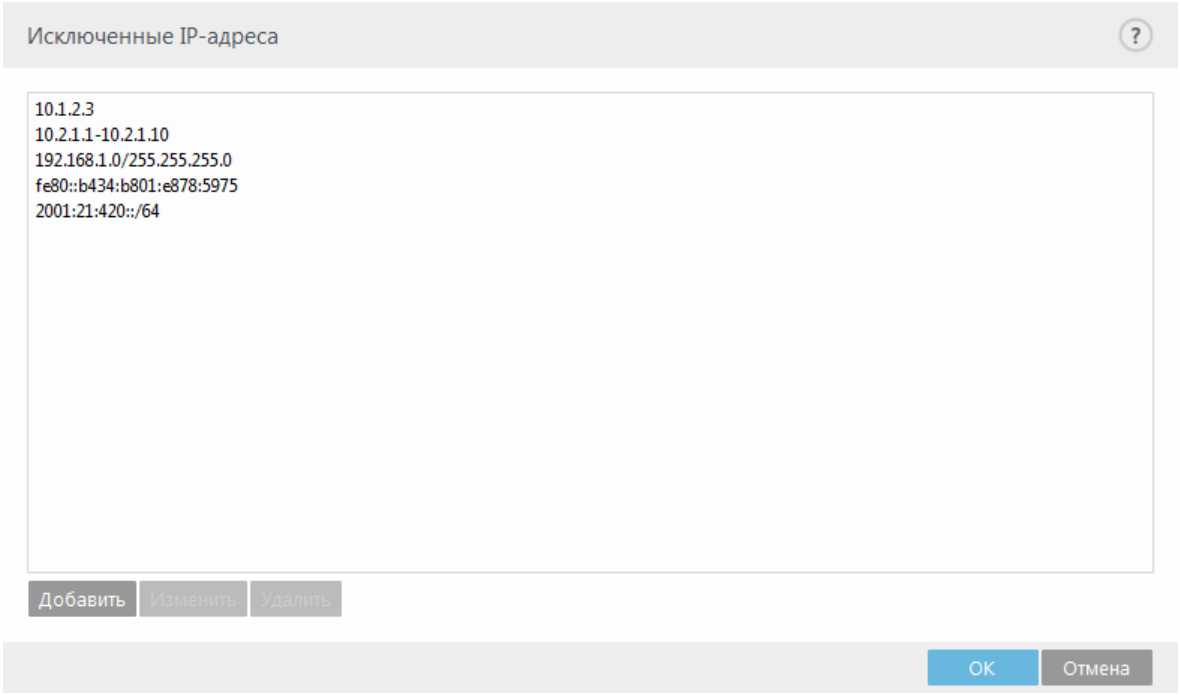
3.9.2.1.3 Исключенные IP-адреса

IP-адреса в этом списке будут исключены из фильтрации содержимого протоколов. Соединения по протоколам HTTP/POP3/IMAP, в которых участвуют выбранные адреса, не будут проверяться на наличие угроз. Этот параметр рекомендуется использовать только для заслуживающих доверия адресов.

Добавить: нажмите, чтобы добавить IP-адрес, диапазон адресов или подсеть удаленной конечной точки, к которой должно быть применено правило.

Изменить: изменение выбранных записей списка.

Удалить: удаление выделенных записей из списка.



3.9.2.1.4 SSL/TLS

ESET Endpoint Antivirus может проверять обмен данных посредством протокола SSL на наличие угроз. Можно использовать различные режимы сканирования для защищенных SSL-соединений, для которых используются доверенные сертификаты, неизвестные сертификаты или сертификаты, исключенные из проверки защищенных SSL-соединений.

Включить фильтрацию протоколов SSL/TLS: если фильтрация протоколов отключена, программа не сканирует обмен данными по протоколу SSL.

Режим фильтрации протоколов SSL/TLS доступен со следующими параметрами.

Автоматический режим: выберите этот вариант, чтобы сканировать все защищенные SSL-соединения за исключением защищенных сертификатами, исключенными из проверки. 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.

Интерактивный режим — при выполнении входа на новый защищенный SSL-сайт (с неизвестным сертификатом) на экран выводится диалоговое окно выбора. Этот режим позволяет создавать список сертификатов SSL, которые будут исключены из сканирования.

Блокировать шифрованное соединение с использованием устаревшего протокола SSL версии 2: соединения, использующие более раннюю версию протокола SSL, будут автоматически блокироваться.

Корневой сертификат

Корневой сертификат: для нормальной работы SSL-подключений в браузерах и почтовых клиентах необходимо добавить корневой сертификат ESET в список известных корневых сертификатов (издателей). Параметр **Добавить корневой сертификат к известным браузерам** должен быть активирован. Выберите этот параметр, чтобы автоматически добавить корневой сертификат ESET в известные браузеры (например, Opera и Firefox). Для браузеров, использующих системное хранилище сертификатов (например, Internet Explorer), сертификат добавляется автоматически.

Для установки сертификата в неподдерживаемые браузеры выберите **Просмотреть сертификат** > **Дополнительно** > **Копировать в файл...**, а затем вручную импортируйте его в браузер.

Срок действия сертификата

Если проверить сертификат с помощью хранилища сертификатов TRCA не удается. В некоторых случаях сертификат невозможно проверить с помощью хранилища доверенных корневых сертификатов сертифицирующих органов (TRCA). Это значит, что у сертификата существует собственная подпись какого-либо другого субъекта (например, администратора веб-сервера или небольшой компании) и принятие решения о выборе такого сертификата как доверенного не всегда представляет опасность. Большинство крупных компаний (например, банки) используют сертификаты, подписанные TRCA. Если установлен флажок **Запрашивать действительность сертификата** (по умолчанию), пользователю будет предложено выбрать действие, которое следует предпринять во время установки зашифрованного соединения. Можно выбрать вариант **Блокировать соединения, использующие сертификат**, чтобы всегда разрывать зашифрованные соединения с сайтом, использующим непроверенный сертификат.

Если сертификат недействителен или поврежден. Это значит, что истек срок действия сертификата или же используется неверное собственное заверение. В этом случае рекомендуется выбрать **Блокировать соединения, использующие сертификат**.

Список известных сертификатов позволяет настроить поведение ESET Endpoint Antivirus в отношении конкретных сертификатов SSL.

3.9.2.1.4.1 Шифрованное соединение SSL

Если в системе настроено сканирование протокола SSL, диалоговое окно с запросом на выбор действия будет отображаться в двух случаях.

Во-первых, если веб-сайт использует непроверенный или недействительный сертификат, а продукт ESET Endpoint Antivirus настроен на выдачу запросов в таких случаях (по умолчанию запросы отображаются для непроверенных сертификатов, а для недействительных — нет), появится запрос на **блокирование** или **разрешение** подключения.

Во-вторых, если в качестве **режима фильтрации протокола SSL** 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 Endpoint Antivirus должна SSL-трафик **игнорировать**.

В каждом их этих случаев пользователь может сохранить в системе выбранное действие. Сохраненные действия хранятся в списке **Список известных сертификатов**.

3.9.2.1.4.2 Список известных сертификатов

Список известных сертификатов позволяет настроить поведение ESET Endpoint Antivirus в отношении конкретных сертификатов SSL, а также настроить запоминание действий пользователя, если в разделе **Режим фильтрации протоколов SSL/TLS** выбран **Интерактивный режим**. Список можно просмотреть и отредактировать, последовательно выбрав элементы **Дополнительные настройки** (F5) > **Интернет и электронная почта** > **SSL/TLS** > **Список известных сертификатов**.

Окно **Список известных сертификатов** содержит указанные ниже пункты.

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, вне зависимости 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. Выберите **Автоматически**, чтобы сканировать в автоматическом режиме и запрашивать действия в интерактивном. Выберите **Запрашивать**, чтобы всегда запрашивать действия пользователя.

Элементы управления

Добавить: сертификат можно загрузить вручную как файл с расширением *.cer*, *.crt* или *.pem*. Щелкните элемент **Файл**, чтобы передать локальный сертификат, или щелкните **URL-адрес**, чтобы указать расположение сертификата в Интернете.

Изменить: выберите сертификат, который нужно настроить, и нажмите кнопку **Изменить**.

Удалить: выберите сертификат, который нужно удалить, и нажмите кнопку **Удалить**.

ОК/Отмена: нажмите **ОК** для сохранения изменений или **Отмена** для их отмены.

3.9.2.2 Защита почтового клиента

3.9.2.2.1 Почтовые клиенты

Интеграция ESET Endpoint Antivirus с почтовыми клиентами увеличивает уровень активной защиты от вредоносного кода в сообщениях электронной почты. Если используемый почтовый клиент поддерживается, в ESET Endpoint Antivirus можно настроить интеграцию. Если интеграция активирована, панель инструментов ESET Endpoint Antivirus вставляется непосредственно в почтовый клиент, обеспечивая более эффективную защиту электронной почты (панель инструментов для последних версий Почты Windows Live не вставляется). Параметры интеграции доступны в разделе **Настройка** > **Дополнительные настройки** > **Интернет и электронная почта** > **Защита почтового клиента** > **Почтовые клиенты**.

Интеграция с почтовым клиентом

В настоящий момент поддерживаются следующие почтовые клиенты: Microsoft Outlook, Outlook Express, Почта Windows и Почта Windows Live. Защита электронной почты реализована в этих программах в виде подключаемого модуля. 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 почтовых клиентов и их версий см. в статье базы знаний ESET.

Даже если интеграция отключена, почтовые клиенты остаются защищены соответствующим модулем (для протоколов POP3, IMAP).

Включите параметр **Отключить проверку при изменении содержимого папки "Входящие"**, если при работе с почтовым клиентом наблюдается замедление работы системы (только для MS Outlook). Это возможно при извлечении сообщения электронной почты из хранилища Kerio Outlook Connector Store.

Сканируемая электронная почта

Включить защиту электронной почты с помощью подключаемых модулей клиента. Даже если защита электронной почты с помощью почтового клиента отключена, проверка почтового клиента посредством фильтрации протоколов все равно будет работать.
Полученные сообщения: включает или отключает проверку входящих сообщений.
Отправленные сообщения: включает или отключает проверку отправленных сообщений.
Прочитанные сообщения: включает или отключает проверку прочитанных сообщений.

Действие, применяемое к зараженному сообщению

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: зараженные сообщения будут автоматически перемещаться в указанную папку.

Папка: выбор папки, в которую будут перемещаться обнаруженные зараженные сообщения электронной почты.

Повторить сканирование после обновления: включает или отключает повторное сканирование после обновления базы данных сигнатур вирусов.

Включить результаты сканирования другими модулями: если установлен этот флажок, модуль защиты электронной почты будет принимать результаты сканирования от других модулей защиты (сканирование каталогов POP3, IMAP).

ПРИМЕЧАНИЕ.
Рекомендуем включить параметры **Включить защиту электронной почты с помощью подключаемых модулей клиента** и **Включить защиту электронной почты с помощью фильтрации протоколов** («Дополнительные настройки» (F5) > «Интернет и электронная почта» > «Защита почтового клиента» > «Протоколы электронной почты»).

3.9.2.2.2 Протоколы электронной почты

IMAP и POP3 — самые распространенные протоколы, используемый для получения электронной почты в почтовых клиентах. ESET Endpoint Antivirus обеспечивает защиту этих протоколов вне зависимости от используемого почтового клиента и без необходимости перенастраивать почтовый клиент.

Настроить проверку протоколов IMAP/IMAPS и POP3/POP3S можно в дополнительных настройках. Чтобы открыть эти настройки, последовательно выберите элементы **Интернет и электронная почта** > **Защита почтового клиента** > **Протоколы электронной почты**.

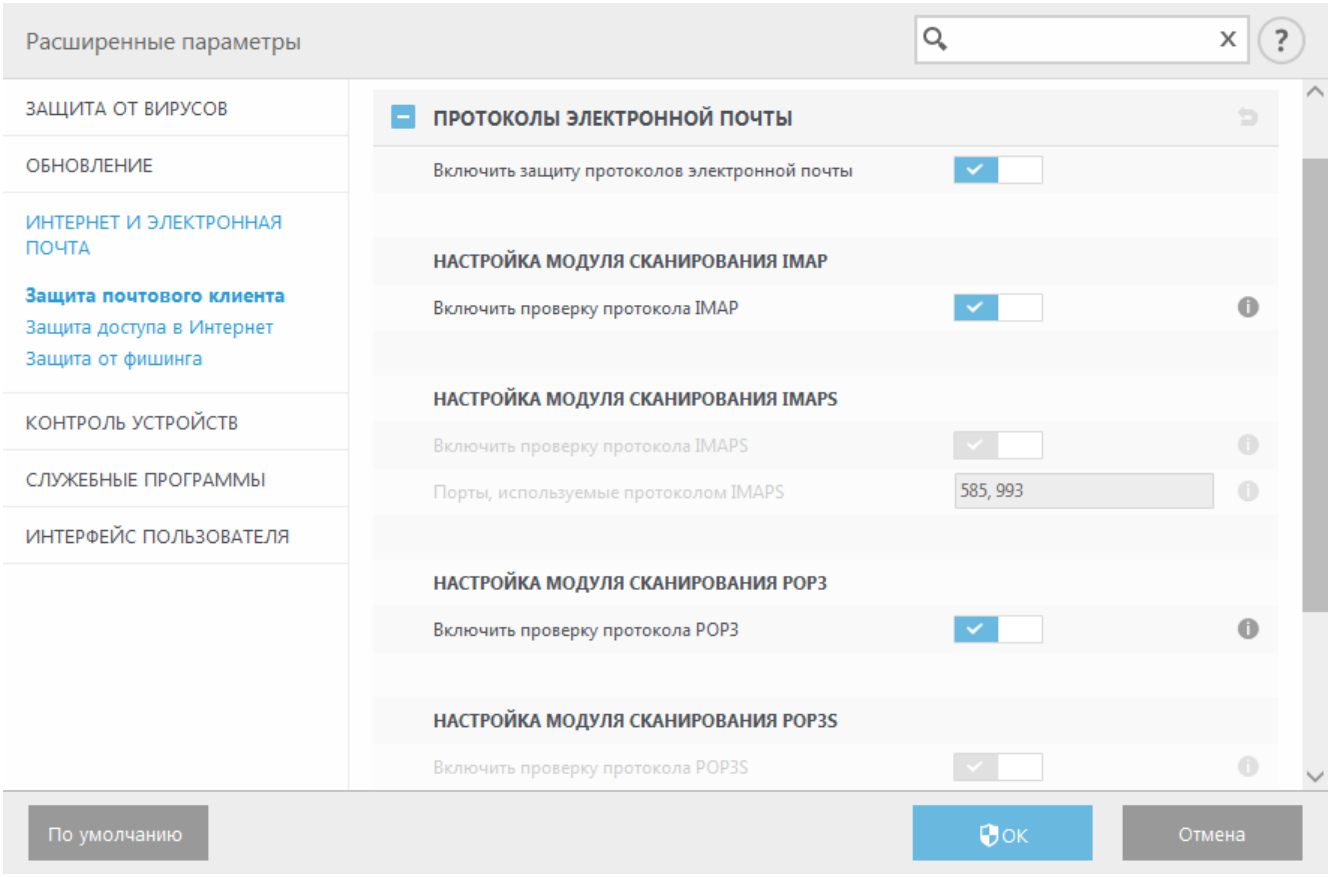
Включить защиту протоколов электронной почты: позволяет включить проверку протоколов электронной почты.

В Windows Vista и более поздних версиях протоколы IMAP и POP3 автоматически определяются и сканируются на всех портах. В Windows XP для всех приложений сканируются только настроенные **порты, используемые протоколом IMAP или POP3**. Все порты также сканируются для приложений, отмеченных как веб-клиенты и почтовые клиенты.

ESET Endpoint Antivirus также поддерживает сканирование протоколов IMAPS и POP3S, которые для передачи информации между сервером и клиентом используют зашифрованный канал. ESET Endpoint Antivirus

проверяет соединения, использующие методы шифрования SSL и TLS. Программа будет выполнять сканирование только трафика на **портах, используемых протоколом IMAPS/POP3S**, вне зависимости от версии операционной системы.

Зашифрованные соединения не будут сканироваться, если используются параметры по умолчанию. Для включения сканирования зашифрованных соединений перейдите к элементу SSL/TLS в разделе «Дополнительные настройки», выберите элементы **Интернет и электронная почта** > **SSL/TLS**, а затем щелкните элемент **Включить фильтрацию протоколов SSL/TLS**.



3.9.2.2.3 Предупреждения и уведомления

Защита электронной почты обеспечивает контроль безопасности обмена данными по протоколам POP3 и IMAP. При использовании подключаемого модуля для Microsoft Outlook и других почтовых клиентов ESET Endpoint Antivirus позволяет контролировать весь обмен данными, осуществляемый почтовым клиентом (по протоколам POP3, MAPI, IMAP, HTTP). При проверке входящих сообщений программа использует все современные методы сканирования, обеспечиваемые модулем сканирования ThreatSense. Это позволяет обнаруживать вредоносные программы даже до того, как данные о них попадают в базу данных сигнатур вирусов. Сканирование соединений по протоколам POP3 и IMAP не зависит от используемого почтового клиента.

Параметры для этой функции настраиваются в **Advanced setup**, раздел **Интернет и электронная почта** > **Защита почтового клиента** > **Предупреждения и уведомления**.

Настройка параметров модуля ThreatSense — расширенная настройка модуля сканирования для защиты от вирусов, которая позволяет настраивать объекты сканирования, методы обнаружения и т. д. Нажмите для вывода на экран окна подробной настройки модуля сканирования.

После проверки к сообщению электронной почты может быть прикреплено уведомление с результатами сканирования. Вы можете выбрать **Добавление уведомлений к полученным и прочитанным сообщениям, Добавление примечаний в поле темы полученных и прочитанных зараженных сообщений** или **Добавление уведомлений к отправленным сообщениям**. Обратите внимание, что в некоторых случаях уведомления могут быть опущены в проблемных HTML-сообщениях или сфабрикованы некоторыми вирусами. 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 будут добавляться вообще.
- **Только для инфицированных сообщений**: будут отмечены только сообщения, содержащие злонамеренные программы (по умолчанию).
- **Во все просканированные сообщения электронной почты**: программа будет добавлять уведомления ко всем просканированным сообщениям электронной почты.

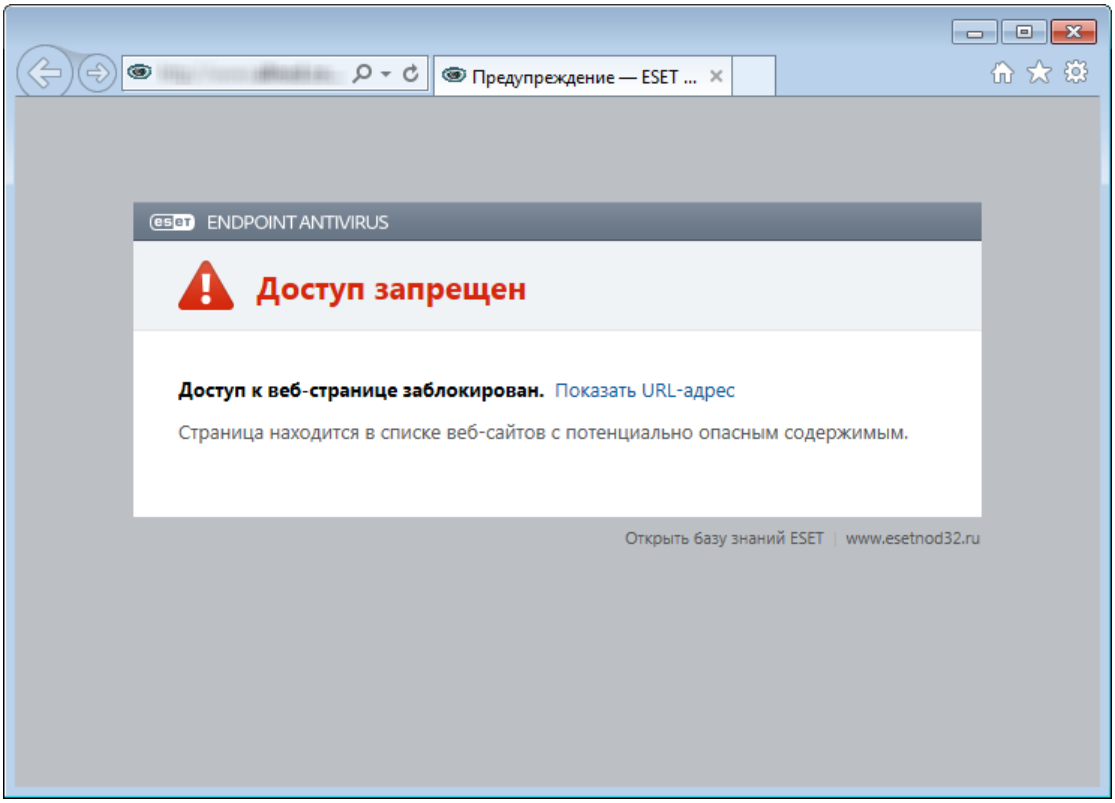
Добавление примечаний в поле темы отправленных сообщений — установите этот флажок, если необходимо, чтобы защита электронной почты добавляла предупреждения о вирусах в тему зараженных сообщений. Эта функция позволяет осуществлять простую фильтрацию зараженных сообщений по теме (если поддерживается почтовым клиентом). Также она повышает уровень доверия для получателя, а в случае обнаружения заражения предоставляет важную информацию об уровне угрозы для конкретного сообщения или отправителя.

Шаблон добавления к теме зараженных писем: этот шаблон можно изменить, если нужно отредактировать формат префикса, добавляемого ко всем зараженным сообщениям. Эта функция заменит тему сообщения *Hello* при заданном значении префикса *[virus]* на такой формат: *[virus] Hello*. Переменная *%VIRUSNAME%* представляет обнаруженную угрозу.

3.9.2.3 Защита доступа в Интернет

Подключение к Интернету стало стандартной функцией большинства персональных компьютеров. К сожалению, Интернет стал также основной средой распространения вредоносного кода. Функция защиты доступа в Интернет отслеживает соединения между веб-браузерами и удаленными серверами в соответствии с правилами протоколов HTTP (протокол переноса гипертекста) и HTTPS (зашифрованный обмен данными).

Доступ к веб-страницам, которые содержат заведомо вредоносное содержимое, блокируется перед его загрузкой. Если обнаруживается вредоносное содержимое, все другие веб-страницы сканируются модулем сканирования ThreatSense. Защита доступа в Интернет предполагает два уровня: блокировка по «черному» списку и блокировка по содержимому.



Настоятельно рекомендуется не отключать защиту доступа в Интернет. Чтобы получить доступ к этой функции, в главном окне программы ESET Endpoint Antivirus выберите **Настройка** > **Интернет и электронная почта** > **Защита доступа в Интернет**.

В разделе **Дополнительные настройки** (F5) > **Интернет и электронная почта** > **Защита доступа в Интернет** доступны указанные ниже варианты.

- **Веб-протоколы** — дает возможность настроить отслеживание в стандартных протоколах, которые используются в большинстве веб-браузеров.
- **Управление URL-адресами**: здесь можно задавать HTTP-адреса, которые следует блокировать, разрешить или исключать из проверки.
- **Настройка параметров модуля ThreatSense**. Это расширенная настройка модуля сканирования. Она дает возможность настраивать определенные параметры, например тип сканируемых объектов (сообщения электронной почты, архивы и т. д.), методы обнаружения для защиты доступа в Интернет и пр.

3.9.2.3.1 Веб-протоколы

По умолчанию ESET Endpoint Antivirus настроен на отслеживание протокола HTTP, используемого большинством интернет-браузеров.

В Windows Vista и более поздних версиях, HTTP-трафик отслеживается для всех портов и приложений. В Windows XP можно изменить **порты, используемые протоколом HTTP**. Для этого последовательно выберите элементы **Дополнительные настройки** (F5) > **Интернет и электронная почта** > **Защита доступа в интернет** > **Веб-протоколы** > **Настройка модуля сканирования HTTP**. HTTP-трафик всех приложений отслеживается на указанных портах и все порты для приложений помечены как Клиенты Интернета и электронной почты.

ESET Endpoint Antivirus также поддерживает проверку протокола HTTPS. В этом типе соединения для передачи информации между сервером и клиентом используется зашифрованный канал. ESET Endpoint Antivirus проверяет соединения, использующие методы шифрования SSL и TLS. Программа сканирует только те порты, которые указаны в списке **Порты, используемые протоколом HTTPS**, вне зависимости от версии операционной системы.

По умолчанию сканирование зашифрованных соединений отключено. Для включения сканирования зашифрованных соединений перейдите к элементу SSL/TLS в разделе «Дополнительные настройки», выберите элементы **Интернет и электронная почта** > **SSL/TLS**, а затем щелкните элемент **Включить фильтрацию протоколов SSL/TLS**.

3.9.2.3.2 Управление URL-адресами

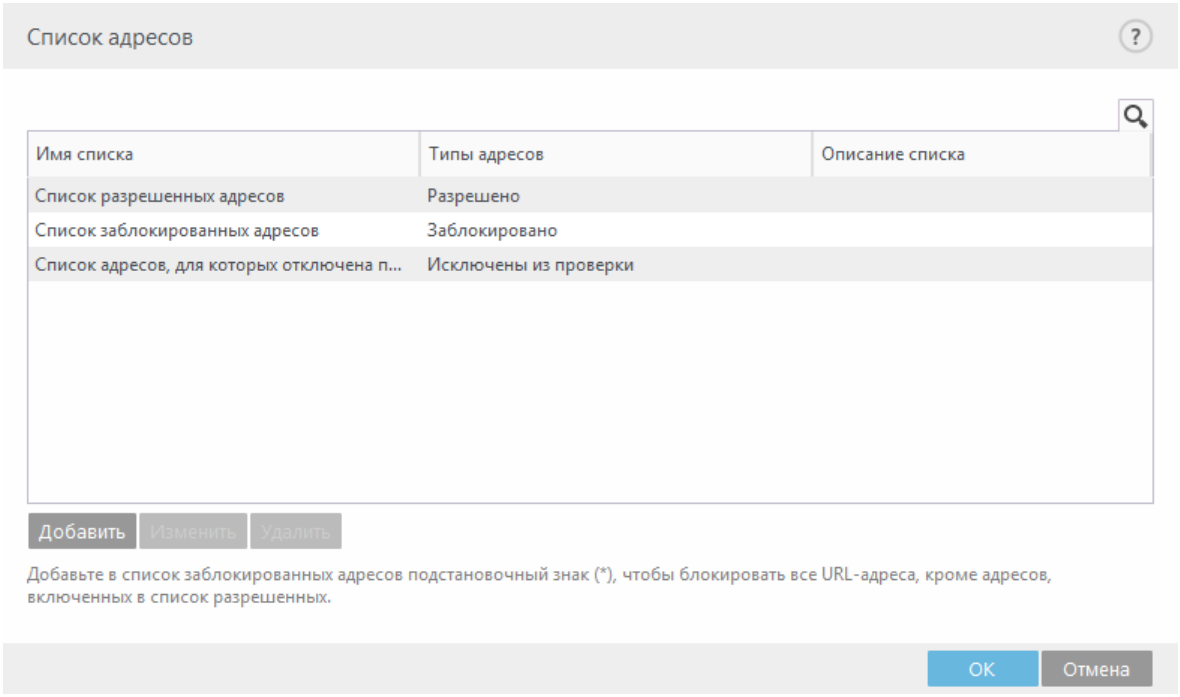
В разделе управления URL-адресами можно задавать HTTP-адреса, которые будут блокироваться, разрешаться или исключаться из проверки.

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 отключена проверка**, загружаются без проверки на вредоносный код.

Если кроме HTTP-сайтов вы также хотите фильтровать веб-сайты, использующие протокол HTTPS, выберите **Включить фильтрацию протокола SSL**. В противном случае в список будут добавлены только посещенные вами домены HTTPS-сайтов, а не полный URL-адрес.

Во всех списках можно использовать символы шаблона «*» (звездочка) и «?» (вопросительный знак). Звездочка означает любое количество символов, а вопросительный знак — только один символ. Работать с содержимым списка исключенных адресов следует особенно аккуратно, так как он должен содержать только доверенные и безопасные адреса. Точно так же нужно убедиться в том, что символы шаблона 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**.

Если вы хотите заблокировать все HTTP-адреса, кроме адресов, включенных в активный **список разрешенных адресов**, добавьте символ звездочки (*) в активный **список заблокированных адресов**.



Добавить — создание нового списка, дополняющего уже имеющиеся. 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 этот пункт для добавления или удаления адресов из списков.

Удалить — удаление существующих списков. Только для списков, созданных посредством команды **Добавить**. Удаление списков по умолчанию невозможно.

