ESET **SMART SECURITY 10**

Руководство пользователя

(для версии 10.0 и более поздних версий продукта)

Microsoft® Windows® 10 / 8.1 / 8 / 7 / Vista

Щелкните здесь, чтобы загрузить последнюю версию этого документа.

ENJOY SAFER TECHNOLOGY™

ESET SMART SECURITY

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

Версия от 24.10.2016

Содержание

Содержание

1. ESET Smart Security

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

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

Возможности и преимущества

Улучшенный интерфейс	Пользовательский интерфейс версии 10 значительно улучшен и упрощен с учетом результатов тестирования на предмет удобства использования. Все формулировки и уведомления, присутствующие в графическом интерфейсе пользователя, были тщательно проанализированы, и теперь интерфейс поддерживает языки с написанием справа налево, например иврит и арабский. **Интернет-справка** теперь интегрирована в ESET Smart Security и содержит динамически обновляемые статьи по поддержке.
Защита от вирусов и шпионских программ	Упреждающее обнаружение и очистка большего количества известных и неизвестных вирусов, червей, троянских программ и руткитов. Метод **расширенной эвристики** идентифицирует даже раннее неизвестные вредоносные программы, обеспечивая защиту вашего компьютера от неизвестных угроз и нейтрализуя их до того, как они могут причинить какой-либо вред. Функции **защиты доступа в Интернет** и **защиты от фишинга** работают путем отслеживания обмена данными между веб-браузерами и удаленными серверами (в том числе SSL). Функция **защиты почтового клиента** обеспечивает контроль обмена сообщениями через протоколы POP3(S) и IMAP(S).
Регулярные обновления	Регулярное обновление базы данных сигнатур вирусов и программных модулей — наилучший способ обеспечить максимальный уровень безопасности компьютера.
ESET LiveGrid® (репутация на основе облака)	Вы можете проверить репутацию запущенных процессов и файлов непосредственно с помощью ESET Smart Security.
Контроль устройств	Автоматически сканирует все USB-устройства флэш-памяти, карты памяти, а также компакт- и DVD-диски. Блокирует съемные носители на основании типа носителя, производителя, размера и других характеристик.
Функция HIPS	Вы можете более детально настроить поведение системы, задать правила для системного реестра, активных процессов и программ, а также точно настроить проверку состояния безопасности.
Игровой режим	Откладывает все всплывающие окна, обновления или другие действия, требующие большой нагрузки на систему, чтобы обеспечить экономию системных ресурсов для игр или других полноэкранных процессов.

Возможности ESET Smart Security

Защита банковской оплаты	Функция защиты банковских платежей обеспечивает защиту браузера при использовании шлюзов интернет-банкинга или платежей в

	Интернете, чтобы все финансовые операции в Интернете осуществлялись в заслуживающей доверия и безопасной среде.
Поддержка сетевых подписей	Сетевые подписи обеспечивают быструю идентификацию и блокируют на устройствах пользователя вредоносный входящий и исходящий трафик, имеющий отношение к ботам и пакетным средствам эксплуатации уязвимостей. Эту функцию можно считать улучшением в области защиты от ботнетов.
Интеллектуальный файервол	Предотвращает несанкционированный доступ к вашему компьютеру и использование ваших личных данных пользователями, не имеющими соответствующего разрешения.
Защита от спама ESET	Доля спама в общем объеме передаваемых по электронной почте сообщений составляет около 80 %. Защита от спама ограждает от этой проблемы.
ESET Антивор	ESET Антивор повышает уровень безопасности пользовательской информации на случай потери или кражи компьютера. После установки пользователем программы ESET Smart Security и модуля ESET Антивор соответствующее устройство будет отображаться в веб-интерфейсе. С помощью веб-интерфейса пользователи могут управлять конфигурацией модуля ESET Антивор и администрировать параметры функции «Антивор» на своих устройствах.
Родительский контроль	Обеспечивает защиту семьи от потенциально нежелательного веб-содержимого, блокируя веб-сайты различных категорий.

Для работы функций ESET Smart Security необходимо иметь активную лицензию. Рекомендуется продлевать лицензию ESET Smart Security за несколько недель до истечения срока ее действия.

1.1 Новые возможности в версии 10

ESET Smart Security версии 10 включает в себя следующие усовершенствования:

- **Защита домашней сети**: защита ваших компьютеров от входящих сетевых угроз.
- **Защита веб-камеры**: контроль процессов и приложений, осуществляющих