3.9.2.4 Защита от фишинга

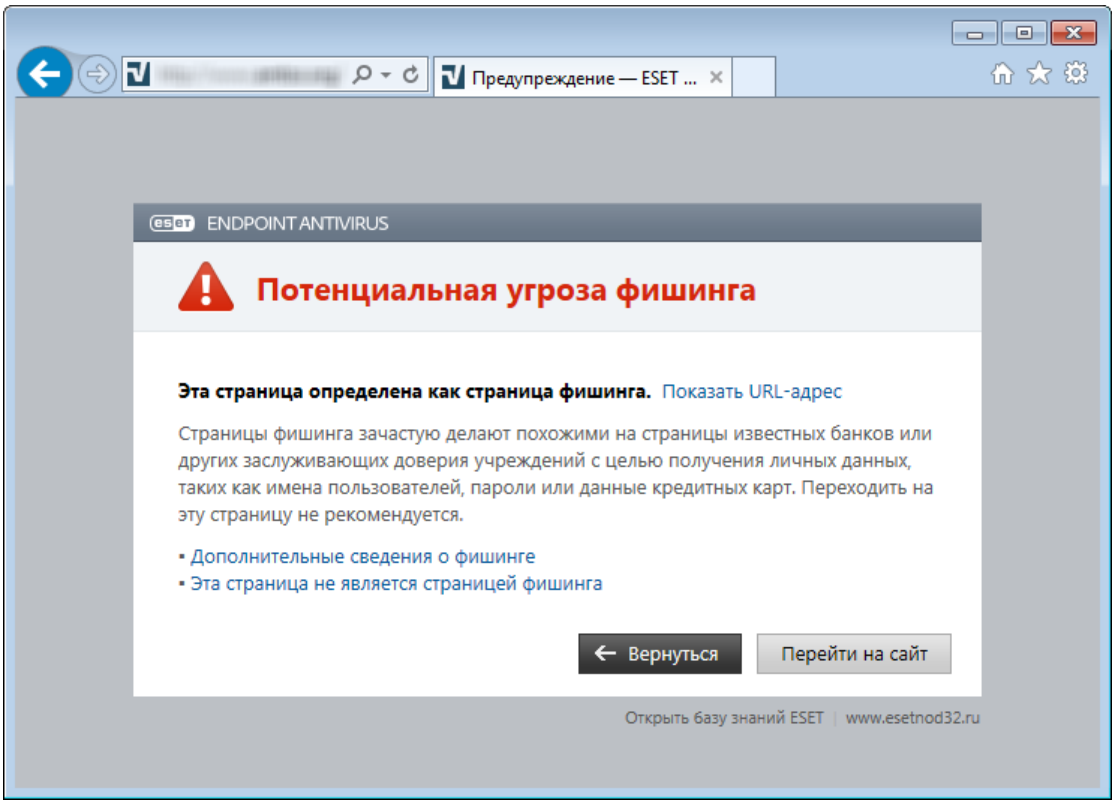
Термин «фишинг» обозначает преступную деятельность, в рамках которой используется социальная инженерия (манипулирование пользователями, направленное на получение конфиденциальной информации). Фишинг часто используется для получения доступа к конфиденциальным сведениям, таким как номера банковских счетов, PIN-коды и т. п. Дополнительные сведения об этой деятельности приведены в глоссарии. Программа ESET Endpoint Antivirus обеспечивает защиту от фишинга: веб-страницы, которые заведомо распространяют такой тип содержимого, могут быть заблокированы.

Настоятельно рекомендуется включить защиту от фишинга в программе ESET Endpoint Antivirus. Для этого нужно в окне **Дополнительные настройки** (F5) последовательно щелкнуть элементы **Интернет и электронная почта** > **Защита от фишинга**.

Дополнительные сведения о защите от фишинга в программе ESET Endpoint Antivirus см. в статье нашей базы знаний.

Доступ к фишинговому веб-сайту

Когда открывается фишинговый веб-сайт, в веб-браузере отображается следующее диалоговое окно. Если вы все равно хотите открыть этот веб-сайт, щелкните элемент **Перейти на сайт** (не рекомендуется).



ПРИМЕЧАНИЕ.
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** (F5) последовательно щелкните элементы **Интернет и электронная почта** > **Защита доступа в Интернет** > **Управление URL-адресами** > **Список адресов**, выберите команду **Изменить** и добавьте необходимый веб-сайт в список.

Сообщение о фишинговом сайте

Ссылка Сообщить позволяет сообщить о фишинговом или вредоносном веб-сайте в компанию ESET с целью проведения его анализа.

ПРИМЕЧАНИЕ.
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.

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.).

3.9.3 Обновление программы

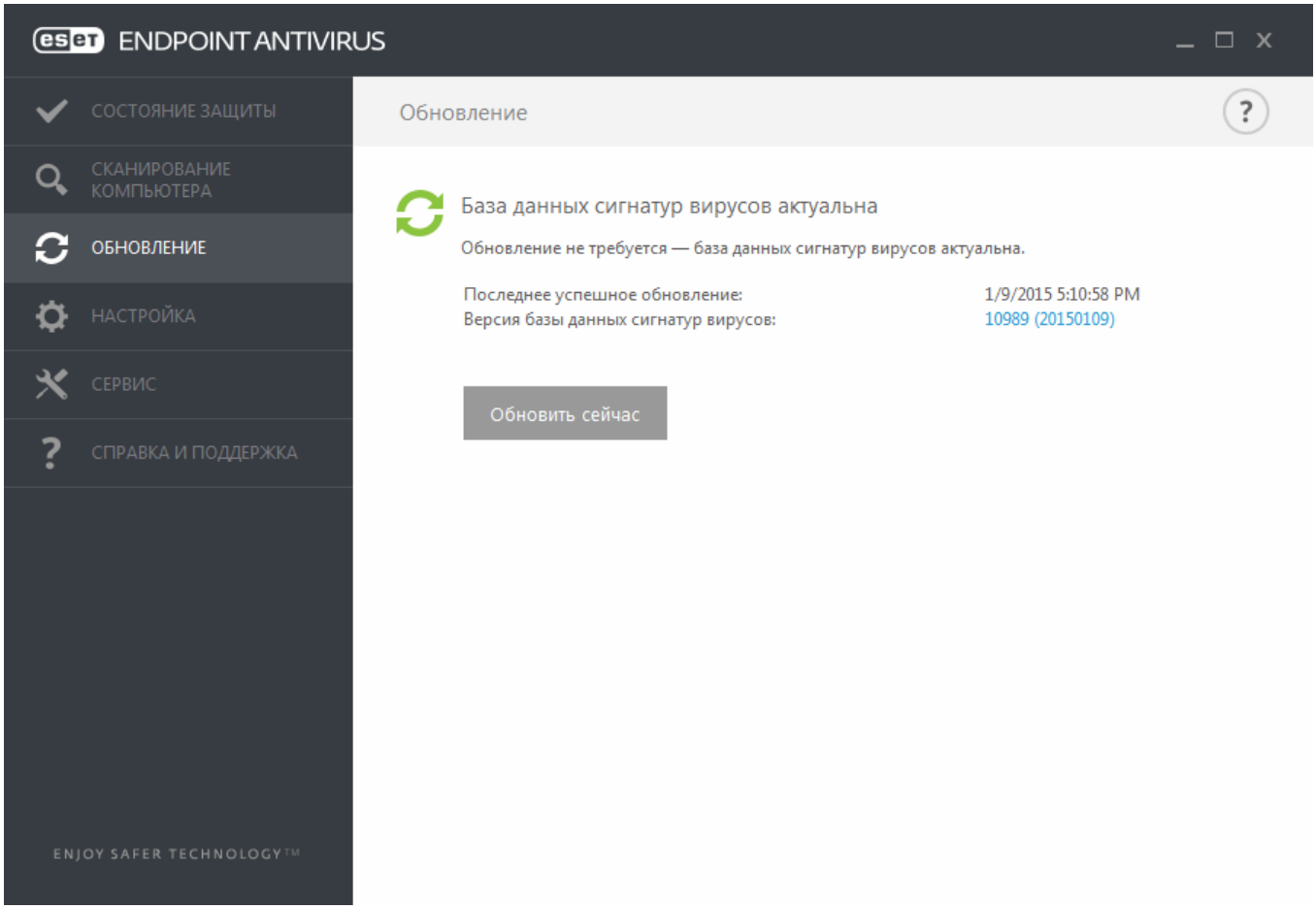
Регулярное обновление ESET Endpoint Antivirus — лучший способ добиться максимального уровня безопасности компьютера. Модуль обновления поддерживает актуальность программы двумя способами: путем обновления базы данных сигнатур вирусов и путем обновления компонентов системы.

Выбрав пункт **Обновление** в главном окне программы, можно получить информацию о текущем состоянии обновления, в том числе дату и время последнего успешно выполненного обновления, а также сведения о необходимости обновления. Также в основном окне указывается версия базы данных сигнатур вирусов. Этот числовой индикатор представляет собой активную ссылку на страницу веб-сайта ESET, где перечисляются все сигнатуры, добавленные при данном обновлении.

Кроме того, вы можете вручную запустить обновление — **Обновить базу данных сигнатур вирусов**. Обновление базы данных сигнатур вирусов и компонентов программы является важнейшей частью обеспечения полной защиты компьютера от злонамеренного кода. Уделите особое внимание изучению конфигурирования и работы этого процесса. Если в процессе установки не были указаны сведения о лицензии, лицензионный ключ можно указать при обновлении. Чтобы получить доступ к серверам обновлений ESET, щелкните элемент **Активировать продукт**.

Если активировать ESET Endpoint Antivirus с помощью автономного файла лицензии (не вводя имя пользователя и пароль) и попробовать выполнить обновление, отобразится красного цвета текст **При обновлении базы данных сигнатур вирусов произошла ошибка**. Он означает, что загружать обновления можно только с зеркала.

ПРИМЕЧАНИЕ
Лицензионный ключ предоставляет компания ESET после приобретения ESET Endpoint Antivirus.



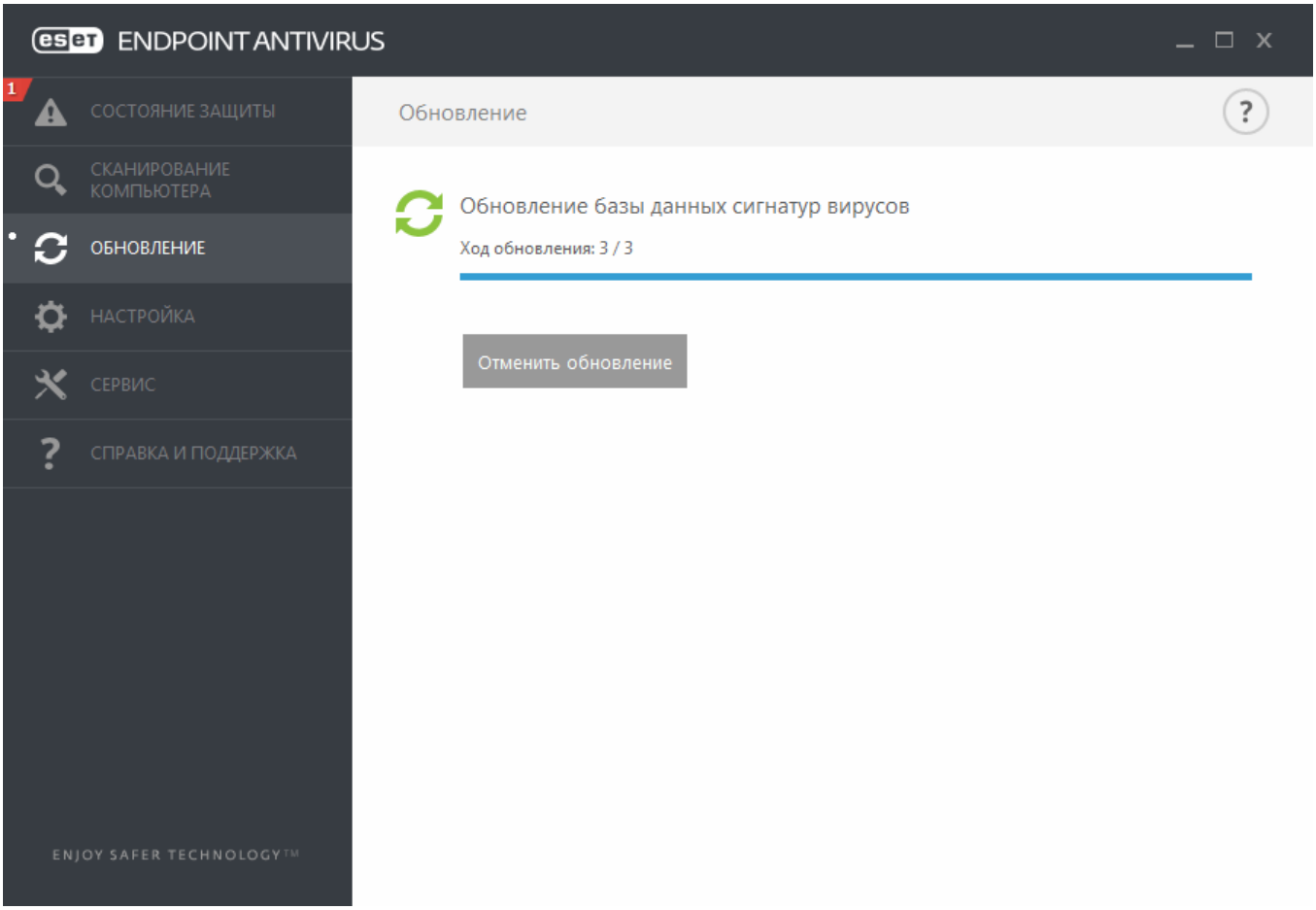
Последнее успешное обновление — дата последнего обновления. Следует убедиться, что в этом поле указана недавняя дата, поскольку это значит, что база данных сигнатур вирусов актуальна.

База данных сигнатур вирусов: номер версии базы данных сигнатур вирусов, также являющийся активной ссылкой на веб-сайт ESET. Эту ссылку можно нажать, чтобы просмотреть все сигнатуры, добавленные в данном

обновлении.

Процесс обновления

После нажатия **Обновить базу данных сигнатур вирусов** начинается процесс загрузки. На экран будут выведены индикатор выполнения загрузки и время до ее окончания. Чтобы прервать обновление, нажмите кнопку **Отменить обновление**.

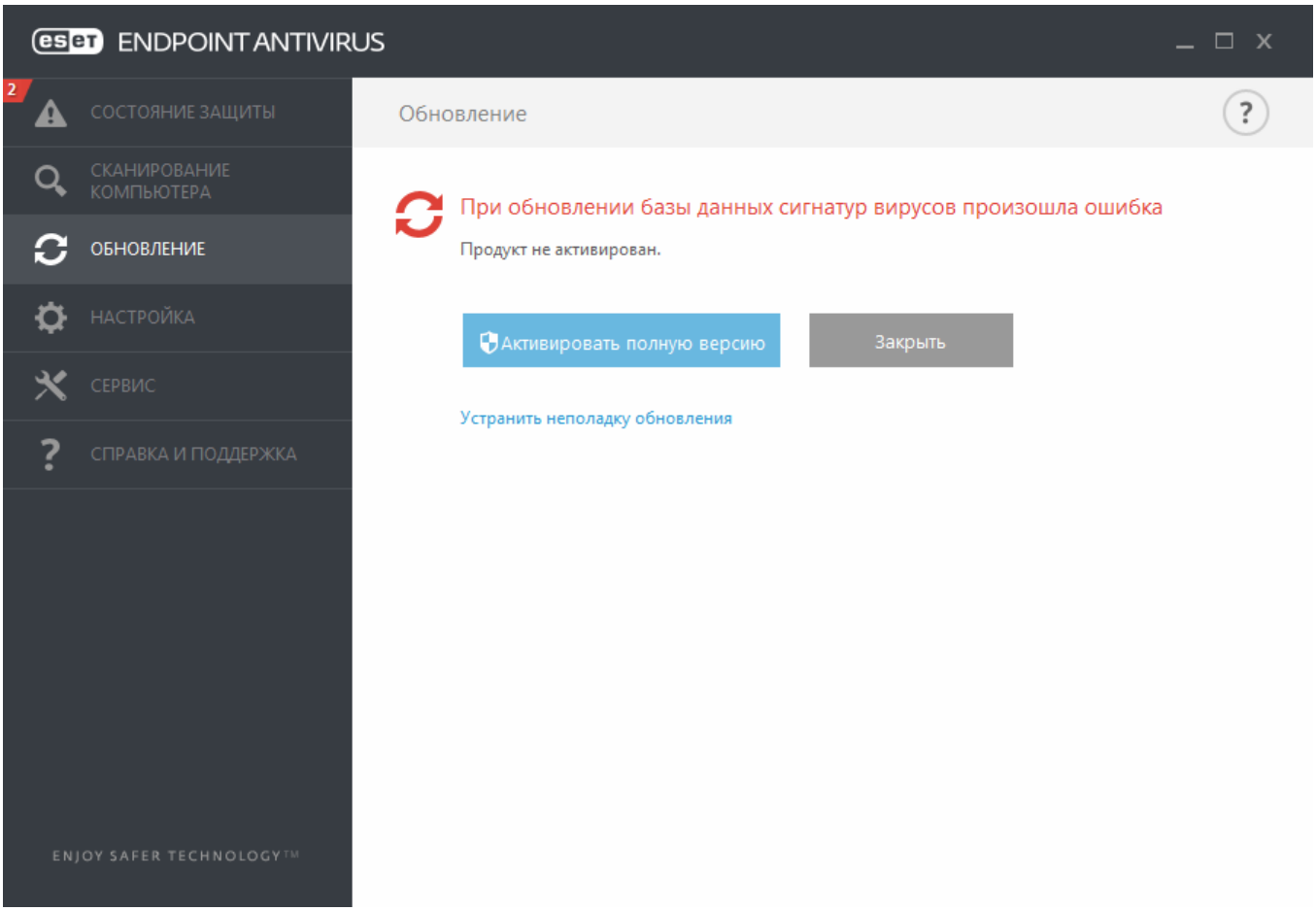


ВАЖНО!
В обычных обстоятельствах после нормального завершения загрузки в окне **Обновление** будет выведено сообщение **Обновления не требуется — установлена последняя база данных сигнатур вирусов**. Если этого сообщения нет, программа устарела. При этом повышается риск заражения. Необходимо обновить базу данных сигнатур вирусов как можно скорее.

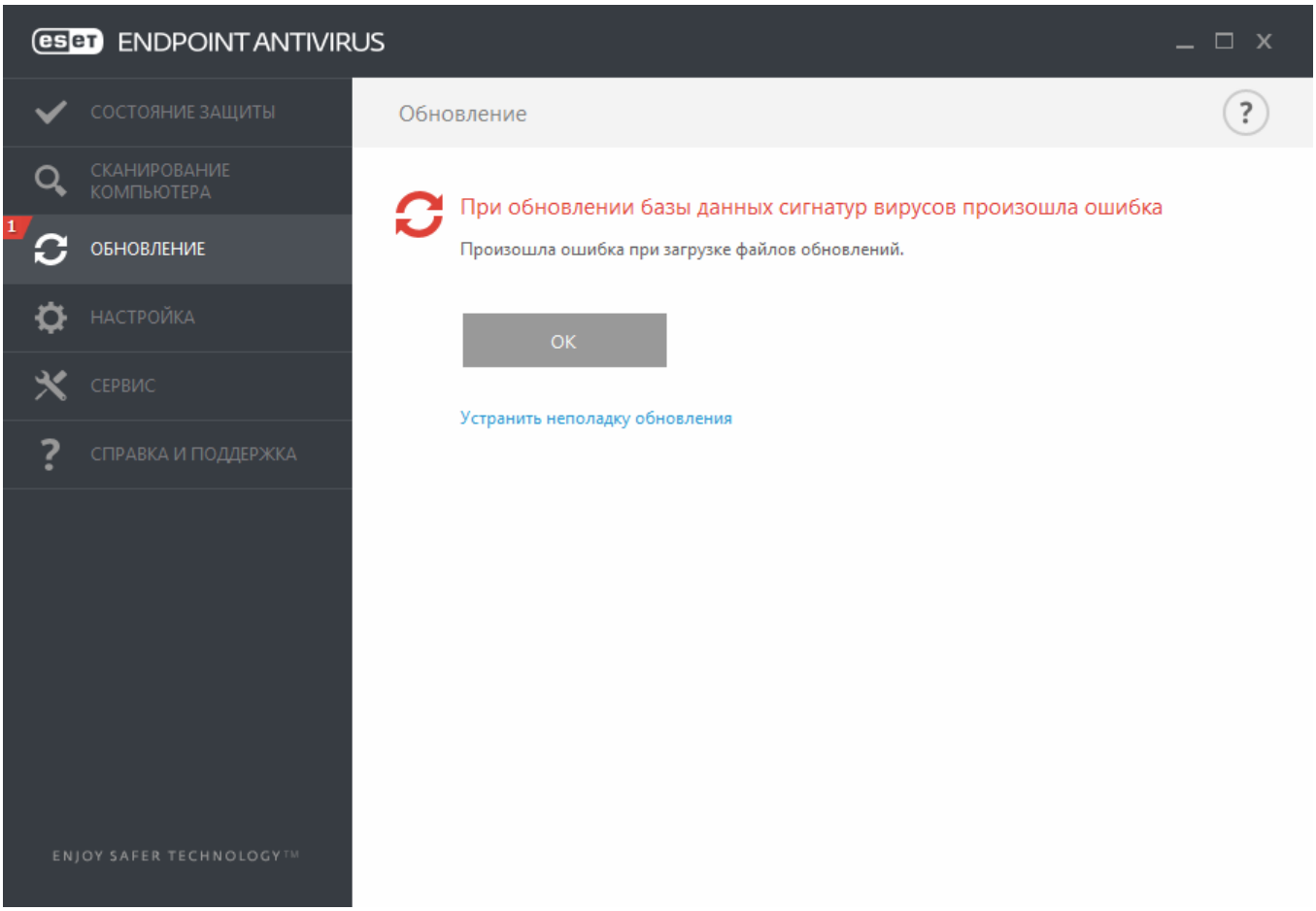
База данных сигнатур вирусов устарела: эта ошибка появится после нескольких неудачных попыток обновить базу данных сигнатур вирусов. Рекомендуется проверить параметры обновлений. Наиболее частая причина этой ошибки — неправильно введенные данные для аутентификации или неверно настроенные параметры подключения.

Предыдущее уведомление связано с двумя указанными ниже сообщениями об ошибках при обновлении (**Произошла ошибка обновления баз сигнатур**).

1. **Недействительная лицензия**: в разделе параметров обновления введен неправильный лицензионный ключ. Рекомендуется проверить данные аутентификации. В окне «Расширенные параметры» (в главном меню выберите пункт **Настройка**, после чего щелкните **Расширенные параметры** или нажмите клавишу F5) содержатся расширенные параметры обновления. В главном меню последовательно щелкните элементы **Справка и поддержка** > **Управление лицензией** и введите новый лицензионный ключ.



2. **Произошла ошибка при загрузке файлов обновлений**: возможная причина этой ошибки — неверные 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.



ПРИМЕЧАНИЕ.
Дополнительные сведения можно найти в этой статье базы знаний ESET.

3.9.3.1 Настройка обновлений

Параметры обновления доступны в дереве **Дополнительные настройки** (F5) в разделе **Обновление**. В этом разделе указывается информация об источниках обновлений, таких как серверы обновлений и данные аутентификации для них.

Общие

Текущий профиль обновления отображается в раскрывающемся меню **Профиль обновления**. Чтобы создать новый профиль, перейдите на вкладку **Профили** и нажмите кнопку **Изменить** рядом с элементом **Список профилей**, введите собственное **имя профиля** и затем нажмите **Добавить**.

Если во время загрузки обновлений базы данных сигнатур вирусов возникли проблемы, щелкните **Очистить**, чтобы удалить временные файлы обновлений (очистить кэш).

Предупреждения об устаревшей базе данных сигнатур вирусов

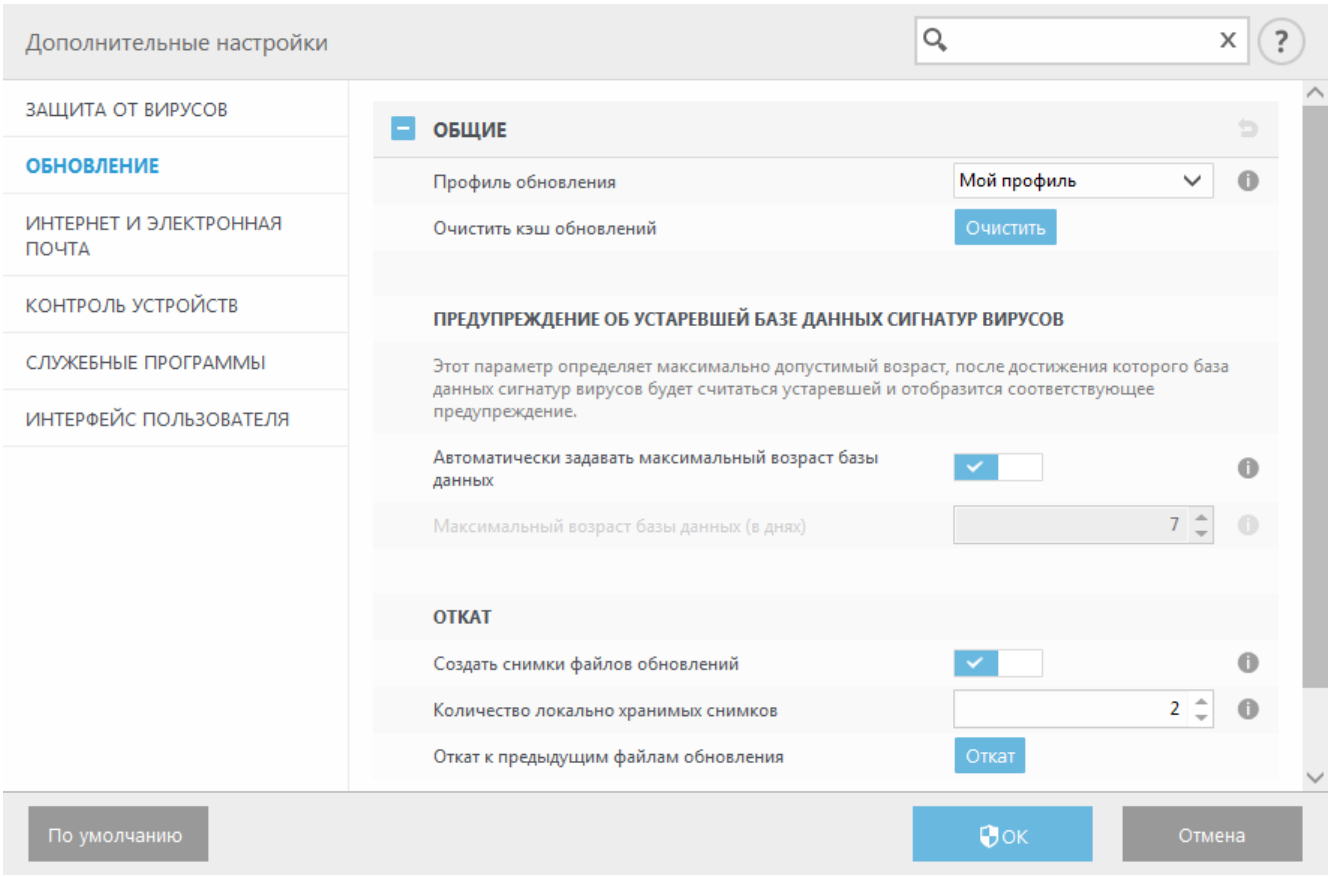
Автоматически задавать максимальный возраст базы данных: позволяет задать максимальное время в днях, по истечении которого база данных сигнатур вирусов будет считаться устаревшей. Значение по умолчанию — 7.

Откат

Если вы подозреваете, что последнее обновление базы данных сигнатур вирусов и/или модулей программы повреждено или работает нестабильно, вы можете выполнить откат к предыдущей версии и отключить обновления на установленный период времени. Или же можно включить ранее отключенные обновления, если они отложены на неопределенный период времени.

Программа ESET Endpoint Antivirus создает снимки базы данных сигнатур вирусов и модулей программы. Эти снимки используются функцией *отката*. Если нужно, чтобы снимки файлов обновлений создавались, оставьте флажок **Создать снимки файлов обновлений** установленным. В поле **Количество локально хранимых снимков** указывается количество хранящихся снимков предыдущих баз данных сигнатур вирусов.

После нажатия кнопки **Откат** (**Дополнительные настройки** (F5) > **Обновление** > **Общие**) в раскрывающемся меню нужно выбрать промежуток времени, на который будет приостановлено обновление базы данных сигнатур вирусов и модулей программы.



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

Чтобы создать профиль, рядом с элементом **Список профилей** нажмите кнопку **Изменить**, введите **имя профиля** и нажмите кнопку **Добавить**. Чтобы изменить созданный профиль, выберите его и нажмите кнопку **Изменить** возле элемента **Список профилей**.

Основные сведения

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. **Тестовое обновление** — это обновление, которое уже прошло полное внутреннее тестирование и в ближайшее время станет доступным всем пользователям. Преимущество тестовых обновлений заключается в том, что у вас появляется возможность использовать новейшие исправления и способы обнаружения. Однако такие обновления иногда могут быть недостаточно стабильны и НЕ ДОЛЖНЫ использоваться на

производственных серверах и рабочих станциях, где требуются максимальные работоспособность и стабильность. Вариант **Отложенное обновление** позволяет загружать обновления со специальных серверов с задержкой в несколько часов (т. е. после того, как обновления будут протестированы в реальных средах и признаны стабильными).

Отключить оповещение об успешном обновлении — отключает уведомления на панели задач в правом нижнем углу экрана. Этот параметр удобно использовать, если какое-либо приложение или игра работает в полноэкранном режиме. Обратите внимание, что в режиме презентаций все уведомления отключены.

Обновить со съемного носителя: позволяет выполнить обновление со съемного носителя, если он содержит созданное зеркало. Если установлен флажок **Автоматически**, обновление будет выполняться в фоновом режиме. Если диалоговые окна обновления должны отображаться, выберите **Всегда спрашивать**.

По умолчанию в меню **Сервер обновлений** установлен параметр **Выбирать автоматически**. Сервер обновлений — это компьютер, на котором хранятся файлы обновлений. При использовании сервера ESET рекомендуется оставить параметры по умолчанию.

При использовании локального HTTP-сервера, который также называется зеркалом, сервер обновлений должен быть указан следующим образом:
http://имя_компьютера_или_его_IP-адрес:2221.

При использовании локального HTTP-сервера с поддержкой SSL, сервер обновлений должен быть указан следующим образом:
https://имя_компьютера_или_его_IP-адрес:2221.

При использовании локальной общей папки, сервер обновлений должен быть указан следующим образом:
\\имя компьютера или его IP-адрес\общая папка

Обновление с зеркала

На серверах обновлений для аутентификации используется **лицензионный ключ**, который создается и отправляется после покупки. При использовании сервера зеркала можно определить, с помощью каких учетных данных клиентам следует выполнять вход на этот сервер перед получением обновлений. По умолчанию проверка не требуется, то есть поля **Имя пользователя** и **Пароль** остаются пустыми.

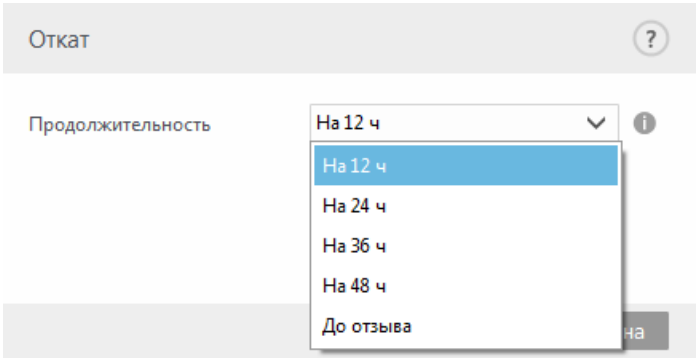
3.9.3.1.1 Профили обновления

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 **Профиль обновления** отображается текущий профиль. По умолчанию для него задано значение **Мой профиль**. Чтобы создать профиль, рядом с элементом **Список профилей** нажмите кнопку **Изменить**, введите **имя профиля** и нажмите кнопку **Добавить**.

3.9.3.1.2 Откат обновления

После нажатия кнопки **Откат** (**Дополнительные настройки** (F5) > **Обновление** > **Профиль**) в раскрывающемся меню нужно выбрать промежуток времени, на который будет приостановлено обновление базы данных сигнатур вирусов и модулей программы.



Выберите вариант **До отзыва**, чтобы отложить регулярные обновления на неопределенный период времени, пока функция обновлений не будет восстановлена вручную. Поскольку он подвергает систему опасности, его не рекомендуется использовать.

Программа возвращается к самой старой версии базы данных сигнатур вирусов, которая хранится в качестве снимка в файловой системе локального компьютера.

ПРИМЕЧАНИЕ.
Предположим, последней версии базы данных сигнатур вирусов присвоен номер 10646. Версии 10645 и 10643 хранятся в качестве снимков. Обратите внимание, что версия 10644 недоступна, поскольку, например, компьютер был выключен и более новая версия обновления стала доступна до того, как была загружена версия 10644. Если в поле **Количество локально хранимых снимков** установить значение 2 и нажать кнопку **Откат**, программа восстановит версию базы данных сигнатур вирусов под номером 10643 (включая модули программы). Это может занять некоторое время. Чтобы проверить, произведен ли откат к предыдущей версии, в главном окне ESET Endpoint Antivirus откройте раздел Обновление.

3.9.3.1.3 Режим обновления

Вкладка **Режим обновления** содержит параметры, относящиеся к обновлениям компонентов программы. Программа позволяет предопределить ее поведение в тех случаях, когда становятся доступны обновления компонентов.

Обновления компонентов программы активируют новые функции или вносят изменения в уже существующие. Это действие может выполняться как в автоматическом режиме без вмешательства пользователя, так и с уведомлением. После установки обновления компонентов программы может потребоваться перезагрузка компьютера. В разделе **Обновление компонентов программы** доступны три описанных далее варианта.

- **Запросить подтверждение перед загрузкой компонентов** — вариант по умолчанию. Пользователю будет предлагаться подтвердить обновление компонентов программы или отказаться от него, когда такое обновление становится доступно.
- **Выполнять обновление компонентов программы, если доступно**: обновления компонентов программы будут автоматически загружаться и устанавливаться. Обратите внимание на то, что может потребоваться перезагрузка компьютера.
- **Никогда не обновлять компоненты программы**: обновление компонентов программы выполняться не будет. Этот вариант подходит для серверной установки, поскольку серверы обычно перезапускаются только при техническом обслуживании.

ПРИМЕЧАНИЕ.
Наиболее подходящий вариант зависит от конкретной рабочей станции, на которой будут применяться параметры. Необходимо помнить о том, что существует разница между рабочими станциями и серверами. Так, автоматический перезапуск сервера после обновления программы может привести к серьезным проблемам.

Включить ручное обновление компонентов программы — по умолчанию отключено. Если этот параметр включен и доступна более новая версия ESET Endpoint Antivirus, можно проверить наличие обновлений на панели **Обновление** и **установить** новую версию.

Если установлен флажок **Запрашивать подтверждение перед загрузкой обновления**, на экран будет выводиться уведомление каждый раз, когда появляется новое обновление.

Если размер файла обновления больше значения, указанного в параметре **Запрашивать подтверждение, если размер обновления превышает (КБ)**, на экран будет выводиться уведомление.

3.9.3.1.4 Прокси-сервер HTTP

Для доступа к параметрам настройки прокси-сервера для конкретного профиля обновлений щелкните элемент **Обновление** в дереве **Дополнительные настройки** (F5), а затем щелкните элемент **Профили** > **HTTP-прокси**. Откройте раскрывающееся меню **Режим прокси-сервера** и выберите один из трех перечисленных далее вариантов.

- Не использовать прокси-сервер
- Подключение через прокси-сервер
- Использовать общие параметры прокси-сервера

Если выбрать вариант **Использовать общие параметры прокси-сервера**, будут использоваться глобальные параметры прокси-сервера, уже заданные в разделе **Дополнительные настройки** > **Служебные программы** > **Прокси-сервер**.

Выберите вариант **Не использовать прокси-сервер**, чтобы указать, что прокси-сервер не будет использоваться для обновления ESET Endpoint Antivirus.

Флажок **Подключение через прокси-сервер** должен быть установлен в следующих случаях.

- Для обновления ESET Endpoint Antivirus должен использоваться прокси-сервер, отличный от указанного в глобальных параметрах (**Служебные программы** > **Прокси-сервер**). В этом случае нужно указать параметры: адрес **прокси-сервера**, **порт** передачи данных (3128 по умолчанию), а также **имя пользователя** и **пароль** для прокси-сервера (если необходимо).
- Не были заданы общие параметры прокси-сервера, однако ESET Endpoint Antivirus 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 впоследствии (например, при смене поставщика услуг Интернета) нужно убедиться в том, что указанные в этом окне параметры прокси HTTP 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: если прокси-сервер недоступен, он не будет использоваться при обновлении.

ПРИМЕЧАНИЕ.
Данные для аутентификации, такие как **имя пользователя** и **пароль**, предназначены для доступа к прокси-серверу. Заполнять эти поля необходимо только в том случае, если требуются имя пользователя и пароль. Обратите внимание, что эти поля не имеют отношения к имени пользователя и паролю для программы ESET Endpoint Antivirus и должны быть заполнены только в том случае, если подключение к Интернету осуществляется через защищенный паролем прокси-сервер.

3.9.3.1.5 Подключение к локальной сети

При обновлении с локального сервера под управлением ОС Windows NT по умолчанию требуется аутентификация всех сетевых подключений.

Чтобы настроить такую учетную запись, выберите в раскрывающемся меню **Тип локального пользователя** один из следующих вариантов:

- **системная учетная запись (по умолчанию)**;
- **текущий пользователь**;
- **указанный пользователь**.

Выберите вариант **Учетная запись системы (по умолчанию)**, чтобы использовать для аутентификации учетную запись системы. Если данные аутентификации в главном разделе параметров обновлений не указаны, как правило, процесса аутентификации не происходит.

Для того чтобы программа использовала для аутентификации учетную запись, под которой в данный момент выполнен вход в систему, выберите вариант **Текущий пользователь**. Недостаток этого варианта заключается в

том, что программа не может подключиться к серверу обновлений, если в данный момент ни один пользователь не выполнил вход в систему.

Выберите **Указанный пользователь**, если нужно указать учетную запись пользователя для аутентификации. Этот метод следует использовать в тех случаях, когда невозможно установить соединение с помощью учетной записи системы. Обратите внимание на то, что указанная учетная запись должна обладать правами на доступ к каталогу на локальном сервере, в котором хранятся файлы обновлений. В противном случае программа не сможет установить соединение и загрузить обновления.

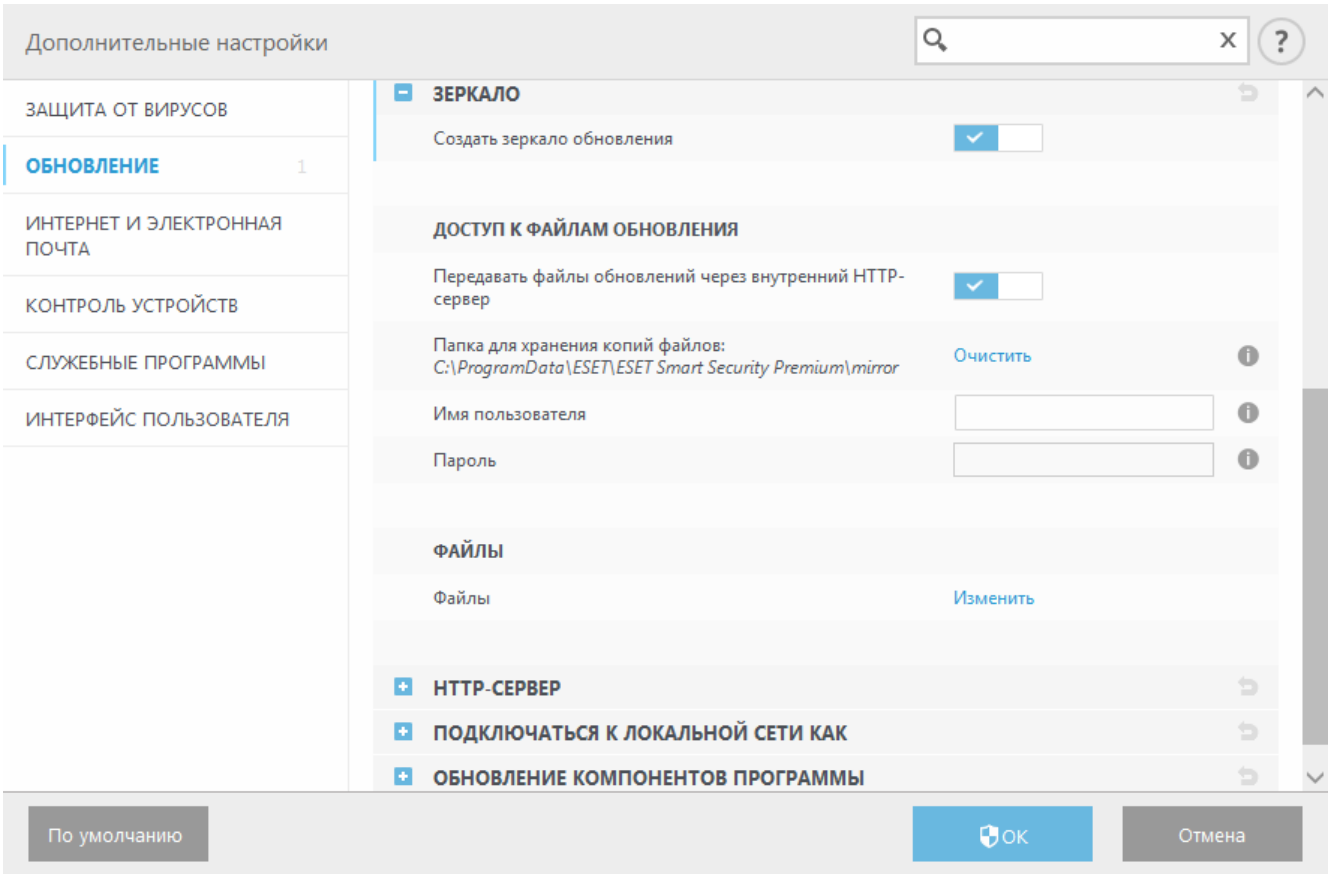
ВНИМАНИЕ!
Если выбран вариант **Текущий пользователь** или **Указанный пользователь**, может произойти ошибка при изменении учетной записи программы. В главном разделе параметров обновления рекомендуется указывать данные для аутентификации в локальной сети. В этом разделе параметров обновлений укажите данные аутентификации следующим образом: *имя_домена\пользователь* (а для рабочей группы *рабочая_группа\имя*) и пароль. При обновлении по протоколу HTTP с сервера локальной сети аутентификации не требуется.

Выберите параметр **Отключиться от сервера после завершения обновления** для принудительного отключения, если подключение к серверу остается активным после загрузки обновлений.

3.9.3.1.6 Зеркало

ESET Endpoint Antivirus дает возможность создавать копии файлов обновлений, которые могут использоваться для обновления других рабочих станций в сети. Использование *зеркала* (копии файлов обновлений в локальной сети) позволяет избежать загрузки одних и тех же обновлений с сервера производителя всеми рабочими станциями. Обновления загружаются на локальный сервер зеркала, а затем распространяются на рабочие станции. Это позволяет избежать перерасхода трафика. Обновление клиентских рабочих станций с зеркала оптимизирует трафик в сети и сокращает объем потребляемого интернет-трафика.

Настроить локальный сервер зеркала можно в дополнительных настройках в разделе **Обновление**. Чтобы попасть в этот раздел, нажмите клавишу **F5** (откроется меню «Дополнительные настройки»), щелкните **Обновление** > **Профили** и выберите вкладку **Зеркало**.



Чтобы создать зеркало на клиентской рабочей станции, установите флажок **Создать зеркало обновления**.

После этого станут доступными другие параметры настройки зеркала, такие как способ доступа к файлам обновлений и путь к файлам зеркала.

Доступ к файлам обновления

Передавать файлы обновлений через внутренний HTTP-сервер: если этот параметр активирован, файлы обновлений будут доступны просто по протоколу HTTP, причем указывать имя пользователя и пароль не нужно.

ПРИМЕЧАНИЕ.
Для использования HTTP-сервера в Windows XP необходимо установить пакет обновления 2.

Способы доступа к серверу зеркала детально описаны в статье Обновление с зеркала. Существуют два основных способа доступа к зеркалу: папка с файлами обновлений может существовать как общая сетевая папка, или клиенты могут получить доступ к зеркалу на HTTP-сервере.

Папка, предназначенная для хранения файлов обновлений для зеркала, указывается в разделе **Папка для хранения копий файлов**. Чтобы выбрать другую папку, щелкните **Очистить** для удаления предварительно заданной папки *C:\ProgramData\ESET\ESET Endpoint Antivirus\mirror*, а затем щелкните **Изменить** для выбора папки на локальном компьютере или общей сетевой папки. Если для указанной папки нужна авторизация, данные аутентификации должны быть указаны в полях **Имя пользователя** и **Пароль**. Если выбранная папка назначения расположена на сетевом диске компьютера под управлением ОС Windows NT/2000/XP, указанные имя пользователя и пароль должны принадлежать пользователю с правами на запись в указанную папку. Имя пользователя и пароль следует вводить в формате *Домен/Пользователь* или *Рабочая_группа/Пользователь*. Не забудьте ввести соответствующие пароли.

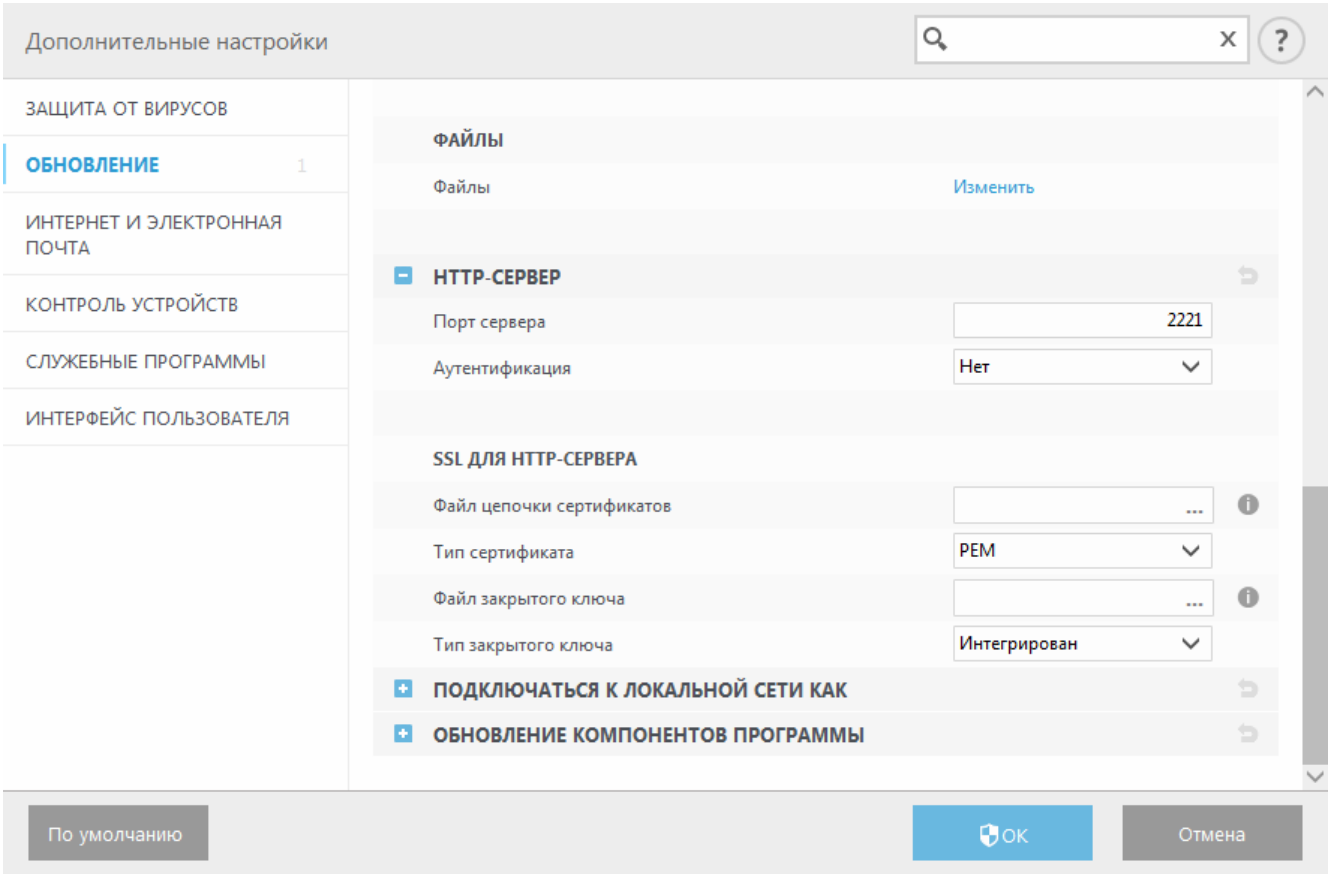
Файлы: при настройке зеркала можно указать предпочитаемые языки обновлений. Выбранные языки должны поддерживаться сервером зеркала, который настроил пользователь.

HTTP-сервер

Порт сервера: по умолчанию порт сервера имеет значение 2221.

В параметре **Аутентификация** определяется метод аутентификации, используемый для доступа к файлам обновлений. Доступны варианты **Нет**, **Обычная** и **NTLM**. Чтобы использовать кодировку base64 и упрощенную аутентификацию по имени пользователя и паролю, выберите **Обычная**. Вариант **NTLM** обеспечивает шифрование с использованием безопасного метода. Для аутентификации используется учетная запись пользователя, созданная на рабочей станции, которая предоставляет общий доступ к файлам обновлений. Значение по умолчанию — **Нет**. Этот вариант дает доступ к файлам обновлений без аутентификации.

Чтобы использовать HTTP-сервер с поддержкой протокола HTTPS (SSL), прикрепите свой **файл цепочки сертификатов** или создайте самозаверяющий сертификат. Доступны следующие типы сертификатов: ASN, PEM и PFX. Из соображений дополнительной безопасности можно использовать протокол HTTPS для загрузки файлов обновления. При его использовании практически невозможно отследить передаваемые сведения и учетные данные. По умолчанию для параметра **Тип закрытого ключа** задается значение **Интегрированный** (поэтому параметр **Файл закрытого ключа** по умолчанию неактивен). Это означает, что закрытый ключ является частью выбранного файла цепочки сертификатов.



Подключение к локальной сети

Тип локального пользователя: варианты **Учетная запись системы (по умолчанию)**, **Текущий пользователь** и **Указанный пользователь** отображаются в соответствующих раскрывающихся меню. **Имя пользователя** и **Пароль** указывать необязательно. См.статью Подключение к локальной сети.

Выберите параметр **Отключиться от сервера после завершения обновления** для принудительного отключения, если подключение к серверу остается активным после загрузки обновлений.

Обновление компонентов программы

Автоматически обновлять компоненты: разрешает установку новых и обновление существующих компонентов. Обновление может выполняться как в автоматическом режиме без вмешательства пользователя, так и с уведомлением. После установки обновления компонентов программы может потребоваться перезагрузка компьютера.

Обновить компоненты сейчас: обновляет компоненты программы до последней версии.

3.9.3.1.6.1 Обновление с зеркала

Существует два способа настройки зеркала. Зеркало — это, по сути, репозиторий, с которого клиенты могут загружать файлы обновлений. Папкой с файлами обновлений может выступать общий сетевой ресурс или HTTP-сервер.

Доступ к файлам зеркала с помощью внутреннего HTTP-сервера

Это вариант по умолчанию, выбранный в предварительно заданной конфигурации программы. Для обеспечения доступа к зеркалу с помощью HTTP-сервера перейдите на вкладку **Дополнительные настройки** > **Обновление** > **Профили** > **Зеркало** и выберите элемент **Создать зеркало обновления**.

В разделе **HTTP-сервер** вкладки **Зеркало** можно указать **Порт сервера**, на котором HTTP-сервер будет принимать запросы, а также тип **аутентификации**, используемой HTTP-сервером. По умолчанию порт сервера имеет значение **2221**. С помощью параметра **Аутентификация** определяется метод аутентификации, используемый для доступа к файлам обновлений. Доступны варианты **Нет**, **Обычная** и **NTLM**. Чтобы использовать кодировку base64 и упрощенную аутентификацию по имени пользователя и паролю, выберите

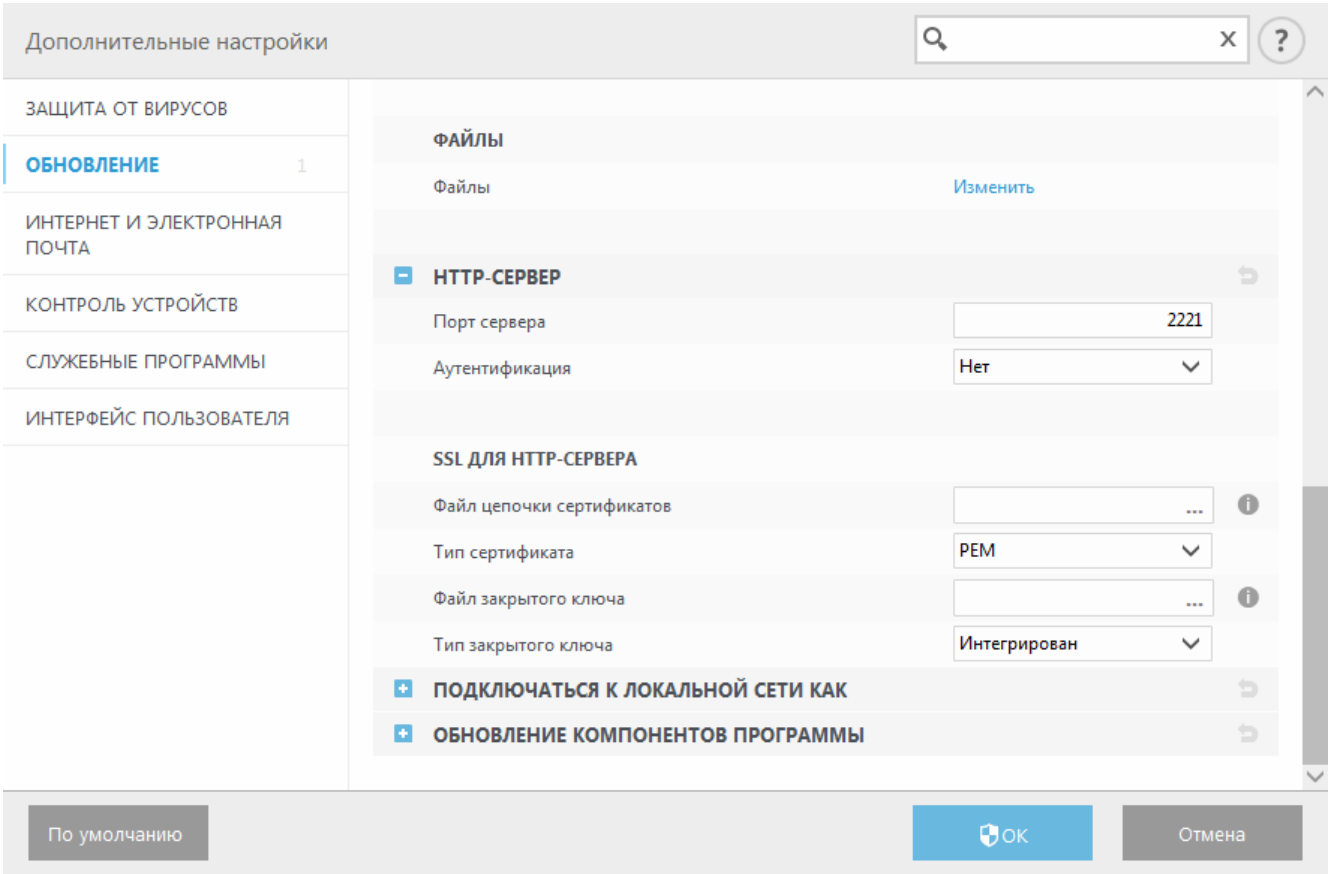
Обычная. Вариант **NTLM** обеспечивает шифрование с использованием безопасного метода. Для аутентификации используется учетная запись пользователя, созданная на рабочей станции, которая предоставляет общий доступ к файлам обновлений. Значение по умолчанию — **Нет**. Этот вариант дает доступ к файлам обновлений без аутентификации.

ВНИМАНИЕ!
Если планируется организовать доступ к файлам обновлений с помощью HTTP-сервера, папка зеркала должна находиться на том же компьютере, что и экземпляр ESET Endpoint Antivirus, который ее создает.

SSL для HTTP-сервера

Чтобы использовать HTTP-сервер с поддержкой протокола HTTPS (SSL), прикрепите свой **файл цепочки сертификатов** или создайте самозаверяющий сертификат. Доступны следующие типы сертификатов: **PEM, PFX** и **ASN**. Из соображений дополнительной безопасности можно использовать протокол HTTPS для загрузки файлов обновления. При его использовании практически невозможно отследить передаваемые сведения и учетные данные. Для параметра **Тип закрытого ключа** по умолчанию установлено значение **Интегрированный**. Это значит, что закрытый ключ является частью выбранного файла цепочки сертификатов.

ПРИМЕЧАНИЕ.
После нескольких неудачных попыток обновить базу данных сигнатур вирусов с зеркала в главном меню на панели обновления появится ошибка **Неверные имя пользователя и (или) пароль**. Рекомендуем перейти в меню **Дополнительные настройки** > **Обновление** > **Профили** > **Зеркало** и проверить указанные имя пользователя и пароль. Обычно эта ошибка вызвана неправильными аутентификационными данными.



После настройки сервера зеркала вам следует добавить сервер обновлений на клиентские рабочие станции. Для этого выполните следующие действия.

- Откройте меню **Дополнительные настройки** (F5) и последовательно щелкните элементы **Обновление** > **Профили** > **Обычное**.
- Снимите флажок **Выбирать автоматически** и добавьте в поле **Сервер обновлений** новый сервер. Укажите сервер в одном из таких форматов:
  http://IP_адрес_нового_сервера:2221
  https://IP_адрес_нового_сервера:2221 (если используется SSL)

Доступ к зеркалу через общие системные папки

Сначала необходимо создать общую папку на локальном или сетевом устройстве. При создании папки для зеркала необходимо предоставить права на *запись* пользователю, который будет размещать в ней файлы обновлений, и права на *чтение* всем пользователям, которые будут получать обновления для ESET Endpoint Antivirus из папки зеркала.

Далее на вкладке **Дополнительные настройки** > **Обновление** > **Профили** > **Зеркало** необходимо настроить доступ к зеркалу, сняв флажок **Передавать файлы обновлений через внутренний HTTP-сервер**. Этот вариант включен по умолчанию после установки программы.

Если общая папка расположена на другом компьютере в сети, необходимо указать данные аутентификации для доступа к нему. Для этого откройте в ESET Endpoint Antivirus раздел **Дополнительные настройки** (F5) и щелкните **Обновление** > **Профили** > **Подключаться к локальной сети как**. Этот параметр аналогичен используемому для обновления и описан в разделе Подключение к локальной сети.

После окончания настройки зеркала укажите на рабочих станциях адрес нового сервера обновлений в формате //*UNC**ПУТЬ*.

1. Откройте в ESET Endpoint Antivirus меню **Дополнительные настройки** > **Обновление** > **Профили** > **Обычное**.
2. Снимите флажок **Выбирать автоматически** и добавьте новый сервер в поле **Сервер обновлений**. Для этого используйте формат *UNC**ПУТЬ*.

ПРИМЕЧАНИЕ.
Для корректной работы обновлений путь к папке зеркала должен быть указан в формате UNC. Обновления с сопоставленных сетевых дисков могут не работать.

Последний раздел контролирует компоненты программы (PCU). По умолчанию после загрузки их можно копировать в локальное зеркало. Если установлен флажок **Обновление компонентов программы**, не нужно нажимать кнопку **Обновить**, т. к. файлы автоматически копируются на локальное зеркало. Дополнительные сведения об обновлении компонентов программы см. в разделе Режим обновления.

3.9.3.1.6.2 Устранение проблем при обновлении с зеркала

В большинстве случаев проблемы при обновлении с сервера зеркала возникают в связи с по крайней мере одной из следующих причин: неверное указание параметров папки зеркала, неверные данные аутентификации для папки зеркала, неверные параметры на рабочих станциях, которые пытаются загружать файлы обновлений с зеркала, а также различные сочетания этих причин. Ниже приведен краткий обзор наиболее часто возникающих проблем при обновлении с зеркала.

Ошибка при подключении ESET Endpoint Antivirus к серверу зеркала: обычно происходит при указании неправильных данных сервера обновлений (сетевого пути к папке зеркала), с которого рабочие станции загружают обновления. Для проверки папки нажмите кнопку **Пуск** в системе Windows, выберите **Выполнить**, введите имя папки и нажмите кнопку **ОК**. На экран должно быть выведено содержимое папки.

ESET Endpoint Antivirus запрашивает имя пользователя и пароль: вероятная причина заключается в том, что введены неверные данные аутентификации (имя пользователя и пароль) в разделе обновлений. Имя пользователя и пароль используются для доступа к серверу обновлений, с которого выполняется обновление программы. Убедитесь, что данные аутентификации указаны верно и в правильном формате. Например, *Домен/Имя_пользователя* или *Рабочая_группа/имя_пользователя* в сочетании с соответствующим паролем. Если сервер зеркала доступен всем участникам сети, это не означает, что у любого пользователя есть к нему доступ. Параметр «Все участники» означает то, что папка доступна всем пользователям домена, а не то, что предоставляется доступ без авторизации. Т. е., если папка доступна всем участникам, все же необходимо указать доменное имя пользователя и пароль в настройках обновления.

Ошибка при подключении ESET Endpoint Antivirus к серверу зеркала: подключение к порту, указанному для доступа к HTTP-версии зеркала, блокируется.

3.9.3.2 Создание задач обновления

Обновление можно запустить вручную, нажав **Обновить базу данных сигнатур вирусов** в основном окне, которое появляется после выбора пункта **Обновление** в главном меню.

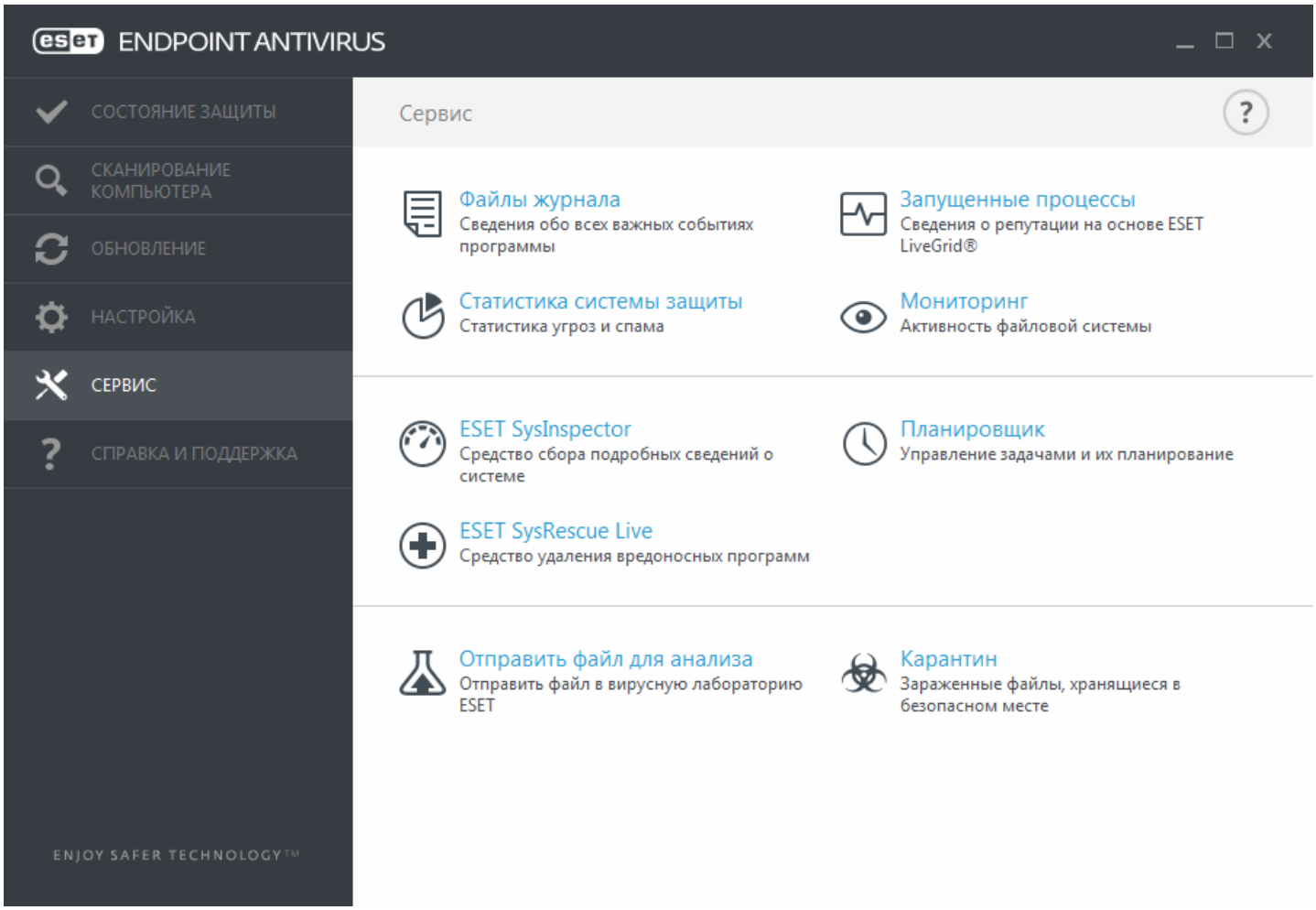
Обновления также можно выполнять как запланированную задачу. Для настройки запланированной задачи перейдите в раздел **Служебные программы** > **Планировщик**. По умолчанию в ESET Endpoint Antivirus активированы указанные ниже задачи.

- **Регулярное автоматическое обновление**
- **Автоматическое обновление после установки модемного соединения**
- **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.

3.9.4 Служебные программы

В меню **Сервис** перечислены модули, которые позволяют упростить процесс администрирования программы, и также содержит дополнительные возможности администрирования для опытных пользователей.



В этом меню представлены следующие служебные программы.

- Файлы журнала
- Статистика защиты
- Наблюдение
- Запущенные процессы (если использование системы ESET Live Grid включено в ESET Endpoint Antivirus)
- Планировщик
- Карантин
- ESET SysInspector

Отправка образца на анализ: возможность отправить подозрительный файл на анализ в вирусную лабораторию ESET. Диалоговое окно, открывающееся при использовании этой функции, описано в разделе Отправка образцов на анализ.

ESET SysRescue: перенаправляет на страницу ESET SysRescue, с которой можно загрузить образ ESET SysRescue Live или Live CD/USB Creator для операционной системы Microsoft Windows.

3.9.4.1 Файлы журнала

Файлы журнала содержат информацию о важных программных событиях и предоставляют сводные сведения об обнаруженных угрозах. Журналы являются важнейшим элементом анализа, обнаружения угроз и устранения неполадок. Оно выполняется в фоновом режиме без вмешательства пользователя. Данные сохраняются в соответствии с текущими параметрами степени детализации журнала. Просматривать текстовые сообщения и журналы можно непосредственно в среде ESET Endpoint Antivirus. Также предусмотрена возможность архивации файлов журнала.

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**. Доступны указанные ниже журналы.

- **Обнаруженные угрозы**: журнал угроз содержит подробную информацию о заражениях, обнаруженных модулями ESET Endpoint Antivirus. Регистрируется информация о времени обнаружения, название угрозы, место обнаружения, выполненные действия и имя пользователя, который находился в системе при обнаружении заражения. Дважды щелкните запись журнала для просмотра подробного содержимого в отдельном окне.
- **События**: в журнале событий регистрируются все важные действия, выполняемые программой ESET Endpoint Antivirus. Он содержит информацию о событиях и ошибках, которые произошли во время работы программы. Он помогает 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. Чтобы получить подробную информацию о той или иной операции сканирования, дважды щелкните соответствующую запись.
- **Система предотвращения вторжений на узел**: содержит записи о конкретных правилах, которые были помечены для регистрации. Протокол показывает приложение, которое вызвало операцию, результат (было правило разрешено или запрещено) и имя созданного правила.
- **Отфильтрованные веб-сайты**: этот список используется для просмотра списка веб-сайтов, заблокированных при помощи защиты доступа в Интернет. В этих журналах отображается время, URL-адрес, пользователь и приложение, с помощью которого установлено соединение с конкретным веб-сайтом.
- **Контроль устройств**: содержит список подключенных к компьютеру съемных носителей и устройств. В файл журнала записываются только устройства с правилом контроля устройств. В противном случае в журнале не создаются записи о них. Также здесь отображаются такие сведения, как тип устройства, серийный номер, имя поставщика и размер носителя (при его наличии).

Чтобы скопировать в буфер обмена информацию из любого раздела журнала (сочетание клавиш **CTRL+C**), выделите нужную запись и нажмите кнопку **Копировать**. Для выделения нескольких записей можно

использовать клавиши **CTRL** и **SHIFT**.

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

Щелчок записи правой кнопкой мыши выводит на экран контекстное меню. В контекстном меню доступны перечисленные ниже параметры.

- **Показать**: просмотр в новом окне более подробной информации о выбранном журнале.
- **Фильтрация одинаковых записей**: после активации этого фильтра будут показаны только записи одного типа (диагностические, предупреждения и т. д.).
- **Фильтровать.../Найти...**: при выборе этого параметра на экран выводится окно Поиск в журнале, 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**: копируется информация обо всех записях в окне.
- **Удалить/Удалить все**: удаляются выделенные записи или все записи в окне; для этого действия нужны права администратора.
- **Экспорт...**: экспорт информации о записях в файл формата XML.
- **Экспортировать все...**: экспорт информации о всех записях в файл формата XML.
- **Прокрутить журнал**: установите этот флажок, чтобы выполнялась автоматическая прокрутка старых журналов, а на экран в окне **Файлы журнала** выводились активные журналы.

3.9.4.1.1 Поиск в журнале

В журналах хранится информация о важных системных событиях. Функция фильтрации журнала позволяет отображать записи о событиях определенного типа.

Введите ключевое слово для поиска в поле **Найти текст**. Если нужно искать это ключевое слово в конкретных столбцах, измените фильтр с помощью раскрывающегося меню **Искать в столбцах**.

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,и т. п.).

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

Только слова целиком: установите этот флажок, если для получения более точных результатов нужно искать определенные слова целиком.

С учетом регистра: установите этот флажок, если при фильтрации должен учитываться регистр букв.

Искать вверх: сначала отображаются результаты, которые находятся выше в документе.

3.9.4.2 Настройка прокси-сервера

В больших локальных сетях подключение компьютеров к Интернету может осуществляться через прокси-сервер. Ориентируясь на эту конфигурацию, нужно задать описанные ниже параметры. Если этого не сделать, программа не сможет обновляться автоматически. В ESET Endpoint Antivirus настройку прокси-сервера можно выполнить в двух разных разделах дерева расширенных настроек.

Во-первых, параметры прокси-сервера можно конфигурировать в разделе **Дополнительные настройки**, доступном через **Служебные программы** > **Прокси-сервер**. Настройка прокси-сервера на этом уровне позволяет задать его параметры для программы ESET Endpoint Antivirus в целом. Они используются всеми модулями программы, которым требуется подключение к Интернету.

Для настройки параметров прокси-сервера на этом уровне установите флажок **Использовать прокси-сервер**, а

затем введите адрес прокси-сервера в поле **Прокси-сервер**, а также укажите номер его **порта** в соответствующем поле.

Если требуется аутентификация на прокси-сервере, установите флажок **Прокси-сервер требует аутентификации**, а затем в соответствующих полях укажите **имя пользователя** и **пароль**. Нажмите кнопку **Найти**, чтобы автоматически определить параметры прокси-сервера и подставить их. Будут скопированы параметры, указанные в Internet Explorer.

ПРИМЕЧАНИЕ.
В настройках **прокси-сервера** имя пользователя и пароль нужно вводить вручную.

Использовать прямое подключение, если прокси-сервер недоступен: если в программе настроено использование прокси-сервера HTTP, а он недоступен, программа будет обходить прокси-сервер и подключаться к серверам ESET напрямую.

Параметры прокси-сервера также можно настроить в расширенных параметрах обновления (последовательно откройте **Дополнительные настройки** > **Обновление** > **Прокси-сервер HTTP** и в раскрывающемся меню **Режим прокси-сервера** выберите пункт **Подключение через прокси-сервер**). Эти параметры применяются к конкретному профилю обновления и рекомендуются для ноутбуков, которые часто получают обновления сигнатур вирусов из разных источников. Для получения дополнительных сведений об этих параметрах см. раздел Дополнительные настройки обновления.

3.9.4.3 Планировщик

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

Перейти к планировщику можно из главного окна программы ESET Endpoint Antivirus, открыв раздел меню **Служебные программы** > **Планировщик**. **Планировщик** содержит полный список всех запланированных задач и свойства конфигурации, такие как предварительно заданные дата, время и используемый профиль сканирования.

Планировщик предназначен для планирования выполнения следующих задач: обновление базы данных сигнатур вирусов, 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). 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 установки модемного соединения**
- **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 базы данных сигнатур вирусов)
- **Автоматическое первое сканирование**

Чтобы изменить параметры запланированных задач (как определенных по умолчанию, так и пользовательских), щелкните правой кнопкой мыши нужную задачу и выберите команду **Изменить...** или выберите 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 сканирование компьютера** - создание снимка состояния компьютера в ESET SysInspector. При этом 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.
- **Первое сканирование** - по умолчанию через 20 минут после установки или перезагрузки выполняется сканирование компьютера как задание с низким приоритетом.
- **Обновление** - планирование задачи обновления, в рамках которой обновляется база данных сигнатур вирусов и программные модули.

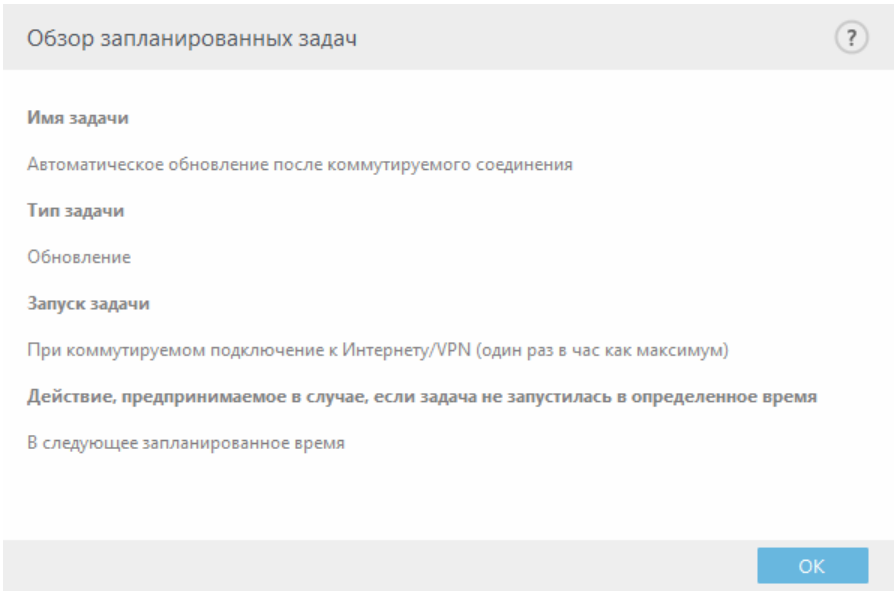
4. Активируйте кнопку **Включено** при необходимости активировать задачу (это можно сделать позже, установив/сняв флажок в списке запланированных задач), нажмите кнопку **Далее** и выберите один из режимов времени выполнения:

- **Однократно**: задача будет выполнена однократно в установленную 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**
- **Незамедлительно, если с момента последнего запуска прошло больше времени, чем указано** (интервал можно указать с помощью параметра **Время с момента последнего запуска**).

Можно просмотреть запланированную задачу, щелкнув правой кнопкой мыши и выбрав **Показать информацию о задаче**.



3.9.4.4 Статистика защиты

Для просмотра диаграммы статистических данных, связанных с модулями защиты ESET Endpoint Antivirus, нажмите **Служебные программы** > **Статистика защиты**. Выберите интересующий вас модуль защиты в раскрывающемся меню **Статистика**, в результате чего на экран будет выведена соответствующая диаграмма и легенда. Если навести указатель мыши на элемент в легенде, на диаграмме отобразятся данные только для этого элемента.

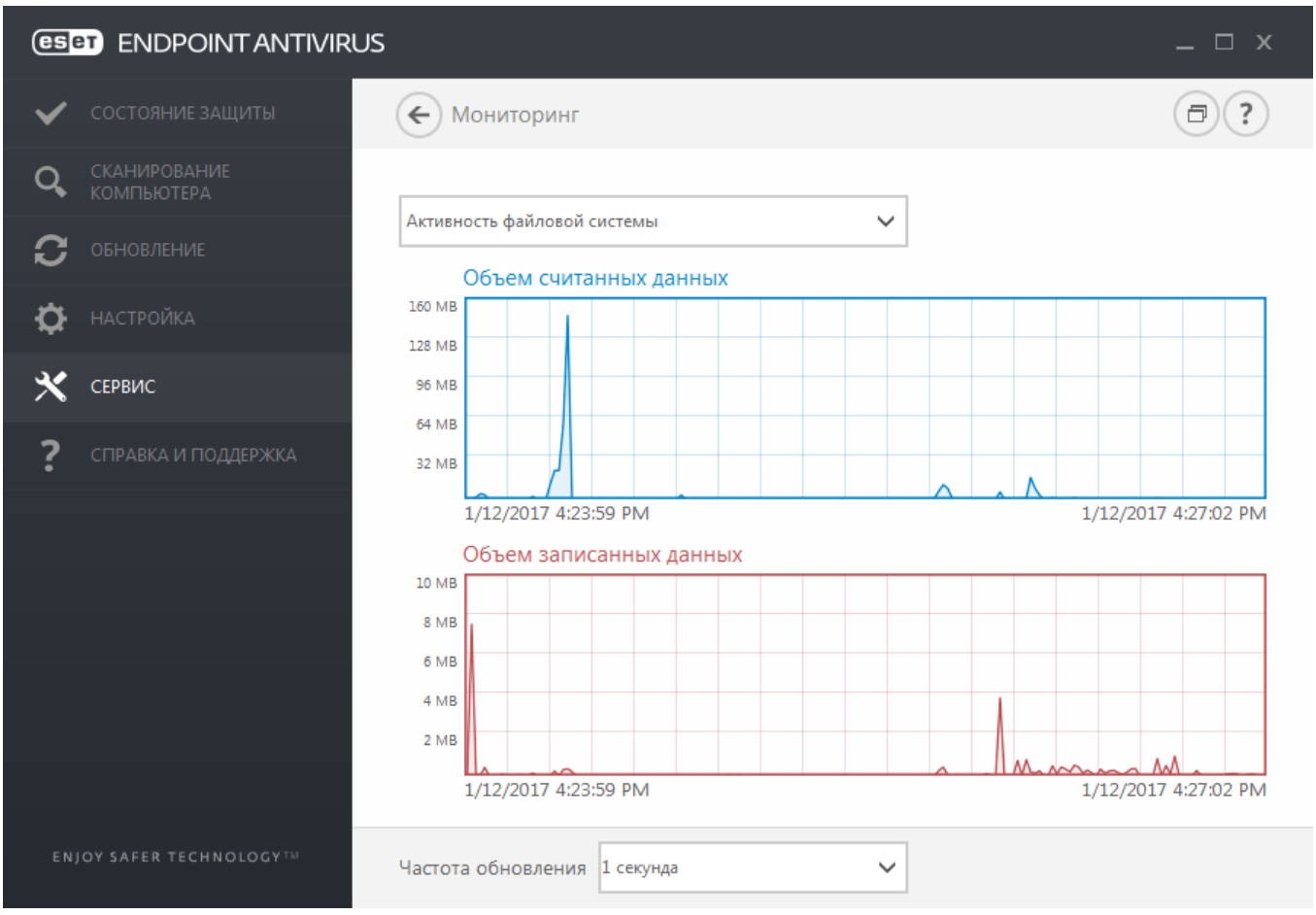
Доступны следующие статистические диаграммы.

- **Защита от вирусов и шпионских программ**: отображение количества зараженных и очищенных объектов.
- **Защита файловой системы**: отображение только объектов, считанных из файловой системы и записанных в нее.
- **Защита почтового клиента**: отображение только объектов, отправленных или полученных почтовыми клиентами.
- **Защита доступа в Интернет и защита от фишинга**: отображение только объектов, загруженных веб-браузерами.

Возле графиков статистики отображается количество просканированных, зараженных, очищенных и чистых объектов. Нажмите кнопку **Сброс**, чтобы очистить данные статистики, или нажмите кнопку **Сбросить все**, чтобы очистить и удалить все существующие данные.

3.9.4.5 Наблюдение

Чтобы просмотреть текущую **активность файловой системы** в графическом виде, выберите **Служебные программы** > **Наблюдение**. В нижней части диаграммы находится временная шкала, на которой отображается активность файловой системы в режиме реального времени за выбранный временной интервал. Чтобы изменить временной интервал, выберите необходимое значение в раскрывающемся меню **Частота обновления**.



Доступны указанные ниже варианты.

- **Шаг: 1 секунда**: диаграмма обновляется каждую секунду, временная шкала охватывает последние 10 минут.
- **Шаг: 1 минута (последние 24 часа)**: диаграмма обновляется каждую минуту, временная шкала охватывает последние 24 часа.
- **Шаг: 1 час (последний месяц)**: диаграмма обновляется каждый час, временная шкала охватывает последний месяц.
- **Шаг: 1 час (выбранный месяц)**: диаграмма обновляется каждый час, временная шкала охватывает последние X выбранных месяцев.

На вертикальной оси **графика** активности файловой системы отображается объем считанных (синий цвет) и записанных (красный цвет) данных. Оба значения измеряются в КБ (килобайтах)/МБ/ГБ. Если навести указатель мыши на прочитанные или записанные данные в легенде под диаграммой, на графике отобразятся данные только для выбранного типа активности.

3.9.4.6 ESET SysInspector

ESET SysInspector — это приложение, которое тщательно проверяет компьютер и собирает подробные сведения о компонентах системы, таких 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.

В окне SysInspector отображаются такие данные о созданных журналах.

- **Время**: время создания журнала.
- **Комментарий**: краткий комментарий.
- **Пользователь**: имя пользователя, создавшего журнал.
- **Состояние**: состояние создания журнала.

Доступны перечисленные далее действия.

- **Открыть**: открывает созданный журнал. Вы также можете щелкнуть файл журнала правой кнопкой мыши и выбрать в контекстном меню пункт **Показать**.
- **Сравнить**: сравнение двух существующих журналов.
- **Создать...**: создание журнала. Прежде чем открывать журнал, подождите, пока программа ESET SysInspector завершит работу (отобразится состояние журнала «Создано»).
- **Удалить**: удаление выделенных журналов из списка.

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

- **Показать**: открытие выделенного журнала в ESET SysInspector (аналогично двойному щелчку).
- **Сравнить**: сравнение двух существующих журналов.
- **Создать**: создание журнала. Прежде чем открывать журнал, подождите, пока программа ESET SysInspector завершит работу (отобразится состояние журнала «Создано»).
- **Удалить все**: удаление всех журналов.
- **Экспорт...**: экспорт журнала в файл или архив в формате *XML*.

3.9.4.7 ESET Live Grid

Сеть ESET Live Grid — это современная система раннего обнаружения угроз, состоящая из нескольких облачных технологий. Она обнаруживает возникающие угрозы, пользуясь принципом репутации, и оптимизирует процесс сканирования благодаря использованию «белого» списка. За счет потоковой передачи информации об угрозах в облако вирусная лаборатория ESET своевременно реагирует на угрозы и предоставляет актуальную и постоянную защиту. Пользователь может проверять репутацию запущенных процессов и файлов непосредственно в интерфейсе программы или в контекстном меню, благодаря чему становится доступна дополнительная информация из ESET Live Grid. При установке ESET Endpoint Antivirus выберите один из описанных ниже параметров.

1. Систему ESET Live Grid можно не включать. Функциональность программного обеспечения при этом не теряется, но в некоторых случаях решение ESET Endpoint Antivirus может реагировать на новые угрозы медленнее, чем обновление базы данных сигнатур вирусов.
2. В ESET Live Grid можно настроить отправку анонимной информации о новых угрозах и файлах, содержащих неизвестный опасный код. Файл может быть отправлен в ESET для тщательного анализа. Изучение этих угроз поможет компании ESET обновить средства обнаружения угроз.

ESET Live Grid собирает о компьютерах пользователей информацию, которая связана с новыми обнаруженными угрозами. Это может быть образец кода или копия файла, в котором возникла угроза, путь к такому файлу, его имя, дата и время, имя процесса, в рамках которого угроза появилась на компьютере, и сведения об операционной системе.

По умолчанию программа ESET Endpoint Antivirus 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.

Система репутации ESET Live Grid использует «белый» и «черный» списки, которые хранятся в облаке. Чтобы открыть настройки ESET Live Grid, нажмите клавишу **F5**. В окне дополнительных настроек последовательно щелкните **Служебные программы** > **ESET Live Grid**.

Включить систему репутации ESET Live Grid (рекомендуется). Система репутации ESET Live Grid увеличивает эффективность решений ESET для защиты от вредоносных программ, так как благодаря ей сканируемые файлы сопоставляются с элементами «белого» и «черного» списков в облаке.

Отправить анонимную статистическую информацию. С помощью этого параметра можно разрешить продукту ESET собирать информацию о недавно обнаруженных угрозах: название угрозы, дата и время обнаружения, способ обнаружения, связанные метаданные, версия и конфигурация продукта и операционная система.

Отправить файлы. Компании ESET на анализ отправляются подозрительные файлы, похожие на угрозы, и файлы с необычными характеристиками или поведением.

Установите флажок **Вести журнал**, чтобы создать журнал событий для регистрации фактов отправки файлов и статистической информации. В журнал событий будут вноситься записи при каждой отправке файлов или статистики.

Ваш адрес электронной почты (необязательно): можно отправить адрес электронной почты вместе с подозрительными файлами, 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.

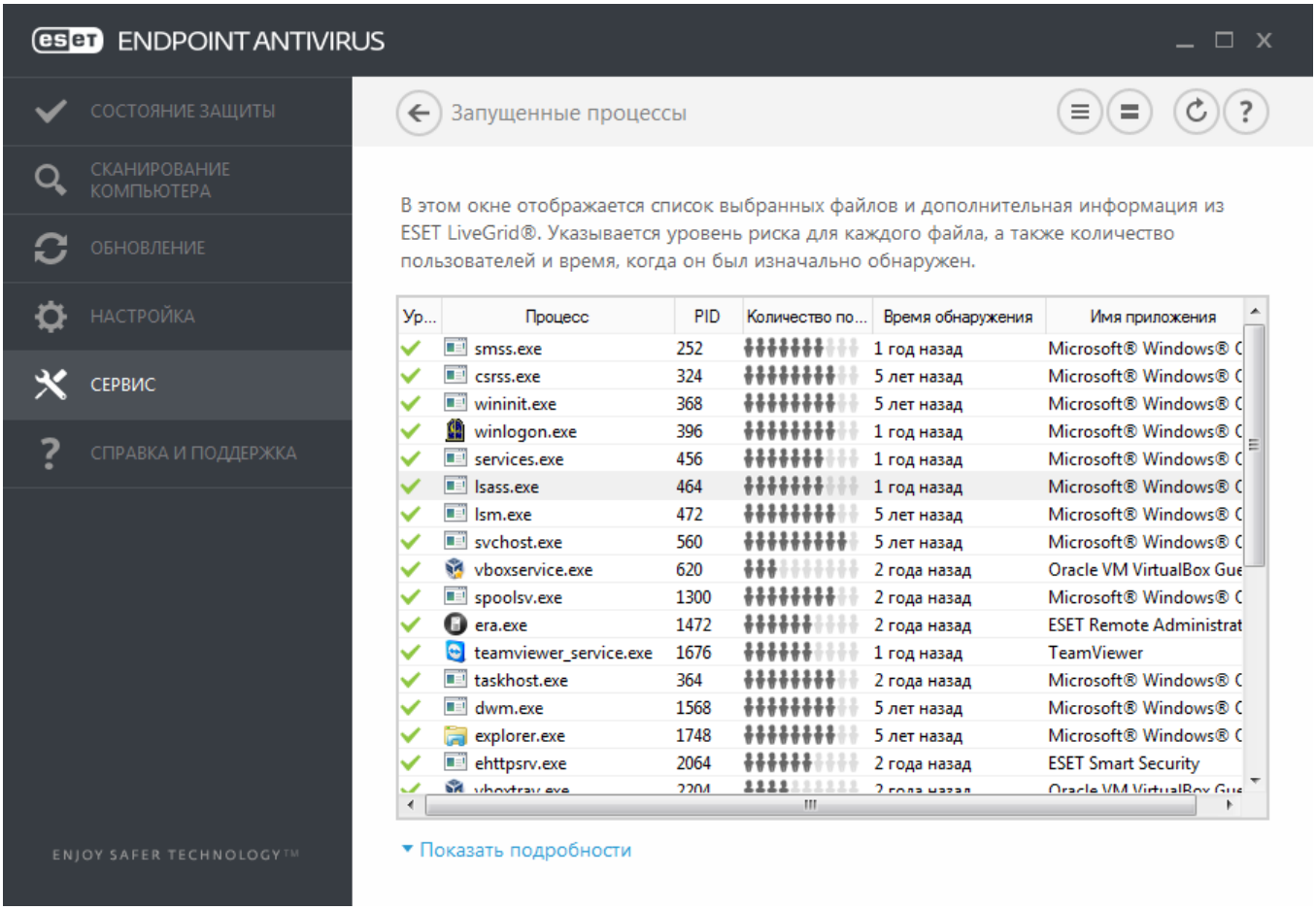
Исключение: фильтр исключений дает возможность указать папки и файлы, которые не нужно отправлять на анализ (например, может быть полезно исключить файлы, в которых может присутствовать конфиденциальная информация, такие как документы и электронные таблицы). Перечисленные в этом списке файлы никогда 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.

Если система ESET Live Grid использовалась ранее, но была отключена, могут существовать 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.

3.9.4.8 Запущенные процессы

В разделе «Запущенные процессы» отображаются выполняемые на компьютере программы или процессы. Кроме того, эта функция позволяет оперативно и непрерывно уведомлять компанию ESET о новых заражениях. ESET Endpoint Antivirus предоставляет подробные сведения о запущенных процессах для защиты пользователей с помощью технологии ESET Live Grid.



Уровень риска: в большинстве случаев ESET Endpoint Antivirus и технология ESET Live Grid 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 и выберите пункт "Диспетчер задач" или одновременно нажмите клавиши **Ctrl**+**Shift**+**Esc** на клавиатуре.

Идентификатор процесса: отображение идентификаторов процессов, запущенных в операционных системах Windows.

ПРИМЕЧАНИЕ.
Известные приложения, помеченные как Безопасно (зеленый), точно являются безопасными (внесены в «белый» список) и исключаются при сканировании, благодаря чему ускоряется сканирование компьютера по требованию или защита файловой системы в режиме реального времени.

Количество пользователей: количество пользователей данного приложения. Эта информация собирается технологией ESET Live Grid.

Время обнаружения: время, прошедшее с момента обнаружения приложения технологией ESET Live Grid.

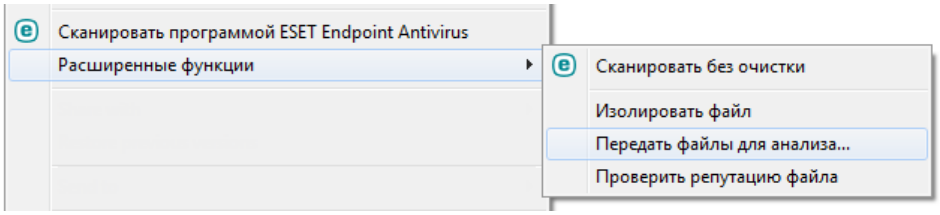
ПРИМЕЧАНИЕ.
Если для приложения выбран уровень безопасности Неизвестно (оранжевый), оно не обязательно является вредоносной программой. Обычно это просто новое приложение. Если вы не уверены в безопасности файла, воспользуйтесь функцией отправки на анализ, чтобы отправить файл в вирусную лабораторию ESET. Если файл окажется вредоносным приложением, необходимая для его обнаружения информация будет включена в последующие обновления базы данных сигнатур вирусов.

Имя приложения: конкретное имя программы или процесса.

Если выбрать определенное приложение внизу, будет выведена указанная ниже информация.

- **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**: дата и время создания приложения.
- **Дата изменения**: дата и время последнего изменения приложения.

ПРИМЕЧАНИЕ.
Также вы можете проверить репутацию файлов, которые не являются запущенными программами или процессами. Для этого пометьте нужные файлы, щелкните их правой кнопкой мыши и в контекстном меню выберите **Расширенные параметры** > **Проверить репутацию файла с помощью ESET Live Grid**.



3.9.4.9 Отправка образцов на анализ

Диалоговое окно отправки образцов позволяет отправить файл или сайт на анализ в ESET. Чтобы открыть это окно, выберите **Служебные программы** > **Отправить образец на анализ**. При обнаружении на компьютере файла, проявляющего подозрительную активность, или подозрительного сайта в Интернете его можно отправить в вирусную лабораторию ESET. Если файл или веб-сайт окажется вредоносным приложением, функция его обнаружения будет включена в последующие обновления.

Другим способом отправки является электронная почта. Если этот способ для вас удобнее, заархивируйте файлы с помощью программы WinRAR или WinZIP, защитите архив паролем «infected» и отправьте его по адресу samples@eset.com. Помните, что тема письма должна описывать проблему, а текст должен содержать как можно более полную информацию о файле (например, адрес веб-сайта, с которого он был загружен).

ПРИМЕЧАНИЕ.
Прежде чем отправлять образец в компанию ESET, убедитесь в том, что он соответствует одному или нескольким из следующих критериев:

- файл или веб-сайт совсем не обнаруживается;
- файл или веб-сайт ошибочно обнаруживается как угроза.

Ответ на подобный запрос будет отправлен только в том случае, если потребуется дополнительная информация.

В раскрывающемся меню **Причина отправки образца** выберите наиболее подходящее описание своего сообщения.

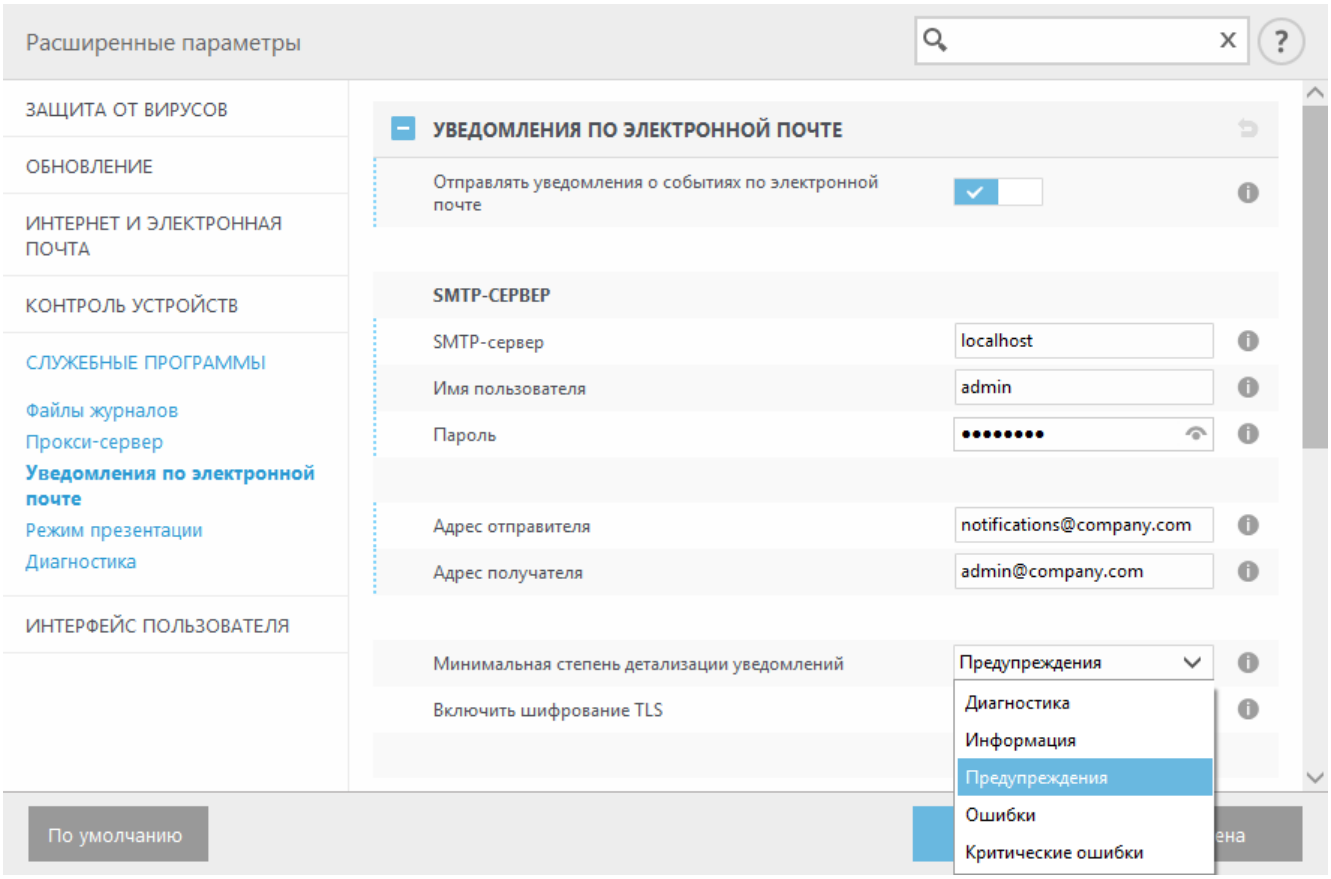
- **Подозрительный файл**
- **Подозрительный сайт** (веб-сайт, зараженный вредоносной программой)
- **Ложно обнаруженный файл** (файл обнаружен как зараженный, хотя не является таковым)
- **Ложно обнаруженный сайт**
- **Другое**

Файл/сайт — путь к файлу или веб-сайту, который вы собираетесь отправить.

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. 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.

3.9.4.10 Уведомления по электронной почте

ESET Endpoint Antivirus поддерживает отправку сообщений электронной почты при возникновении событий с заданной степенью детализации. Чтобы включить эту функцию, установите флажок **Отправлять уведомления по электронной почте**.



SMTP-сервер

SMTP-сервер: SMTP-сервер, используемый для отправки оповещений (например, *smtp.provider.com:587*, номер предварительно заданного порта — 25).

ПРИМЕЧАНИЕ.
ESET Endpoint Antivirus поддерживает SMTP-серверы, использующие шифрование TLS.

Имя пользователя и **пароль**: если требуется аутентификация на SMTP-сервере, заполните эти поля для получения доступа к нему.

Адрес отправителя: в этом поле указывается адрес отправителя, который будет отображаться в заголовке

писем с уведомлением.

Адреса получателей: в этом поле указываются адреса получателей, которые будут отображаться в заголовке писем с уведомлением. Для разделения адресов электронной почты используется точка с запятой (;).

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 успешном выполнении обновления, а также все перечисленные выше записи.
- **Предупреждения**: записываются критические ошибки и предупреждения (например, не удалось выполнить обновление или система Antistealth работает неправильно).
- **Ошибки**: записываются ошибки (не активирована защита документов) и критические ошибки.
- **Критические ошибки**: записываются только критические ошибки (ошибки запуска защиты от вирусов или уведомления о наличии вируса в системе).

Включить шифрование TLS: разрешить отправку предупреждений об угрозе и уведомлений с использованием протокола TLS.

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.

Отправлять уведомления в отдельных сообщениях электронной почты: если этот параметр активирован, получатель будет получать каждое уведомление в отдельном сообщении. Это может привести к получению большого количества почты за короткий промежуток времени.

Формат сообщений

Формат сообщений о событиях: формат сообщений о событиях, отображаемых на удаленных компьютерах.

Формат предупреждений об угрозах: предупреждения об угрозе и уведомления по умолчанию имеют предопределенный формат. Изменять этот формат не рекомендуется. Однако в некоторых случаях (например, при наличии системы автоматизированной обработки электронной почты) может понадобиться изменить формат сообщений.

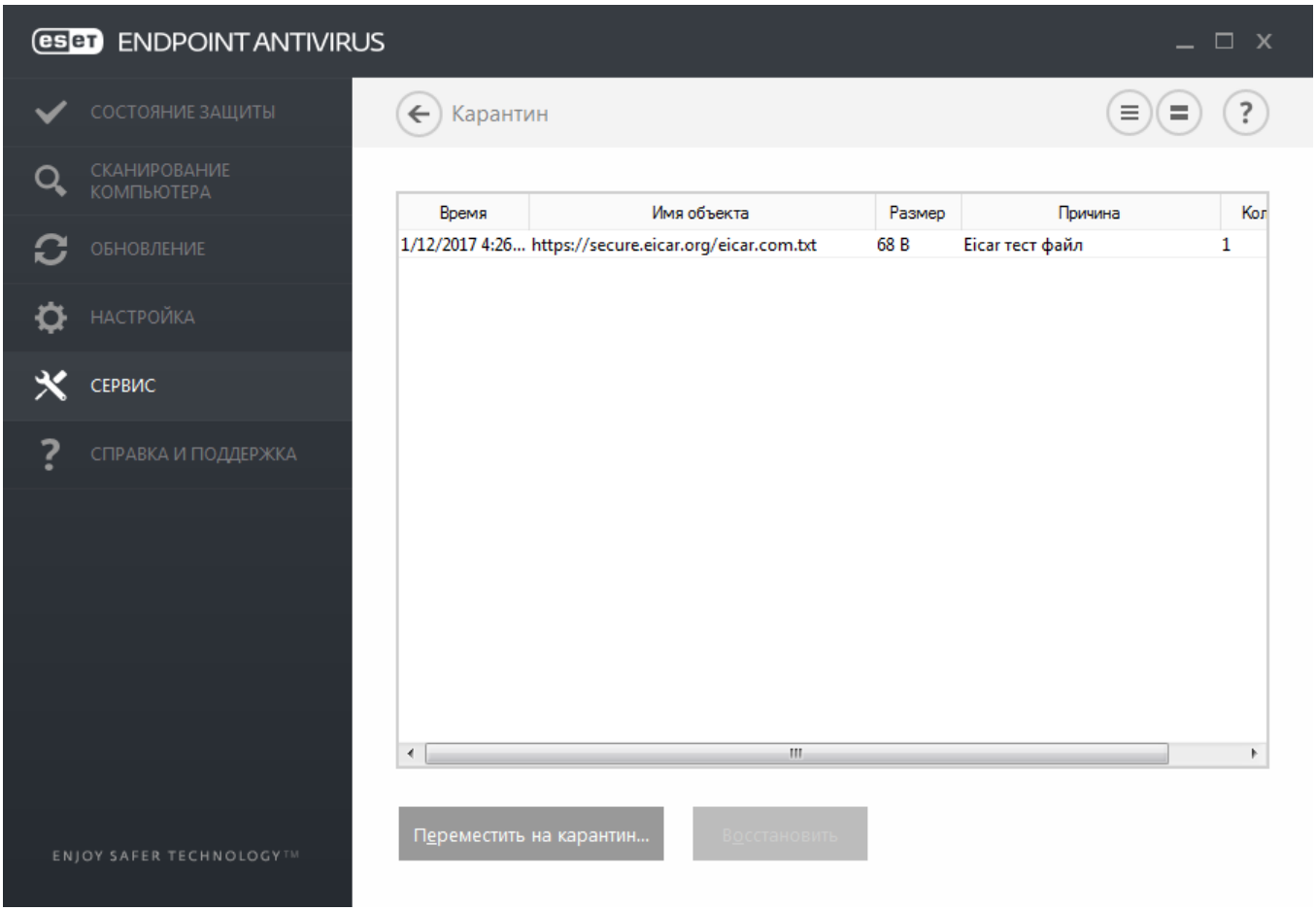
Использовать символы местного алфавита: преобразовывает кодировку сообщения электронной почты в кодировку ANSI на основе региональных параметров Windows (например, windows-1250). Если не устанавливать этот флажок, сообщение будет преобразовано с использованием 7-битной кодировки ACSII (например, «á» будет преобразовано в «a», а неизвестные символы — в «?»).

Использовать местную кодировку символов: сообщение будет преобразовано в формат Quoted Printable (QP), в котором используются знаки ASCII, что позволяет правильно передавать символы национальных алфавитов по электронной почте в 8-битном формате (áéíóú).

3.9.4.11 Карантин

Карантин предназначен в первую очередь для изоляции и безопасного хранения зараженных файлов. Файлы следует помещать на карантин, если их нельзя вылечить или безопасно удалить либо если они отнесены программой ESET Endpoint Antivirus к зараженным по ошибке.

Поместить на карантин можно любой файл. Рекомендуется помещать на карантин файлы с подозрительной активностью, которые, тем не менее, не обнаруживаются модулем сканирования защиты от вирусов. Файлы на карантине можно отправить в вирусную лабораторию ESET на анализ.



Информацию о файлах, помещенных на карантин, можно просмотреть в виде таблицы, содержащей дату и время помещения файла на карантин, путь к его исходному расположению, его размер в байтах, причину помещения файла на карантин (например, объект добавлен пользователем) и количество угроз (например, если архив содержит несколько заражений).

Помещение файлов на карантин

Программа ESET Endpoint Antivirus автоматически помещает удаленные файлы в карантин (если этот параметр не был отменен пользователем в окне предупреждения). При желании любой подозрительный файл можно поместить в карантин вручную с помощью кнопки **Карантин**. В этом случае исходный файл будет удален из исходного расположения. Для этого также можно воспользоваться контекстным меню, нажав правой кнопкой мыши в окне **Карантин** и выбрав пункт **Карантин**.

Восстановление из карантина

Файлы, находящиеся на карантине, можно восстановить в исходном месте. Чтобы восстановить файл из карантина, щелкните его правой кнопкой мыши в окне карантина и в контекстном меню выберите пункт **Восстановить**. Если файл помечен как потенциально нежелательное приложение, будет также доступен пункт **Восстановить и исключить из сканирования**. Контекстное меню содержит также пункт **Восстановить в**, с помощью которого можно восстановить файл в расположение, отличное от исходного.

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. Вы также можете

выделить и удалить несколько элементов одновременно.

ПРИМЕЧАНИЕ.
Если программа поместила незараженный файл в карантин по ошибке, исключите этот файл из процесса сканирования после восстановления и отправьте его в службу поддержки клиентов ESET.

Отправка файла из карантина

Если вы поместили в карантин файл, который программа не смогла определить как опасный, или если файл был ошибочно определен как угроза и помещен в карантин, передайте этот файл в вирусную лабораторию ESET. Чтобы отправить файл из карантина, щелкните его правой кнопкой мыши и выберите пункт **Передать на анализ**.

3.9.4.12 Microsoft Windows Update

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 Endpoint Antivirus уведомляет пользователя об отсутствующих обновлениях в соответствии с выбранным уровнем. Доступны следующие уровни.

- **Без обновлений**: не будет предлагаться загрузить обновления системы.
- **Необязательные обновления**: будет предлагаться загрузить обновления, помеченные как имеющие низкий и более высокий приоритет.
- **Рекомендованные обновления**: будет предлагаться загрузить обновления, помеченные как имеющие обычный и более высокий приоритет.
- **Важные обновления**: будет предлагаться загрузить обновления, помеченные как важные и имеющие более высокий приоритет.
- **Критические обновления**: пользователю будет предлагаться загрузить только критические обновления.

Для сохранения изменений нажмите кнопку **ОК**. После проверки статуса сервера обновлений на экран будет выведено окно «Обновления системы», поэтому данные об обновлении системы могут быть недоступны непосредственно после сохранения изменений.

3.9.4.13 ESET CMD

Эта функция включает расширенные команды ecmd. Она дает возможность экспортировать и импортировать параметры с помощью командной строки (ecmd.exe). До этого экспорт и импорт параметров был возможен только с использованием графического интерфейса. Конфигурацию <%PN%> можно экспортировать в файл в формате *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** — использование защиты паролем. Файл в формате *XML*, из которого импортируется конфигурация, должен быть подписан (см. информацию о подписании файла конфигурации в формате *XML* ниже). При этом методе авторизации в ходе импорта конфигурации пароль проверяется на соответствие паролю, указанному в разделе Параметры доступа. Если настройка доступа не включена, пароль не совпадает или файл конфигурации в формате *XML* не подписан, конфигурация не будет импортирована.

После включения функции ESET CMD можно начать использовать командную строку для экспорта и импорта конфигурации <%PN%>. Это можно сделать вручную или создать сценарий с целью автоматизации.

ВАЖНО!
Для использования расширенных команд ecmd необходимо выполнять их с правами администратора или же открыть командную строку Windows (cmd) в режиме **Запуск от имени администратора**. В противном случае появится сообщение **Error executing command.**. Кроме того, во время экспорта конфигурации должна существовать папка назначения.

ПРИМЕЧАНИЕ.
Расширенные команды ecmd можно выполнить только локально. Выполнение клиентской задачи **Выполнение команды** с использованием ERA не сработает.

ПРИМЕР
Команда экспорта параметров:
```
ecmd /getcfg c:\config\settings.xml
```

Команда импорта параметров:
```
ecmd /setcfg c:\config\settings.xml
```

Подписание файла конфигурации в формате *XML*:

1. Загрузите средство **XmlSignTool** со страницы загрузки средств и утилит ESET и извлеките его. Это средство было разработано специально для подписания файлов конфигурации ESET в формате *XML*.
2. Откройте командную строку Windows (cmd) в режиме **Запуск от имени администратора**.
3. Перейдите в папку с файлом `XmlSignTool.exe`.
4. Выполните команду для подписания файла конфигурации в формате *XML*. Использование: `XmlSignTool <путь_к_файлу_xml>`
5. Введите пароль для расширенной настройки, а затем введите его еще раз по запросу средства XmlSignTool. Теперь файл конфигурации в формате *XML* подписан и его можно импортировать на другом экземпляре <% PN%> с функцией ESET CMD с помощью метода авторизации «Пароль для расширенной настройки».

ВНИМАНИЕ!
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.

3.9.5 Интерфейс

В разделе **Интерфейс** можно конфигурировать поведение графического интерфейса пользователя программы.

С помощью служебной программы Элементы интерфейса можно изменить внешний вид программы и используемые эффекты.

Для обеспечения максимального уровня безопасности программного обеспечения можно предотвратить несанкционированное изменение с помощью инструмента Настройка доступа.

Путем настройки параметров в разделе Предупреждения и уведомления можно изменить поведение предупреждений об обнаруженных угрозах и системных уведомлений. Их можно настроить в соответствии со своими потребностями.

Если запретить отображение каких-то уведомлений, они будут отображаться в разделе **Элементы интерфейса** > **Состояния приложения**. Здесь можно проверить состояние этих уведомлений и настроить запрет на их отображение.

Щелчок по выделенному объекту правой кнопкой мыши открывает контекстное меню. Эта возможность позволяет интегрировать элементы управления ESET Endpoint Antivirus в контекстное меню.

Режим презентации предназначен для пользователей, которые хотят работать с приложениями, не отвлекаясь на всплывающие окна, запланированные задачи и любые компоненты, которые могут загружать процессор и оперативную память.

3.9.5.1 Элементы интерфейса

Параметры интерфейса пользователя в ESET Endpoint Antivirus позволяют настроить рабочую среду в соответствии с конкретными требованиями. Эти параметры доступны в ветви **Интерфейс** > **Элементы интерфейса** дерева расширенных параметров ESET Endpoint Antivirus.

В разделе **Элементы интерфейса** можно настроить рабочую среду. Щелкните раскрывающееся меню **Режим запуска графического интерфейса пользователя** и выберите один из следующих режимов.

Полный: будет отображаться полный графический интерфейс пользователя.

Минимальный: графический интерфейс запущен, но отображаются только уведомления.

Ручной: уведомления и предупреждения не отображаются.

Скрытый: уведомления и предупреждения не отображаются. Этот режим может пригодиться в ситуациях, в которых нужно экономить ресурсы системы. Он может быть запущен только администратором.

ПРИМЕЧАНИЕ.
После выбора минимального графического интерфейса и перезагрузки компьютера уведомления будут отображаться, а графический интерфейс — нет. Чтобы из этого режима перейти в режим полного графического интерфейса, запустите интерфейс из меню «Пуск». Для этого последовательно щелкните элементы **Все программы** > **ESET** и войдите в ESET Endpoint Antivirus в качестве администратора. Это также можно сделать в ESET Remote Administrator, применив соответствующую политику.

Чтобы отключить заставку ESET Endpoint Antivirus, снимите флажок **Показывать заставку при запуске**.

Если вы хотите, чтобы программа ESET Endpoint Antivirus воспроизводила звуковой сигнал, если во время сканирования происходит важное событие, например обнаружена угроза или сканирование закончено, выберите **Использовать звуки**.

Интегрировать с контекстным меню: можно интегрировать элементы управления ESET Endpoint Antivirus в контекстное меню.

Состояния

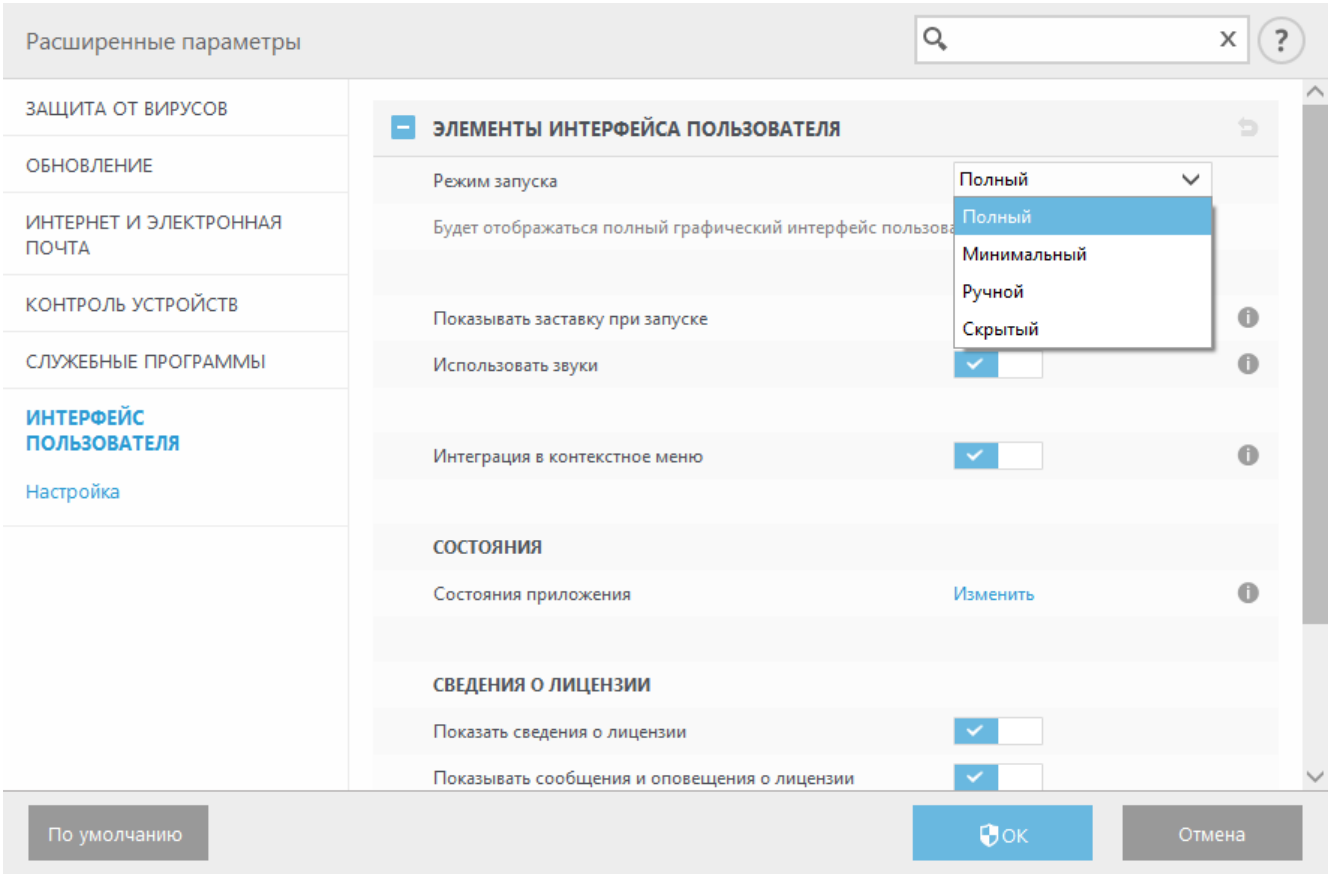
Состояния приложения. Чтобы включить или выключить отображение состояний в области главного меню **Состояние защиты**, щелкните элемент **Изменить**.

Информация о лицензии

Показать сведения о лицензии: если этот параметр отключен, сведения о лицензии не будут отображаться в окнах **Состояние защиты** и **Справка и поддержка**.

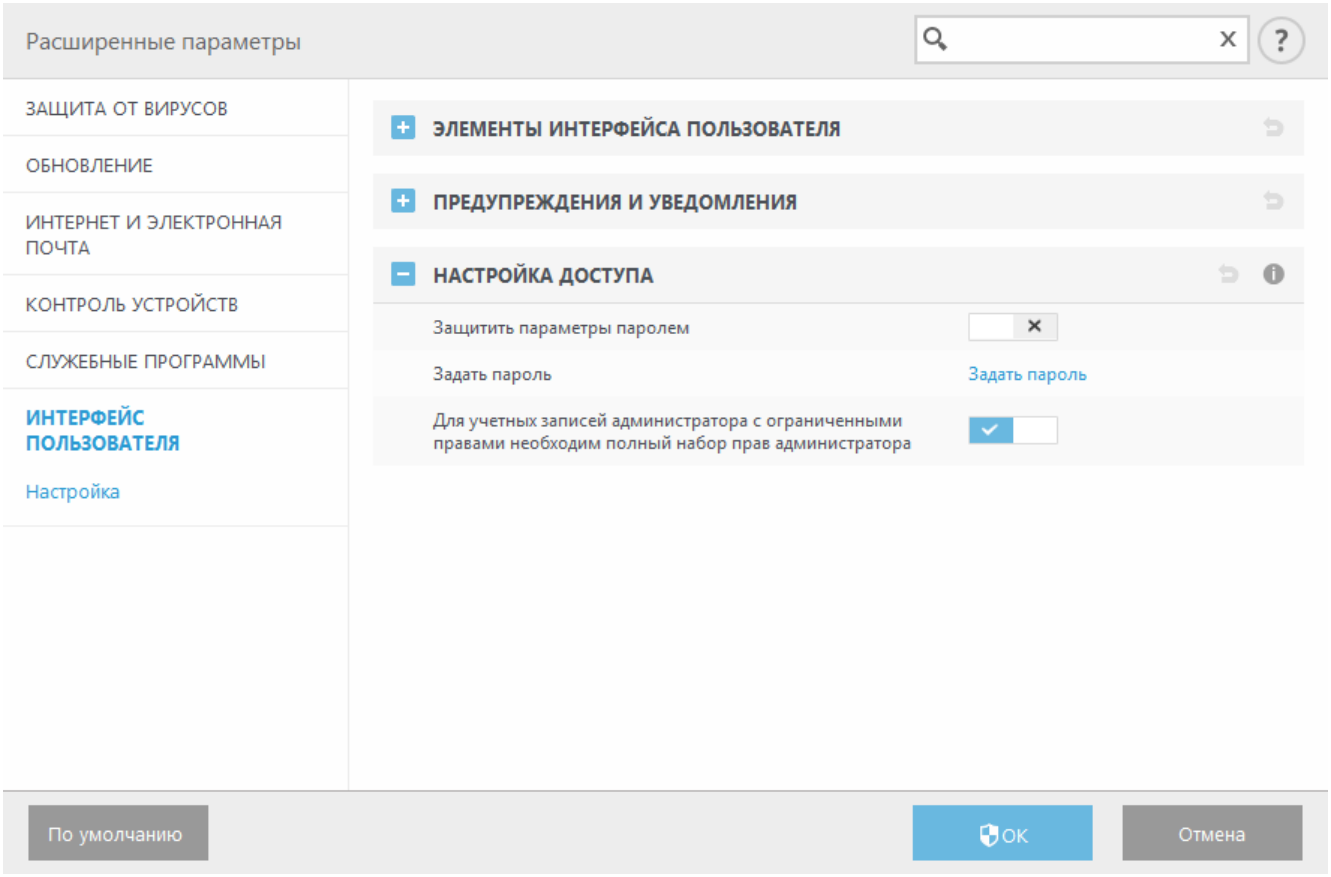
Показывать сообщения и уведомления о лицензии: если этот параметр отключен, уведомления и сообщения будут отображаться только по истечении срока действия лицензии.

ПРИМЕЧАНИЕ.
Настройки сведений о лицензии применяются, но являются недоступными, если продукт ESET Endpoint Antivirus активирован с помощью лицензии MSP.



3.9.5.2 Настройка доступа

Для обеспечения максимальной безопасности системы важно правильно настроить ESET Endpoint Antivirus. Неквалифицированное изменение параметров может привести к потере важных данных. Для предотвращения несанкционированного изменения параметры ESET Endpoint Antivirus можно защитить паролем. Настройки парольной защиты находятся в меню **Дополнительные настройки** (F5) > **Настройка доступа** > **Интерфейс пользователя**.



Защитить параметры паролем: выбор настроек парольной защиты. Щелкните, чтобы открыть окно настройки пароля.

Чтобы установить или изменить пароль для защиты параметров настройки, щелкните **Настроить**.

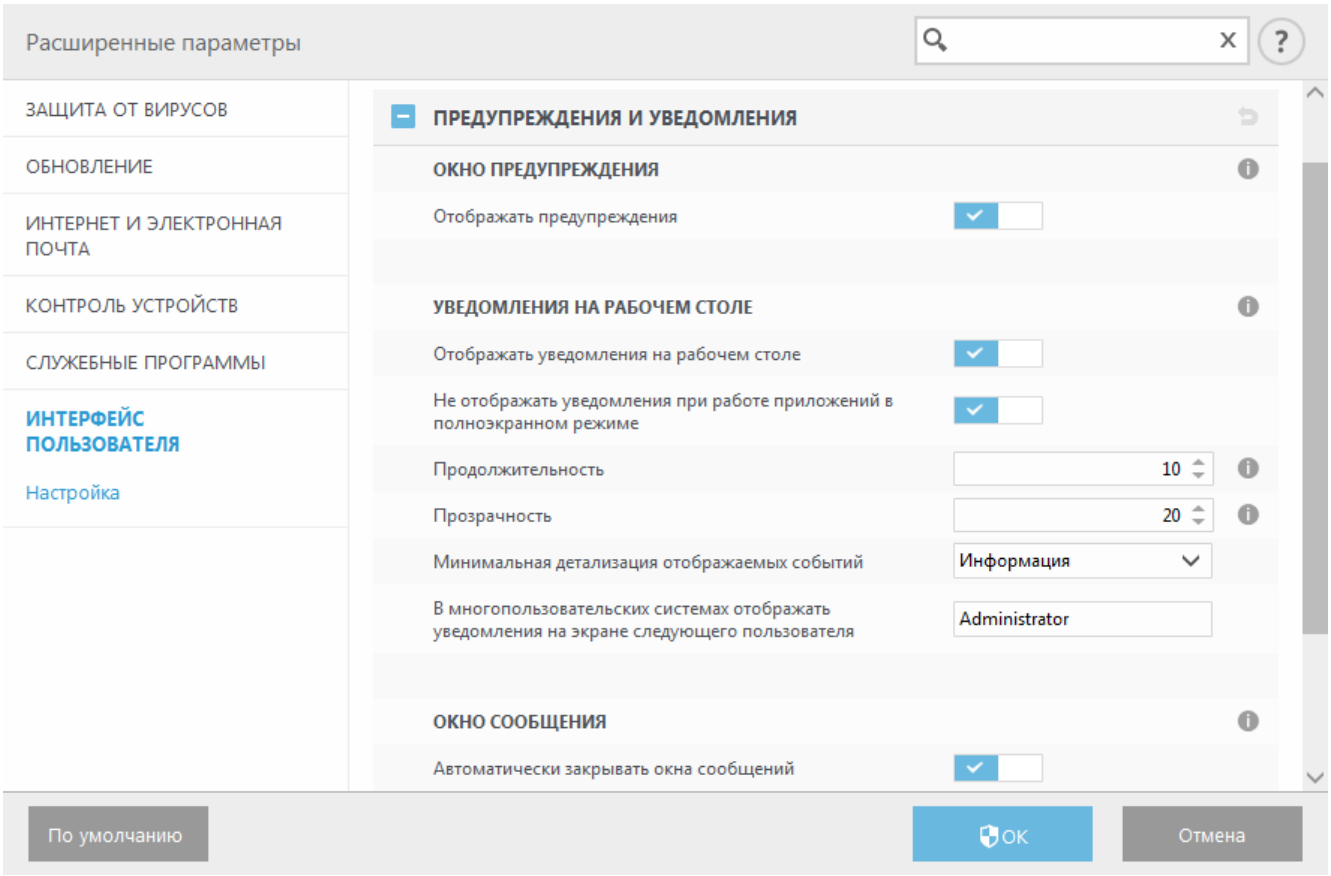
Для учетных записей администратора с ограниченными правами необходим полный набор прав администратора: оставьте этот флажок установленным, чтобы при изменении определенных параметров системы текущему пользователю (если у такого пользователя нет прав администратора) предлагалось ввести имя и пароль администратора (аналогично контролю учетных записей в Windows Vista). К изменениям относится отключение модулей защиты.

Только для Windows XP:

Требуются права администратора (система без поддержки UAC): установите этот флажок, чтобы программа ESET Endpoint Antivirus предлагала ввести учетные данные администратора.

3.9.5.3 Предупреждения и уведомления

В разделе **Предупреждения и уведомления** окна **Интерфейс** можно настроить способ обработки предупреждений об угрозах и системных уведомлений (например, сообщений об успешном выполнении обновлений) для программы ESET Endpoint Antivirus. Здесь также можно настроить время отображения и прозрачность уведомлений на панели задач (применяется только к системам, поддерживающим уведомления на панели задач).



Окно предупреждения

Если отключить параметр **Отображать предупреждение**, окна предупреждения не будут выводиться на экран. Такой подход следует использовать только в небольшом количестве особых ситуаций. В большинстве случаев рекомендуется оставить для этого параметра значение по умолчанию (включен).

Уведомления на рабочем столе

Уведомления на рабочем столе и всплывающие подсказки предназначены только для информирования и не требуют участия пользователя. Они отображаются в области уведомлений в правом нижнем углу экрана. Чтобы активировать уведомления на рабочем столе, установите флажок **Отображать уведомления на рабочем**

столе. Установите флажок **Не отображать уведомления при работе приложений в полноэкранном режиме**, чтобы запретить все неинтерактивные уведомления. Более подробные параметры, такие как время отображения и прозрачность окна уведомлений, можно изменить, выполнив инструкции ниже.

В раскрывающемся меню **Минимальная детализация отображаемых событий** можно выбрать уровень серьезности предупреждений и уведомлений, которые следует отображать. Доступны указанные ниже варианты.

- **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,и т. п.).

Последний параметр этого раздела позволяет настроить, кто именно должен получать уведомления в многопользовательской среде. В поле **В многопользовательских системах отображать уведомления для пользователя** указывается пользователь, который будет получать системные и прочие уведомления, если одновременно может быть подключено несколько пользователей. Обычно это системный или сетевой администратор. Это особенно полезно для серверов терминалов (если все системные уведомления отправляются администратору).

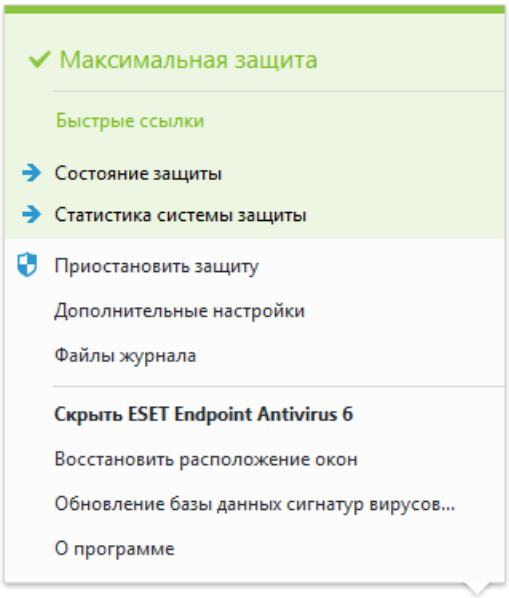
Окно сообщения

Чтобы всплывающие окна 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.

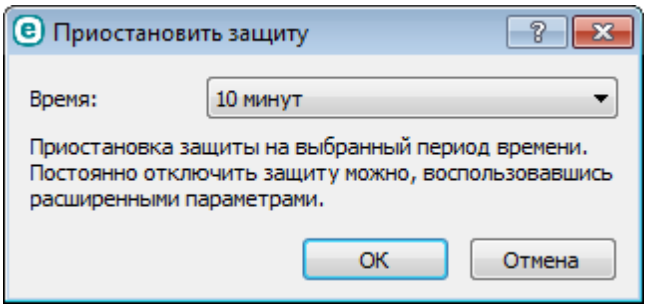
Подтверждения: отображение списка подтверждений, для которых можно настроить параметры отображения.

3.9.5.4 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 защиту от вирусов и шпионских программ, которая предотвращает атаки на компьютер, контролируя обмен файлами и данными через Интернет и электронную почту.



В раскрывающемся меню **Время** указывается период времени, на которое будет полностью отключена защита от вирусов и шпионских программ.

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

Дополнительные настройки: установите этот флажок, чтобы перейти к дереву **Дополнительные настройки**. Чтобы перейти к дополнительным настройкам, можно также нажать клавишу F5 или использовать меню **Настройка** > **Дополнительным настройки**.

Файлы журнала: файлы журнала содержат информацию обо всех важных событиях программы и предоставляют общие сведения об обнаруженных угрозах.

Скрыть ESET Endpoint Antivirus: позволяет скрыть окно ESET Endpoint Antivirus.

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

Обновление базы данных сигнатур вирусов: запуск обновления базы данных сигнатур вирусов для поддержания необходимого уровня защиты от вредоносного кода.

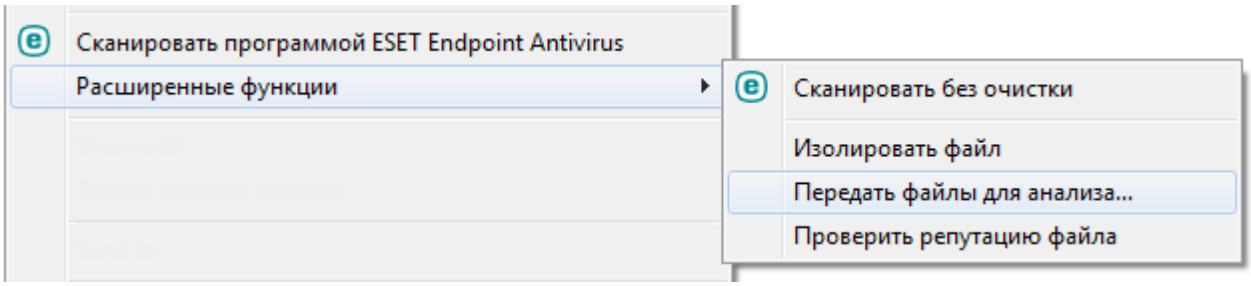
О программе: отображение системной информации, сведений об установленной версии ESET Endpoint Antivirus и модулях программы, а также срока действия лицензии. В нижней части окна представлена информация об операционной системе и системных ресурсах.

3.9.5.5 Контекстное меню

Если щелкнуть объект (файл) правой кнопкой мыши, отобразится контекстное меню. В меню указаны все действия, которые можно выполнить по отношению к объекту.

Элементы управления ESET Endpoint Antivirus можно интегрировать в контекстное меню. Настройка этих функций выполняется в дереве расширенных параметров, в разделе **Интерфейс** > **Элементы интерфейса**.

Интегрировать с контекстным меню: можно интегрировать элементы управления ESET Endpoint Antivirus в контекстное меню.



3.10 Для опытных пользователей

3.10.1 Диспетчер профилей

Диспетчер профилей используется в двух разделах ESET Endpoint Antivirus: в разделе **Сканирование компьютера по требованию** и в разделе **Обновление**.

Сканирование компьютера по требованию

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).

Для создания профиля откройте окно «Дополнительные настройки» (F5) и щелкните **Защита от вирусов** > **Сканирование компьютера по требованию**, а затем нажмите кнопку **Изменить** рядом с элементом **Список профилей**. В раскрывающемся меню **Профиль обновления** отображаются существующие профили сканирования. Для создания профиля сканирования в соответствии с конкретными потребностями см. раздел Настройка параметров модуля ThreatSense, где описывается каждый параметр, используемый для настройки сканирования.

Пример. Предположим, пользователю требуется создать собственный профиль сканирования, причем конфигурация сканирования Smart частично устраивает его, но не нужно сканировать упаковщики или потенциально опасные приложения, но при этом нужно применить **тщательную очистку**. Введите имя нового профиля в окне **Диспетчер профилей** и нажмите кнопку **Добавить**. Выберите новый профиль в раскрывающемся меню **Профиль обновления** 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.

3.10.2 Диагностика

Функция диагностики формирует аварийные дампы приложения процессов ESET (например, *ekrn*). Если происходит сбой приложения, формируется дамп памяти. Это может помочь разработчикам выполнять отладку и устранять различные проблемы ESET Endpoint Antivirus. Откройте раскрывающееся меню рядом с элементов **Тип дампа** и выберите один из трех доступных вариантов.

- Выберите **Отключить** (установлено по умолчанию), чтобы отключить эту функцию.
- **Мини**: регистрируется самый малый объем полезной информации, которая может помочь выявить 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**: регистрируется все содержимое системной памяти, когда неожиданно прекращается работа приложения. Полный дамп памяти может содержать данные процессов, которые выполнялись в момент создания дампа.

Включить расширенное ведение журнала фильтрации протоколов: запись всех сетевых данных, проходящих через модуль фильтрации протоколов в формате PCAP. Это помогает разработчикам диагностировать и устранять проблемы, связанные с фильтрацией протоколов.

Файлы журналов хранятся в расположении:
C:\ProgramData\ESET\ESET Smart Security\Diagnostics в ОС Windows Vista или более поздних версиях Windows либо по адресу *C:\Documents and Settings\All Users\...* в старых версиях Windows.

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*.

3.10.3 Импорт и экспорт параметров

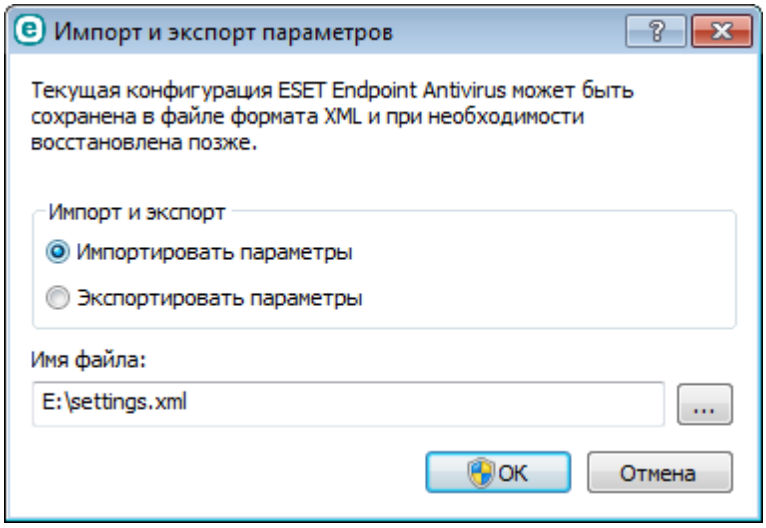
Можно импортировать и экспортировать пользовательский XML-файл конфигурации ESET Endpoint Antivirus с помощью меню **Настройка**.

Импорт и экспорт файлов конфигурации удобны, если нужно создать резервную копию текущей конфигурации программы ESET Endpoint Antivirus для использования в будущем. Экспорт параметров также удобен, если необходимо использовать предпочитаемую конфигурацию на нескольких компьютерах. С этой целью файл *.xml* можно легко импортировать для переноса нужных параметров.

Импортировать конфигурацию несложно. В главном окне программы выберите команду **Настройка** > **Импорт и экспорт параметров**, а затем — **Импортировать параметры**. Введите имя для файла конфигурации или нажмите кнопку **...**, чтобы выбрать файл конфигурации, который следует импортировать.

Процедура экспорта конфигурации похожа на ее импорт. В главном окне программы выберите **Настройка** > **Импорт и экспорт параметров**. Выберите **Экспортировать параметры** и введите имя для файла конфигурации (например, *export.xml*). С помощью проводника выберите место на компьютере для сохранения файла конфигурации.

ПРИМЕЧАНИЕ.
При экспорте параметров может возникнуть ошибка, если у вас недостаточно прав для записи экспортируемого файла в указанный каталог.



3.10.4 Командная строка

Модуль защиты от вирусов ESET Endpoint Antivirus может быть запущен из командной строки вручную (с помощью команды «ecls») или в пакетном режиме (с помощью файла BAT-файла). Использование модуля сканирования командной строки ESET:

```
ecls [ПАРАМЕТРЫ..] ФАЙЛЫ..
```

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=ОГРАНИЧЕНИЕ	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=РАСШИРЕНИЯ	сканировать только файлы с РАСШИРЕНИЯМИ, указанными через двоеточие
/ext-exclude=РАСШИРЕНИЯ	исключить из сканирования файлы с РАСШИРЕНИЯМИ, указанными через двоеточие
/clean-mode=РЕЖИМ	использовать РЕЖИМ очистки для зараженных объектов. Доступны указанные ниже варианты. • «Нет». Автоматическая очистка не выполняется. • «Стандартная (по умолчанию)». 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 независимо от их типа без проведения очистки. • «Удаление». Приложение ecls.exe удалит все файлы без проведения очистки, но не затронет важные файлы (например, 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

ПРИМЕЧАНИЕ.
Значение кода завершения больше 100 означает, что файл не был просканирован и может быть заражен.

3.10.5 Сканирование в состоянии простоя

Настройки сканирования в состоянии простоя можно изменить в меню **Дополнительные настройки** > **Защита от вирусов** > **Сканирование в состоянии простоя** > **Сканирование в состоянии простоя**. Данные параметры позволяют указать условие запуска обнаружения в состоянии простоя, например когда:

- запущена заставка;
- компьютер заблокирован;
- пользователь выполняет выход.

Используйте флажки для каждого состояния, чтобы включить или отключить различные условия обнаружения в состоянии простоя.

3.10.6 ESET SysInspector

3.10.6.1 Знакомство с ESET SysInspector

ESET SysInspector — это приложение, которое тщательно проверяет компьютер и отображает собранные данные в обобщенном виде. Такая информация, как данные об установленных драйверах и приложениях, сетевых соединениях и важных записях в реестре, позволяет определить причину подозрительного поведения системы, которое могло иметь место, например, вследствие несовместимости программного или аппаратного обеспечения или заражения вредоносными программами.

Доступ к программе ESET SysInspector можно получить двумя способами: воспользовавшись ее интегрированной версией в решениях ESET Security или бесплатно загрузив автономную версию (SysInspector.exe) с веб-сайта ESET. Обе версии работают одинаково и имеют одинаковое управление. Единственная разница состоит в способе управления полученными данными. И автономная, и интегрированная версии дают возможность экспортировать снимки системы в *XML*-файлы и сохранять их на диске. Однако интегрированная версия позволяет также сохранять снимки системы непосредственно в меню **Служебные программы** > **ESET SysInspector** (за исключением программы ESET Remote Administrator). Дополнительные сведения см. в разделе ESET SysInspector как часть приложения ESET Endpoint Antivirus.

Подождите некоторое время, пока программа ESET SysInspector сканирует компьютер. Это может занять от 10 секунд до нескольких минут в зависимости от конфигурации оборудования, операционной системы и количества установленных на компьютере приложений.

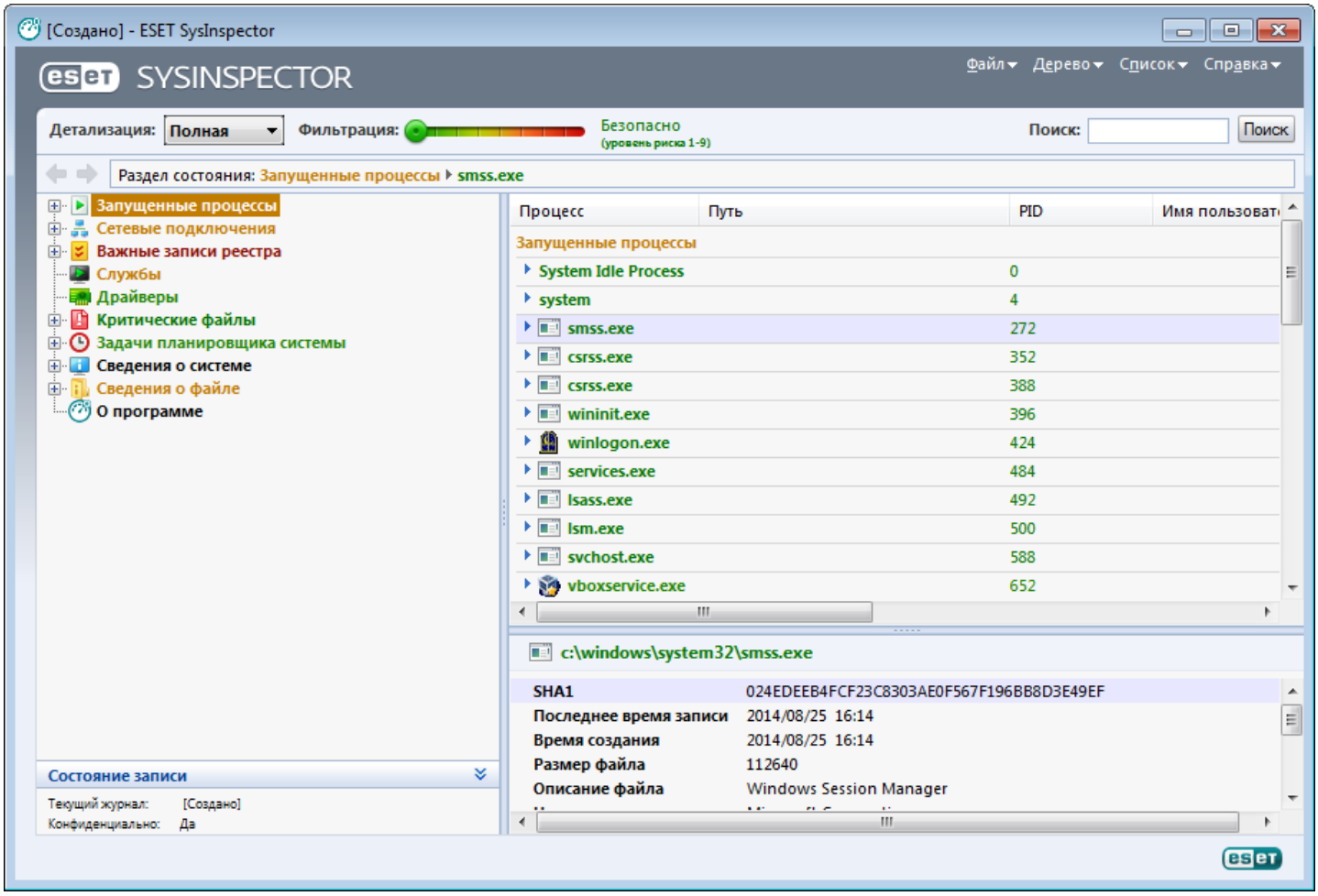
3.10.6.1.1 Запуск ESET SysInspector

Чтобы запустить ESET SysInspector, достаточно выполнить файл *SysInspector.exe*, загруженный с веб-сайта ESET. Если у вас уже установлено одно из решений ESET Security, можно запустить ESET SysInspector непосредственно из меню «Пуск» (**Программы** > **ESET** > **ESET Endpoint Antivirus**).

Подождите, пока программа проверяет систему. Это может занять несколько минут.

3.10.6.2 Интерфейс пользователя и работа в приложении

Для ясности главное окно программы разделено на четыре основных раздела: вверху главного окна программы находятся элементы управления программой, слева — окно навигации, справа — окно описания, а внизу — окно подробных сведений. В разделе «Состояние журнала» отображаются основные параметры журнала (используемый фильтр, тип фильтра, является ли журнал результатом сравнения и т. д.).



3.10.6.2.1 Элементы управления программой

В этом разделе описаны все элементы управления приложением ESET SysInspector.

Файл

Щелкнув элемент **Файл**, можно сохранить данные о текущем состоянии системы для их последующего изучения или открыть ранее сохраненный журнал. Если планируется опубликовать журнал, при его создании рекомендуется использовать параметр **Подходит для отправки**. В этом случае из него исключается конфиденциальная информация (например, имя текущего пользователя, имя компьютера и домена, права текущего пользователя, переменные среды и т. п.).

ПРИМЕЧАНИЕ.
Чтобы открыть сохраненные ранее отчеты ESET SysInspector, достаточно просто перетащить их в главное окно программы. Эта функция недоступна в операционной системе Windows Vista по соображениям

безопасности.

Дерево

Позволяет развернуть или закрыть все узлы, а также экспортировать выбранные разделы в сценарий обслуживания.

Список

Содержит функции, облегчающие навигацию в программе, а также прочие функции, например средства поиска информации в Интернете.

Справка

Содержит сведения о приложении и его функциях.

Подробнее

Этот параметр влияет на выводимую в главном окне программы информацию, облегчая работу с ней. В базовом режиме пользователю доступна информация, необходимая для поиска решений стандартных проблем, возникающих в системе. В среднем режиме отображаются расширенные данные. В полном режиме программа ESET SysInspector отображает всю информацию, необходимую для решения самых нестандартных проблем.

Фильтрация

Используется для поиска подозрительных файлов или записей в реестре системы. С помощью ползунка можно фильтровать элементы по их уровню риска. Если ползунок установлен в крайнее левое положение (уровень риска 1), отображаются все элементы. При перемещении ползунка вправо программа отфильтровывает все элементы с уровнем риска, который меньше текущего, и выводит на экран только те элементы, уровень подозрительности которых выше отображаемого уровня. Если ползунок находится в крайнем правом положении, программа отображает только известные вредоносные элементы.

Все элементы, имеющие уровень риска от 6 до 9, могут представлять угрозу для безопасности. Если вы не используете решение ESET по обеспечению безопасности, после нахождения программой ESET SysInspector такого элемента рекомендуется проверить систему с помощью ESET Online Scanner. ESET Online Scanner является бесплатной службой.

ПРИМЕЧАНИЕ.
Уровень риска элемента легко определяется путем сравнения цвета элемента с цветом на ползунке уровней рисков.

Сравнение

При сравнении двух журналов можно выбрать, какие элементы следует отображать: все элементы, только добавленные элементы, только удаленные элементы или только замененные элементы.

Поиск

Служит для быстрого нахождения определенного элемента по его названию или части названия. Результаты поиска отображаются в окне описания.

Возврат

С помощью стрелок назад и вперед можно вернуться в окно описания к ранее отображенной информации. Вместо стрелок перехода назад и вперед можно использовать клавиши BACKSPACE и пробел.

Раздел состояния

Отображает текущий узел в окне навигации.

ВАЖНО!
Элементы, выделенные красным цветом, являются неизвестными, поэтому программа помечает их как

потенциально опасные. Если элемент выделен красным, это не означает, что его можно удалить. Перед удалением убедитесь в том, что эти файлы действительно опасны и не являются необходимыми.

3.10.6.2.2 Навигация в ESET SysInspector

ESET SysInspector распределяет информацию разного типа по нескольким базовым разделам, называемым узлами. Чтобы получить дополнительные сведения, разверните подузлы соответствующего узла. Чтобы развернуть или свернуть узел, дважды щелкните имя узла либо рядом с именем щелкните значок ⊞ или ⊟. При перемещении по древовидной структуре узлов и подузлов в окне навигации о каждом узле доступны различные сведения, отображаемые в окне описания. При переходе в окне описания к конкретному элементу в окне подробной информации появляются дополнительные сведения о нем.

Ниже описаны главные узлы в окне навигации и относящиеся к ним сведения в окнах описания и подробной информации.

Запущенные процессы

Этот узел содержит сведения о приложениях и процессах, выполняемых в момент создания журнала. В окне описания могут находиться дополнительные сведения о каждом из процессов, например названия динамических библиотек, используемых процессом, и их местонахождение в системе, название поставщика приложения и уровень риска файла.

Окно подробной информации содержит дополнительные сведения об элементах, выбранных в окне описания, например размер файла или его хэш.

ПРИМЕЧАНИЕ.
Любая операционная система состоит из нескольких важных компонентов ядра, которые постоянно работают и обеспечивают работу базовых крайне важных функций для других пользовательских приложений. В определенных случаях путь к файлам таких процессов начинается в программе ESET SysInspector с символов «\??\». Эти символы обеспечивают таким процессам оптимизацию до запуска и с точки зрения системы являются безопасными.

Сетевые подключения

В окне описания перечислены процессы и приложения, которые обмениваются данными через сеть по протоколу, выбранному в окне навигации (TCP или UDP), а также удаленные адреса, с которыми эти приложения устанавливают соединения. Также в нем можно найти IP-адреса DNS-серверов.

Окно подробной информации содержит дополнительные сведения об элементах, выбранных в окне описания, например размер файла или его хэш.

Важные записи реестра

Содержит список определенных записей реестра, которые часто бывают связаны с различными проблемами в системе: например, записи с указанием автоматически загружаемых программ, вспомогательных объектов браузера и т. п.

В окне описания можно узнать, какие файлы связаны с определенными записями реестра. Дополнительная информация отображается в окне подробных сведений.

Службы

В окне описания перечислены файлы, зарегистрированные как службы Windows. В окне подробных сведений можно увидеть способ запуска службы, а также просмотреть некоторую дополнительную информацию.

Драйверы

Список драйверов, установленных в системе.

Критические файлы

В окне описания отображается содержимое критически важных файлов операционной системы Microsoft

Windows.

Задачи системного планировщика

Отображается список задач, инициируемых планировщиком заданий Windows в определенное время/период времени.

Информация о системе

Содержит подробные сведения об оборудовании и программном обеспечении, а также сведения о заданных переменных среды, правах пользователей и журналах системных событий.

Сведения о файле

Список важных системных файлов и файлов из папки Program Files. В окнах описания и подробных сведений может отображаться дополнительная информация о них.

О программе

Сведения о версии программы ESET SysInspector и список программных модулей.

3.10.6.2.2.1 Сочетания клавиш

Ниже перечислены сочетания клавиш, которые можно использовать при работе с программой ESET SysInspector.

Файл

Ctrl+O	открывает существующий журнал
Ctrl+S	сохраняет созданные журналы

Создание

Ctrl+G	создает стандартный снимок состояния компьютера
Ctrl+H	создает снимок состояния компьютера, который также может содержать конфиденциальную информацию

Фильтрация элементов

1, O	безопасно, отображаются элементы с уровнем риска 1–9
2	безопасно, отображаются элементы с уровнем риска 2–9
3	безопасно, отображаются элементы с уровнем риска 3–9
4, U	неизвестно, отображаются элементы с уровнем риска 4–9
5	неизвестно, отображаются элементы с уровнем риска 5–9
6	неизвестно, отображаются элементы с уровнем риска 6–9
7, B	опасно, отображаются элементы с уровнем риска 7–9
8	опасно, отображаются элементы с уровнем риска 8–9
9	опасно, отображаются элементы с уровнем риска 9
-	понижает уровень риска
+	повышает уровень риска
Ctrl+9	режим фильтрации, равный или более высокий уровень
Ctrl+0	режим фильтрации, только равный уровень

Вид

Ctrl+5	просмотр по производителям, все производители
Ctrl+6	просмотр по производителям, только Майкрософт
Ctrl+7	просмотр по производителям, все другие производители
Ctrl+3	отображение полных сведений
Ctrl+2	отображение сведений средней степени подробности
Ctrl+1	основной вид
BACKSPACE	переход на один шаг назад
Пробел	переход на один шаг вперед

Ctrl+W	развертывание дерева
Ctrl+Q	свертывание дерева

Прочие элементы управления

Ctrl+T	переход к исходному расположению элемента после его выбора в результатах поиска
Ctrl+P	отображение базовых сведений об объекте
Ctrl+A	отображение полных сведений об объекте
Ctrl+C	копирование дерева текущего элемента
Ctrl+X	копирование элементов
Ctrl+B	поиск сведений о выбранных файлах в Интернете
Ctrl+L	открытие папки, в которой находится выбранный файл
Ctrl+R	открытие соответствующей записи в редакторе реестра
Ctrl+Z	копирование пути к файлу (если элемент связан с файлом)
Ctrl+F	переход в поле поиска
Ctrl+D	закрытие результатов поиска
Ctrl+E	запуск сценария обслуживания

Сравнение

Ctrl+Alt+O	открытие исходного или сравнительного журнала
Ctrl+Alt+R	отмена сравнения
Ctrl+Alt+1	отображение всех элементов
Ctrl+Alt+2	отображение только добавленных элементов (отображаются только элементы из текущего журнала)
Ctrl+Alt+3	отображение только удаленных элементов (отображаются элементы из предыдущей версии журнала)
Ctrl+Alt+4	отображение только замененных элементов (включая файлы)
Ctrl+Alt+5	отображение только различий между журналами
Ctrl+Alt+C	отображение результатов сравнения
Ctrl+Alt+N	отображение текущего журнала
Ctrl+Alt+P	отображение предыдущей версии журнала

Разное

F1	вызов справки
Alt+F4	закрытие программы
Alt+Shift+F4	закрытие программы без вывода запроса
Ctrl+I	статистика журнала

3.10.6.2.3 Сравнение

С помощью функции сравнения пользователь может сравнить два существующих журнала. Результатом работы этой команды является набор элементов, не совпадающих в этих журналах. Это позволяет отслеживать изменения в системе, что удобно для обнаружения вредоносного кода.

После запуска приложение создает новый журнал, который открывается в новом окне. Чтобы сохранить журнал в файл, в меню **Файл** выберите пункт **Сохранить журнал**. Сохраненные файлы журналов можно впоследствии открывать и просматривать. Чтобы открыть существующий журнал, в меню **Файл** выберите пункт **Открыть журнал**. В главном окне программы ESET SysInspector всегда отображается только один журнал.

Преимуществом функции сравнения двух журналов является то, что она позволяет просматривать активный на данный момент журнал и журнал, сохраненный в файле. Для сравнения журналов в меню **Файл** выберите пункт **Сравнить журналы** и выполните команду **Выбрать файл**. Выбранный журнал сравнивается с активным журналом в главном окне программы. Сравнительный журнал будет содержать только различия между двумя сравниваемыми журналами.

ПРИМЕЧАНИЕ.
При сравнении двух файлов журнала в меню **Файл** выберите пункт **Сохранить журнал** и сохраните журнал как файл в формате ZIP. В результате будут сохранены оба файла. Если такой файл впоследствии открыть,

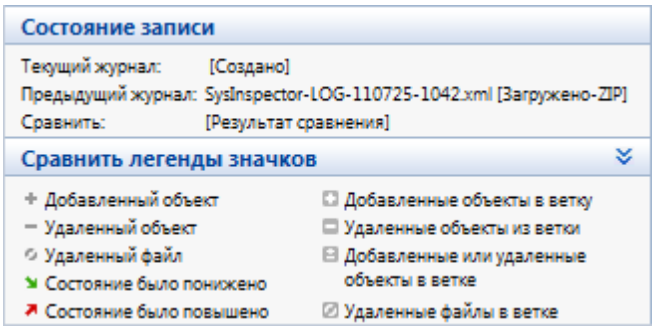
содержащиеся в нем журналы сравниваются автоматически.

Рядом с отображенными элементами ESET SysInspector добавляет символы, указывающие на различия между журналами.

Ниже описаны все символы, которые могут отображаться рядом с элементами.

- + новое значение, отсутствует в предыдущем журнале
- раздел древовидной структуры содержит новые значения
- – удаленное значение, присутствует только в предыдущей версии журнала
- раздел древовидной структуры содержит удаленные значения
- значение или файл были изменены
- раздел древовидной структуры содержит измененные значения или файлы
- уровень риска снизился или был выше в предыдущей версии журнала
- уровень риска повысился или был ниже в предыдущей версии журнала

В разделе пояснений в левом нижнем углу отображается описание всех символов, а также названия сравниваемых журналов.



Любой сравниваемый журнал можно сохранить в файл и открыть позже.

Пример

Создайте и сохраните журнал, содержащий исходную информацию о системе, в файл с названием «предыдущий.xml». Внеся в систему изменения, откройте ESET SysInspector и создайте новый журнал. Сохраните его в файл с названием *текущий.xml*.

Чтобы отследить различия между этими двумя журналами, в меню **Файл** выберите пункт **Сравнить журналы**. Программа создаст сравнительный журнал с перечнем различий между исходными журналами.

Тот же результат можно получить с помощью следующей команды, вызываемой из командной строки:

SysIsnpector.exe текущий.xml предыдущий.xml

3.10.6.3 Параметры командной строки

В ESET SysInspector можно формировать отчеты из командной строки. Для этого используются перечисленные ниже параметры.

/gen	создание журнала из командной строки без запуска графического интерфейса пользователя
/privacy	создание журнала без конфиденциальной информации
/zip	сохранение созданного журнала в ZIP-архиве
/silent	скрытие окна хода выполнения при создании журнала из командной строки
/blank	запуск ESET SysInspector без создания или загрузки журнала

Примеры

Использование:

```
Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]
```

Чтобы открыть определенный журнал непосредственно в браузере, воспользуйтесь следующей командой: *SysInspector.exe .\клиентский_журнал.xml*
Чтобы создать журнал из командной строки, воспользуйтесь следующей командой: *SysInspector.exe /gen=.\мой_новый_журнал.xml*
Чтобы создать журнал, из которого исключена конфиденциальная информация, непосредственно в сжатом файле, воспользуйтесь следующей командой: *SysInspector.exe /gen=.\мой_новый_журнал.zip /privacy /zip*
Чтобы сравнить два журнала и просмотреть различия, воспользуйтесь следующей командой: *SysInspector.exe новый.xml старый.xml*

ПРИМЕЧАНИЕ.
Если название файла или папки содержит пробел, это название необходимо заключить в кавычки.

3.10.6.4 Сценарий обслуживания

Сценарий обслуживания является средством для пользователей программы ESET SysInspector, с помощью которого можно легко удалить из системы нежелательные объекты.

Сценарий обслуживания позволяет целиком или частично экспортировать журнал ESET SysInspector. После экспорта можно отметить нежелательные объекты для удаления. Затем можно запустить отредактированный журнал для удаления отмеченных объектов.

Сценарий обслуживания предназначен для пользователей, имеющих определенный опыт в диагностике компьютерных систем. Неквалифицированное использование данного средства может привести к неисправности операционной системы.

Пример

При наличии подозрения о заражении компьютера вирусом, который не обнаруживается программой защиты от вирусов, выполните приведенные ниже пошаговые инструкции.

1. Запустите ESET SysInspector и создайте новый снимок системы.
2. Выберите первый элемент в разделе слева (в древовидной структуре), нажмите клавишу SHIFT, а затем выберите последний объект, чтобы отметить все элементы в списке.
3. Щелкните выделенные объекты правой кнопкой мыши и в контекстном меню выберите пункт **Экспортировать выбранные разделы в сценарий службы**.
4. Выбранные объекты будут экспортированы в новый журнал.
5. Далее следует наиболее важный шаг всей процедуры: откройте созданный журнал и измените атрибут «-» на «+» для всех объектов, подлежащих удалению. Убедитесь, что не отмечены какие-либо важные для операционной системы файлы или объекты.
6. Откройте ESET SysInspector, выберите **Файл** > **Запустить сценарий обслуживания** и укажите путь к своему сценарию.
7. Нажмите кнопку **ОК**, чтобы запустить сценарий.

3.10.6.4.1 Создание сценария обслуживания

Чтобы создать сценарий, щелкните правой кнопкой мыши любой элемент в древовидном меню (на левой панели) в главном окне ESET SysInspector. В контекстном меню выберите команду **Экспортировать все разделы в сценарий службы** или **Экспортировать выбранные разделы в сценарий службы**.

ПРИМЕЧАНИЕ.
Сценарий обслуживания нельзя экспортировать в ходе сравнения двух журналов.

3.10.6.4.2 Структура сценария обслуживания

Первая строка заголовка сценария содержит данные о версии ядра (ev), версии интерфейса (gv) и версии журнала (lv). Эти данные позволяют отслеживать изменения в XML-файле, используемом для создания сценария. Они гарантируют согласованность на этапе выполнения. Эту часть сценария изменять не следует.

Остальное содержимое файла разбито на разделы, объекты в которых можно редактировать. Те из них, которые должны быть обработаны сценарием, следует пометить. Для этого символ «-» перед объектом надо заменить на символ «+». Разделы отделены друг от друга пустой строкой. Каждый раздел имеет собственный номер и название.

01) Запущенные процессы

Этот раздел содержит список всех процессов, запущенных в системе. Каждый процесс идентифицируется по UNC-пути, а также по хэшу CRC16, заключенному в символы звездочки (*).

Пример

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

В данном примере выбран (помечен символом «+») процесс module32.exe. При выполнении сценария этот процесс будет завершен.

02) Загруженные модули

В этом разделе перечислены используемые в данный момент системные модули.

Пример

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

В данном примере модуль khbekhb.dll помечен символом «+». При выполнении сценария процессы, использующие данный модуль, распознаются и прерываются.

03) TCP-соединения

Этот раздел содержит данные о существующих TCP-соединениях.

Пример

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

При запуске этого сценария обнаруживается владелец сокета помеченного TCP-соединения, после чего сокет останавливается, высвобождая системные ресурсы.

04) Конечные точки UDP

Этот раздел содержит информацию о существующих конечных точках UDP.

Пример

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

При выполнении сценария определяется владелец сокета помеченных конечных точек UDP, после чего сокет останавливается.

05) Записи DNS-сервера

Этот раздел содержит информацию о текущей конфигурации DNS-сервера.

Пример

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

При выполнении сценария помеченные записи DNS-сервера удаляются.

06) Важные записи реестра

Этот раздел содержит информацию о важных записях реестра.

Пример

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

При выполнении сценария помеченные записи будут удалены, сведены к 0-разрядным значениям или сброшены к значениям по умолчанию. Действия, применяемые к конкретным записям, зависят от категории и значения раздела в определенной записи реестра.

07) Службы

Этот раздел содержит список служб, зарегистрированных в системе.

Пример

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

При выполнении сценария помеченные службы и все зависящие от них службы будут остановлены и удалены.

08) Драйверы

В этом разделе перечислены установленные драйверы.

Пример

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

При выполнении сценария выбранные драйверы останавливаются. Следует учесть, что некоторые драйверы не позволяют остановить свою работу.

09) Важные файлы

Этот раздел содержит информацию о файлах, критически важных с точки зрения правильной работы операционной системы.

Пример

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Выбранные объекты будут удалены или возвращены к исходным значениям.

3.10.6.4.3 Выполнение сценариев обслуживания

Отметьте все нужные объекты, а затем сохраните и закройте сценарий. Запустите измененный сценарий непосредственно из главного окна программы ESET SysInspector с помощью команды **Запустить сценарий обслуживания** в меню «Файл». При открытии сценария появится следующее сообщение: **Выполнить сценарий обслуживания «%Scriptname%»?** После подтверждения может появиться еще одно предупреждение, сообщающее о попытке запуска неподписанного сценария. Чтобы запустить сценарий, нажмите кнопку **Запуск**.

В диалоговом окне появится подтверждение успешного выполнения сценария.

Если сценарий может быть обработан только частично, отобразится следующее сообщение: **Сценарий обслуживания выполнен частично. Показать отчет об ошибке?** Чтобы просмотреть полный отчет об ошибках, в котором перечислены невыполненные действия, нажмите кнопку **Да**.

Если сценарий не был признан действительным, отобразится следующее сообщение: **Выбранный сценарий обслуживания не подписан. Выполнение неподписанных и неизвестных сценариев может привести к повреждению данных на компьютере. Выполнить сценарий и все действия?** Это может быть вызвано несоответствиями в сценарии (поврежден заголовок, искажено название раздела, пропущена пустая строка между разделами и т. д.). В этом случае откройте файл сценария и исправьте ошибки либо создайте новый сценарий обслуживания.

3.10.6.5 Часто задаваемые вопросы

Требуются ли для запуска ESET SysInspector права администратора?

Хотя для запуска ESET SysInspector права администратора не требуются, некоторые из собираемых этим приложением данных доступны только для учетной записи администратора. Запуск с правами обычного пользователя или с ограниченными правами приведет к сбору меньшего объема данных о системе.

Создает ли ESET SysInspector файл журнала?

ESET SysInspector может создать файл журнала с конфигурацией системы. Для сохранения такого журнала в главном окне программы выберите **Файл** > **Сохранить журнал**. Журналы сохраняются в формате XML. По умолчанию файлы сохраняются в папке *%USERPROFILE%\Мои документы* и получают название типа «SysInpsector-%COMPUTERNAME%-ГГММДД-ЧЧММ.XML». Перед сохранением файла журнала можно изменить его расположение и имя.

Как просмотреть файл журнала ESET SysInspector?

Для просмотра файла журнала, созданного в ESET SysInspector, запустите программу и в главном окне выберите **Файл** > **Открыть журнал**. Кроме того, файлы журнала можно перетаскивать в окно приложения ESET SysInspector. Если вы часто просматриваете файлы журнала ESET SysInspector, создайте на рабочем столе ярлык для файла SYSINSPECTOR.EXE. После этого файлы для просмотра можно просто перетаскивать на этот ярлык. По соображениям безопасности в ОС Windows Vista/7 может быть запрещено перетаскивать элементы между окнами с разными настройками безопасности.

Доступна ли спецификация для формата файлов журнала? Существует ли пакет SDK?

В настоящее время ни спецификация файла журнала, ни пакет SDK недоступны, поскольку программа все еще находится на стадии разработки. После выхода окончательной версии программы мы можем предоставить эти данные по просьбам клиентов.

Как ESET SysInspector оценивает риск определенного объекта?

В большинстве случаев ESET SysInspector присваивает объектам (файлам, процессам, разделам в реестре и т. п.) уровни риска, используя наборы эвристических правил, которые изучают характеристики каждого объекта и затем оценивают угрозу их вредоносного действия. По результатам этого эвристического анализа объектам присваивается уровень риска от 1 — хорошо (зеленый) до 9 — опасно (красный). В окне навигации слева разделы окрашиваются в разные цвета в зависимости от уровня риска объекта внутри них.

Означает ли уровень риска «6 — неизвестно (красный)», что объект является опасным?

Анализ ESET SysInspector не гарантирует, что данный объект является вредоносным — эта оценка должна выполняться специалистом по безопасности. Приложение ESET SysInspector разработано для того, чтобы специалист по безопасности имел возможность быстро оценить, какие объекты системы следует проверить в связи с их необычным поведением.

Зачем ESET SysInspector в ходе работы подключается к Интернету?

Как и многие приложения, программа ESET SysInspector подписана цифровым сертификатом, гарантирующим, что издателем программы является компания ESET и что программа не была изменена. Для проверки сертификата и подлинности издателя программы операционная система связывается с центром сертификации. Это нормальное поведение программ с цифровой подписью в Microsoft Windows.

Что такое технология Anti-Stealth?

Технология Anti-Stealth обеспечивает эффективное обнаружение руткитов.

Если система атакована вредоносной программой, которая ведет себя как руткит, пользователь может подвергнуться риску потери или кражи данных. Без специального инструмента для борьбы с руткитами такие программы практически невозможно обнаружить.

Почему иногда в файлах, помеченных как «Подписано MS», в записи «Название компании» стоит название другой компании?

В ходе идентификации цифровой подписи исполняемого файла программа ESET SysInspector сначала проверяет наличие в файле встроенной цифровой подписи. Если цифровая подпись найдена, файл будет проверен с использованием этих данных. Если цифровая подпись не найдена, программа ESI начинает поиск соответствующего CAT-файла (в каталоге безопасности *%systemroot%\system32\catroot*), содержащего сведения об обрабатываемом исполняемом файле. Если соответствующий CAT-файл найден, его цифровая подпись применяется при проверке исполняемого файла.

Поэтому иногда в некоторых файлах с пометкой «Подписано MS» имеется запись с названием другой компании.

3.10.6.6 ESET SysInspector как часть приложения ESET Endpoint Antivirus

Чтобы открыть раздел ESET SysInspector в ESET Endpoint Antivirus, выберите **Служебные программы** > **ESET SysInspector**. В окне ESET SysInspector используется примерно такая же система управления, как и в окнах журналов сканирования и запланированных задач. Чтобы выполнить любую операцию со снимками системы (создание, просмотр, сравнение, удаление и экспорт), требуется всего несколько простых действий.

Окно ESET SysInspector содержит основные сведения о созданных снимках, такие как время создания, краткий комментарий, имя создавшего снимок пользователя, а также состояние снимка.

Для сравнения, создания или удаления снимков используются соответствующие кнопки, расположенные в окне ESET SysInspector под списком снимков. Эти функции также можно вызвать из контекстного меню. Для просмотра выбранного снимка системы используется команда контекстного меню **Показать**. Чтобы экспортировать выбранный снимок в файл, щелкните его правой кнопкой мыши и выберите команду **Экспорт...**.

Ниже приведено подробное описание каждой из функций.

- **Сравнить** — сравнение двух существующих журналов. Эта функция пригодится, если вам потребуется проследить различия между текущим и более старым журналом. Для сравнения необходимо выбрать два снимка.
- **Создать...** — создание новой записи. Перед созданием записи нужно ввести краткий комментарий к ней. В столбце **Состояние** отображается ход создания снимка. Все уже созданные снимки помечены надписью **Создано**.
- **Удалить/Удалить все** — удаление записей из списка.
- **Экспорт...** — сохранение выбранной записи в XML-файл с возможностью упаковки в ZIP-архив.

3.11 Глоссарий

3.11.1 Типы угроз

Под заражением понимается вредоносная программа, которая пытается проникнуть на компьютер пользователя и (или) причинить ему вред.

3.11.1.1 Вирусы

Компьютерный вирус — это фрагмент злонамеренного кода, который добавляется в начало или конец файлов на компьютере. Название было выбрано из-за сходства с биологическими вирусами, так как они используют похожие методы для распространения с компьютера на компьютер. Часто термином «вирус» неверно обозначают любые типы угроз. Однако постепенно он выводится из употребления, и на смену ему приходит более точный термин «вредоносная программа».

Компьютерные вирусы атакуют в основном исполняемые файлы и документы. Компьютерный вирус функционирует следующим способом: после запуска зараженного файла вызывается и выполняется злонамеренный код. Это происходит до выполнения исходного приложения. Вирус способен заразить все файлы, на запись в которые у пользователя есть права.

Компьютерные вирусы могут быть разными по целям и степени опасности. Некоторые из вирусов особо опасны, так как могут целенаправленно удалять файлы с жесткого диска. С другой стороны, некоторые вирусы не причиняют никакого вреда. Они просто раздражают пользователя и демонстрируют возможности своих авторов.

Если ваш компьютер заражен вирусом, который не удается очистить, отправьте соответствующие файлы в лабораторию ESET для изучения. В ряде случаев зараженные файлы изменяются настолько, что их невозможно очистить. В таком случае их нужно заменять чистыми копиями.

3.11.1.2 Черви

Компьютерные черви — это содержащие злонамеренный код программы, которые атакуют главные компьютеры и распространяются через сеть. Основное различие между вирусами и червями заключается в том, что черви могут распространяться самостоятельно, так как они не зависят от зараженных файлов или загрузочных секторов. Черви распространяются, используя адресную книгу пользователя или уязвимости в системе безопасности сетевых приложений.

Поэтому черви намного более подвижны, чем компьютерные вирусы. Благодаря широкой популярности Интернета они могут распространяться по всему земному шару за считанные часы или даже минуты после запуска. Эта способность быстро самостоятельно реплицироваться делает черви более опасными, чем другие типы вредоносных программ.

Действующий в системе червь может доставить множество неудобств пользователю: он может удалять файлы, снижать производительность системы или даже отключать другие программы. По сути компьютерный червь может служить в качестве «транспортного средства» для других типов заражений.

Если компьютер заражен червем, рекомендуется удалить зараженные файлы, поскольку они с большой вероятностью содержат злонамеренный код.

3.11.1.3 Троянские программы

Исторически троянскими программами называли такой класс угроз, которые пытаются маскироваться под полезные программы, тем самым заставляя пользователя запускать их.

Так как эта категория весьма широка, ее часто разбивают на несколько подкатегорий.

- **Загрузчик**— вредоносная программа, способная загружать другие угрозы из Интернета.
- **Dropper**— вредоносная программа, которая предназначена для заражения компьютеров другими вредоносными программами.
- **Backdoor**— вредоносная программа, которая обменивается данными со злоумышленниками, позволяя им получить доступ к компьютеру и контроль над ним.
- **Клавиатурный шпион** — программа, которая регистрирует все, что пользователь набирает на клавиатуре, и отправляет эту информацию злоумышленникам.
- **Программа дозвона** — вредоносная программа, которая предназначена для подключения к номерам с высокими тарифными планами, а не к поставщику интернет-услуг пользователя. При этом пользователь практически не может заметить, что создано новое подключение. Программы дозвона могут нанести вред только пользователям модемов. К счастью, модемы уже не распространены столь широко, как раньше.

Если на компьютере обнаружен файл, классифицированный как троянская программа, рекомендуется удалить его, так как он с большой вероятностью содержит злонамеренный код.

3.11.1.4 Руткиты

Руткитом называется вредоносная программа, которая предоставляет злоумышленникам полный доступ к компьютеру, не проявляя при этом своего присутствия в системе. После получения доступа к системе (обычно путем использования ее уязвимостей) руткиты используют функции операционной системы, чтобы избежать обнаружения программным обеспечением защиты от вирусов: используются механизмы маскировки процессов, файлов и данных системного реестра. По этой причине их активность невозможно обнаружить стандартными методами проверки.

Существует два уровня обнаружения, направленных на борьбу с руткитами.

1. Обнаружение при попытке доступа к системе. Их еще нет в системе, то есть они не активны. Многие системы защиты от вирусов способны устранить руткиты на этом уровне (при условии, что они действительно обнаруживают такие файлы как зараженные).
2. Обнаружение при попытке скрыться во время обычной проверки. Пользователям ESET Endpoint Antivirus доступны преимущества технологии Anti-Stealth, которая также позволяет обнаруживать и устранять активные руткиты.

3.11.1.5 Рекламные программы

Под рекламной программой понимается программное обеспечение, существующее за счет рекламы. Программы, демонстрирующие пользователю рекламные материалы, относятся к этой категории. Рекламные приложения часто автоматически открывают всплывающие окна с рекламой в веб-браузере или изменяют домашнюю страницу. Рекламные программы часто распространяются в комплекте с бесплатными программами. Это позволяет их создателям покрывать расходы на разработку полезных (как правило) программ.

Сами по себе рекламные программы не опасны, но они раздражают пользователей. Опасность заключается в том, что в рекламных программах могут быть реализованы дополнительные функции слежения, подобно шпионским программам.

Если пользователь решает использовать бесплатный программный продукт, ему стоить уделить особое внимание установке программы. Чаще всего программа установки предупреждает об установке дополнительной рекламной программы. Зачастую пользователь имеет возможность отказаться от его установки и установить необходимую программу без рекламной.

Некоторые программы нельзя установить без рекламных модулей либо их функциональность будет ограничена. Это приводит к тому, что рекламная программа часто получает доступ к системе на «законных» основаниях, так как пользователь дал согласие на ее установку. В этом случае лучше перестраховаться. В случае обнаружения на компьютере файла, классифицированного как рекламная программа, рекомендуется удалить его, так как он с большой вероятностью содержит злонамеренный код.

3.11.1.6 Шпионские программы

К этой категории относятся все приложения, которые отправляют личную информацию без ведома и согласия владельца. Шпионские программы используют функции слежения для отправки различной статистической информации, такой как список посещенных веб-сайтов, адреса электронной почты из адресных книг пользователя или набираемый на клавиатуре текст.

Авторы шпионских программ утверждают, что эти технологии служат для изучения требований и интересов пользователей и позволяют создавать рекламные материалы, более соответствующие целевой аудитории. Проблема заключается в том, что нет четкой границы между полезными и вредоносными приложениями, и никто не гарантирует, что получаемая информация не будет использована во вред. Данные, полученные шпионскими программами, могут содержать защитные коды, PIN-коды, номера счетов и т. д. Шпионские программы часто поставляются в комплекте с бесплатными версиями программ самими их авторами с целью получения доходов или стимулирования продаж программного обеспечения. Часто пользователей информируют о наличии шпионских программ во время установки основной программы, чтобы поощрить их к приобретению платной версии.

Примерами хорошо известного бесплатного программного обеспечения, вместе с которым поставляется шпионское, могут служить клиенты пиринговых (P2P) сетей. Программы Spyfalcon и Spy Sheriff (и многие другие) относятся к особой подкатегории шпионских программ. Утверждается, что они предназначены для защиты от шпионских программ, но на самом деле они сами являются таковыми.

В случае обнаружения на компьютере файла, классифицированного как шпионская программа, рекомендуется удалить его, так как с высокой вероятностью он содержит злонамеренный код.

3.11.1.7 Упаковщики

Упаковщик — это самораспаковывающийся исполняемый файл, в котором содержится несколько видов вредоносных программ.

Наиболее распространенными упаковщиками являются UPX, PE_Compact, PKLite и ASPack. Одни и те же вредоносные программы могут быть обнаружены разными способами, если их сжатие выполнено при помощи разных упаковщиков. Кроме того, упаковщики обладают свойством, благодаря которому их сигнатуры со временем изменяются, что усложняет задачу обнаружения и удаления вредоносных программ.

3.11.1.8 Потенциально опасные приложения

Существует множество нормальных программ, предназначенных для упрощения администрирования подключенных к сети компьютеров. Однако злоумышленники могут использовать их для причинения вреда. Программное обеспечение ESET Endpoint Antivirus позволяет обнаруживать такие угрозы.

В качестве **потенциально опасных приложений** выступает нормальное коммерческое программное обеспечение. В эту категорию входят такие программы, как средства удаленного доступа, приложения для взлома паролей и клавиатурные шпионы (программы, записывающие нажатия клавиш на клавиатуре).

Если потенциально опасное приложение обнаружено и работает на компьютере (но пользователь не устанавливал его), следует обратиться к администратору сети или удалить приложение.

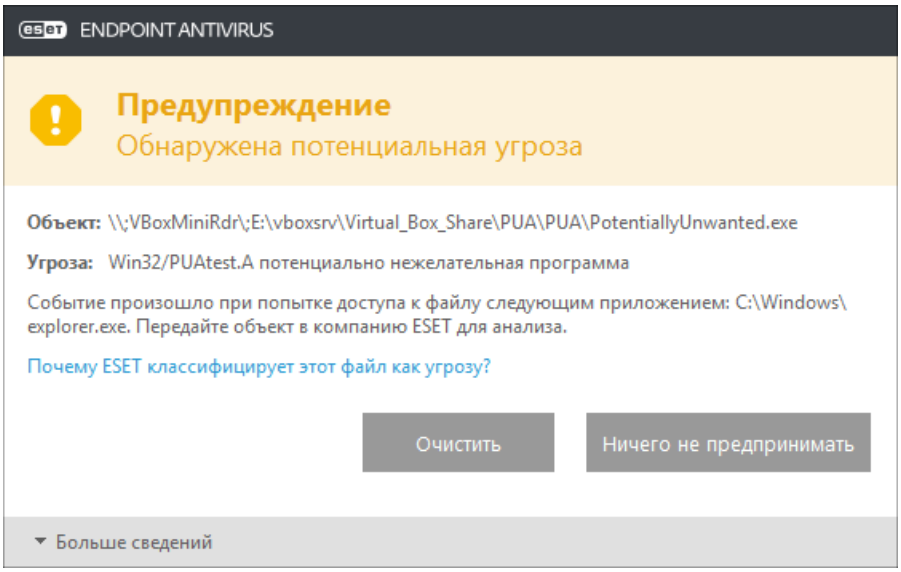
3.11.1.9 Потенциально нежелательные приложения

Потенциально нежелательное приложение содержит рекламу, устанавливает панели инструментов или выполняет другие неясные функции. В некоторых ситуациях может показаться, что преимущества такого приложения перевешивают риски. Поэтому компания ESET помещает эти приложения в категорию незначительного риска, в отличие от других вредоносных программ, например троянских программ или червей.

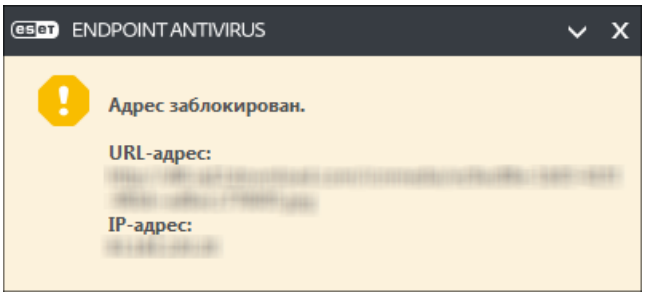
Предупреждение — обнаружена потенциальная угроза

Когда обнаруживается потенциально нежелательное приложение, вы можете самостоятельно решить, какое действие нужно выполнить.

1. **Очистить/отключить**: действие прекращается, и потенциальная угроза не попадает в систему.
2. **Ничего не предпринимать**: эта функция позволяет потенциальной угрозе проникнуть на компьютер.
3. Чтобы разрешить приложению и впредь работать на компьютере без прерываний, щелкните элемент **Дополнительные сведения/показать параметры** и установите флажок **Исключить из проверки**.

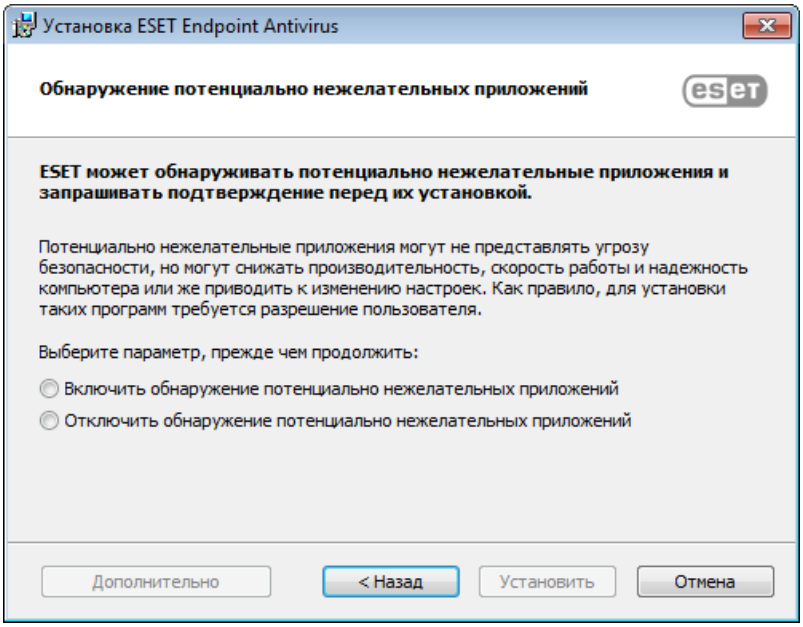


Если обнаружено потенциально нежелательное приложение и его невозможно очистить, в правом нижнем углу экрана отобразится окно уведомлений **Адрес заблокирован**. Дополнительные сведения об этом событии можно получить, последовательно щелкнув в главном меню элементы **Сервис** > **Файлы журнала** > **Отфильтрованные веб-сайты**.



Потенциально нежелательные приложения — параметры

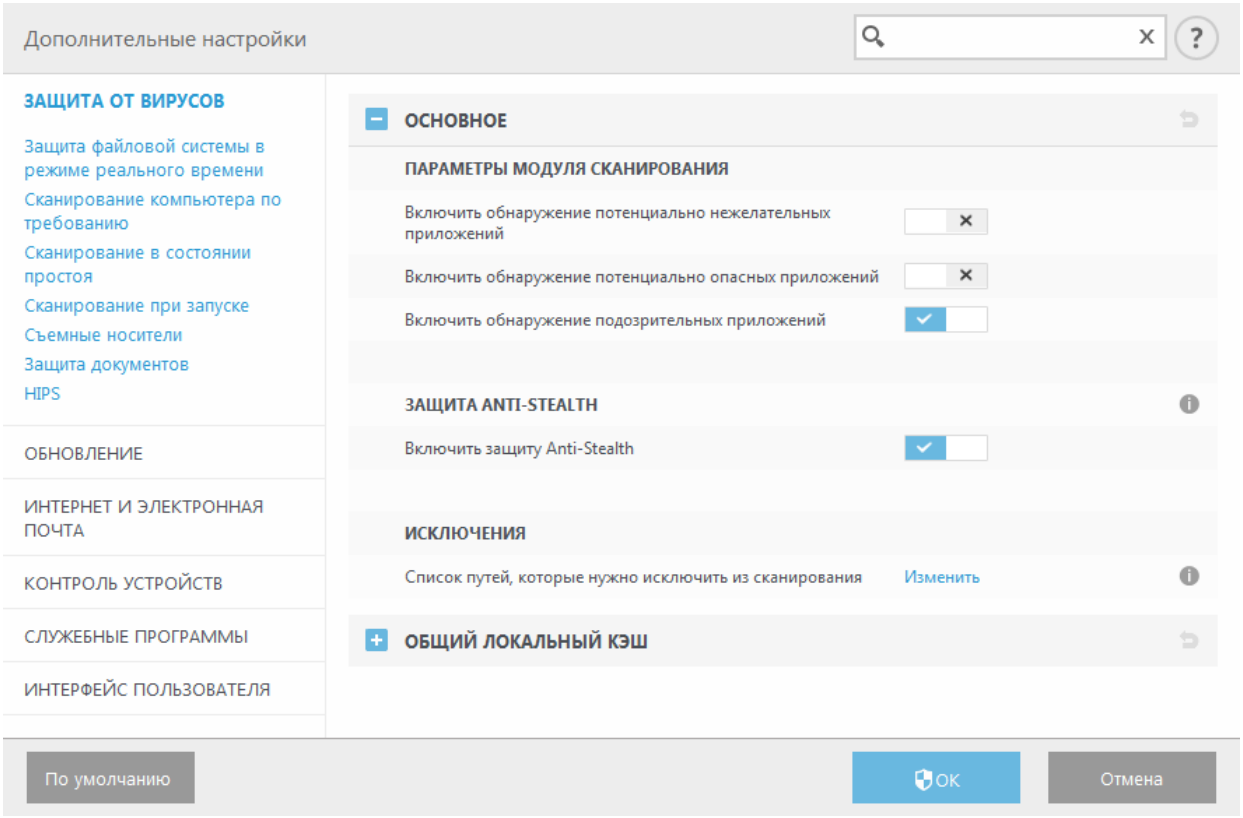
При установке программы ESET можно включить обнаружение потенциально нежелательных приложений (см. изображение ниже).



ВНИМАНИЕ!
Потенциально нежелательные приложения могут устанавливать рекламные программы и панели инструментов или содержать рекламу и другие нежелательные и небезопасные программные компоненты.

Эти параметры можно в любое время изменить в разделе параметров программы. Чтобы включить или отключить обнаружение потенциально нежелательных, небезопасных или подозрительных приложений, следуйте нижеприведенным инструкциям.

1. Откройте программу ESET. Как открыть мой продукт ESET?
2. Нажмите клавишу **F5**, чтобы перейти к разделу **Дополнительные настройки**.
3. Щелкните элемент **Антивирус** и на свое усмотрение включите или отключите параметры **Включить обнаружение потенциально нежелательных приложений**, **Включить обнаружение потенциально опасных приложений** и **Включить обнаружение подозрительных приложений**. Чтобы сохранить настройки, нажмите кнопку **ОК**.



Потенциально нежелательные приложения — оболочки

Оболочка — специальное приложение, используемое на некоторых файлообменных ресурсах. Это стороннее средство, устанавливающее программу, которую нужно загрузить, в комплекте с другим программным обеспечением, например панелью инструментов или рекламой, которые изменяют домашнюю страницу браузера или параметры поиска. При этом файлообменные ресурсы часто не уведомляют производителя программного обеспечения или пользователей о внесенных изменениях, а отказаться от этих изменений непросто. Именно поэтому компания ESET считает оболочки потенциально нежелательными приложениями и дает пользователям возможность отказаться от их загрузки.

Обновленную версию этой страницы справочной системы см. в этой статье базы знаний ESET.

3.11.2 Электронная почта

Электронная почта является современным средством общения, которое применяется во многих областях. Она отличается гибкостью, высокой скоростью и отсутствием посредников и сыграла ключевую роль в распространении Интернета в начале 90-х годов прошлого века.

К сожалению, вследствие высокого уровня анонимности электронная почта и Интернет оставляют пространство для незаконных действий, таких как рассылка спама. К спаму относятся нежелательные рекламные объявления, мистификации и сообщения, предназначенные для распространения вредоносных программ. Доставляемые пользователю неудобства и опасность увеличиваются из-за того, что стоимость рассылки минимальна, а в распоряжении авторов спама есть множество средств для получения новых адресов электронной почты. Кроме того, количество и разнообразие спама сильно затрудняют контроль над ним. Чем дольше используется адрес электронной почты, тем выше вероятность того, что он попадет в базы данных, используемые для рассылки спама. Вот некоторые советы, помогающие избежать этого.

- По возможности не размещайте свой адрес электронной почты в Интернете.
- Давайте свой адрес только тем, кому полностью доверяете.
- Если возможно, не используйте распространенные слова в качестве псевдонимов (чем сложнее псевдоним, тем труднее отследить адрес).
- Не отвечайте на полученный спам.
- Будьте осторожны при заполнении форм на веб-сайтах (особенно если они содержат пункты типа «Да, я хочу получать информацию»).
- Используйте «специализированные» адреса электронной почты (например, заведите один адрес для работы, другой для общения с друзьями и т. д.).
- Время от времени меняйте адрес электронной почты.
- Используйте какое-либо решение для защиты от спама.

3.11.2.1 Рекламные объявления

Реклама в Интернете является одним из наиболее бурно развивающихся видов рекламы. Ее преимуществами являются минимальные затраты и высокая вероятность непосредственного общения с потребителем. Кроме того, сообщения доставляются практически мгновенно. Многие компании используют электронную почту в качестве маркетингового инструмента для эффективного общения с существующими и потенциальными клиентами.

Этот вид рекламы является нормальным, так как потребители могут быть заинтересованы в получении коммерческой информации о некоторых товарах. Однако многие компании занимаются массовыми рассылками нежелательных коммерческих сообщений. В таких случаях реклама по электронной почте выходит за границы допустимого, и эти сообщения классифицируются как спам.

Количество нежелательных сообщений уже стало проблемой, и при этом никаких признаков его сокращения не наблюдается. Авторы нежелательных сообщений часто пытаются выдать спам за нормальные сообщения.

3.11.2.2 Мистификации

Мистификацией называется ложная информация, распространяющаяся через Интернет. Обычно мистификации рассылаются по электронной почте или с помощью таких средств общения, как ICQ и Skype. Собственно сообщение часто представляет собой шутку или городскую легенду.

Связанные с компьютерными вирусами мистификации направлены на то, чтобы вызвать в получателях страх, неуверенность и мнительность, побуждая их верить в то, что «не поддающийся обнаружению вирус» удаляет их файлы, крадет пароли или выполняет какие-либо другие крайне нежелательные действия с компьютерами.

Некоторые мистификации работают, предлагая получателям переслать сообщение своим знакомым, за счет чего увеличивается масштаб мистификации. Существуют мистификации, которые передаются через мобильные телефоны, мистификации, представляющие собой просьбы о помощи, предложения получить деньги из-за границы, и прочие. Часто бывает невозможно понять мотивацию создателя мистификации.

Если сообщение содержит просьбу переслать его всем знакомым, это сообщение с большой вероятностью является мистификацией. Существует большое количество веб-сайтов, которые могут проверить, является ли

сообщение нормальным. Прежде чем пересылать сообщение, которое кажется вам мистификацией, попробуйте найти в Интернете информацию о нем.

3.11.2.3 Фишинг

Термин «фишинг» обозначает преступную деятельность, в рамках которой используются методы социальной инженерии (манипулирование пользователем, направленное на получение конфиденциальной информации). Целью фишинга является получение доступа к таким конфиденциальным данным, как номера банковских счетов, PIN-коды и т. п.

Попытка получения информации обычно представляет собой отправку сообщения якобы от доверенного лица или компании (например, финансового учреждения или страховой компании). Сообщение может казаться благонадежным и содержать изображения и текст, которые могли изначально быть получены от источника, якобы являющегося отправителем данного сообщения. Под разными предлогами (проверка данных, финансовые операции) предлагается предоставить какую-либо личную информацию, такую как номера банковских счетов, имена пользователя, пароли и т. д. Если такие данные предоставляются, они легко могут быть украдены и использованы в преступных целях.

Банки, страховые компании и другие легитимные организации никогда не запрашивают имена пользователей и пароли в незапрошенных сообщениях электронной почты.

3.11.2.4 Распознавание мошеннических сообщений

Вообще существует несколько признаков, которые могут помочь распознать спам (нежелательные сообщения) в почтовом ящике. Если сообщение соответствует хотя бы нескольким из этих критериев, оно, наиболее вероятно, является нежелательным.

- Адрес отправителя отсутствует в адресной книге получателя.
- Предлагается получить большую сумму денег, но сначала нужно оплатить небольшую сумму.
- Под разными предлогами (проверка данных, финансовые операции) предлагается предоставить какие-либо личные данные, такие как номера банковских счетов, имя пользователя, пароль и т. д.
- Сообщение написано на иностранном языке.
- Предлагается покупка продукции, в которой получатель не заинтересован. Однако если получателя заинтересовало предложение, следует проверить, является ли отправитель надежным поставщиком (например, проконсультироваться с представителем производителя продукции).
- Некоторые из слов намеренно написаны с ошибками, чтобы обмануть фильтр спама. Например, «веагро» вместо «виагра» и т. п.

3.11.3 Технологии ESET

3.11.3.1 Блокировщик эксплойтов

Блокировщик эксплойтов предназначен для защиты приложений, которые обычно уязвимы для эксплойтов, например браузеров, программ для чтения PDF-файлов, почтовых клиентов и компонентов MS Office. Он осуществляет мониторинг работы процессов для выявления подозрительных действий, которые могли бы означать использование эксплойта. Он добавляет еще один слой защиты между вами и злоумышленниками, используя технологию, которая полностью отличается от техник, ориентированных на выявление вредоносных программ.

Когда блокировщик эксплойтов обнаруживает подозрительный процесс, он может сразу же остановить его работу и записать данные об угрозе, которые затем отправляются в облачную систему ESET Live Grid. Эти данные затем обрабатываются в лаборатории ESET по изучению угроз и используются для улучшения защиты всех пользователей от неизвестных угроз и атак «нулевого дня» (новые вредоносные программы, для которых еще нет предварительно настроенных средств защиты).

3.11.3.2 Расширенный модуль сканирования памяти

Расширенный модуль сканирования памяти работает в сочетании с Блокировщиком эксплойтов для усиления защиты от вредоносных программ, которые могут избегать обнаружения обычными продуктами для защиты от вредоносных программ за счет использования умышленного запутывания и/или шифрования. В случаях, когда угроза может быть не обнаружена с помощью обычной эмуляции или эвристики, расширенный модуль сканирования памяти может определять подозрительные действия и сканировать угрозы, когда они появляются в системной памяти. Это решение эффективно даже против вредоносных программ с высокой степенью умышленного запутывания. В отличие от блокировщика эксплойтов это метод, применяемый после выполнения, поэтому существует риск того, что некоторые вредоносные действия могли быть выполнены до обнаружения угрозы. Однако если применение других методов обнаружения не дало результатов, такое решение обеспечивает дополнительный уровень безопасности.

3.11.3.3 ESET Live Grid

Сеть ESET Live Grid, основанная на передовой системе раннего обнаружения ThreatSense.Net®, использует данные от пользователей ESET со всего мира и отправляет их в вирусную лабораторию ESET. Сеть ESET Live Grid позволяет получать подозрительные образцы и метаданные в реальных условиях, поэтому мы можем незамедлительно реагировать на потребности пользователей и обеспечить готовность ESET к обезвреживанию новейших угроз. Исследователи вредоносных программ ESET используют эту информацию для получения точного представления о природе и масштабах глобальных угроз, что позволяет нам направлять усилия на решение правильных задач. Данные системы ESET Live Grid играют важную роль при определении приоритетов в наших автоматизированных системах.

Кроме того, применяется система репутации, помогающая улучшить общую эффективность наших решений по борьбе с вредоносными программами. Когда исполняемый файл или архив проверяется на компьютере пользователя, его хэш-тег сначала проверяется по базе элементов, внесенных в «белые» и «черные» списки. Если он находится в «белом» списке, проверяемый файл считается чистым и помечается для исключения из будущих сканирований. Если он находится в «черном» списке, предпринимаются соответствующие действия, исходя из природы угрозы. Если соответствие не найдено, файл тщательно сканируется. На основании результатов сканирования происходит категоризация файлов как угроз или чистых файлов. Такой подход имеет существенное положительное влияние на производительность сканирования.

Система репутации обеспечивает эффективное обнаружение образцов вредоносных программ еще до доставки их сигнатур в обновленную базу данных сигнатур вирусов на компьютере пользователя (что происходит несколько раз в день).

3.11.3.4 Блокировщик эксплойтов Java

Блокировщик эксплойтов Java — это расширение для существующего блокировщика эксплойтов ESET. Он осуществляет мониторинг Java на предмет поведения, которое напоминает поведение эксплойтов. Заблокированные образцы можно передавать аналитикам вредоносных программ, чтобы они могли создавать сигнатуры для блокировки таких программ на разных уровнях (блокировка URL-адресов, загрузка файлов и т. п.).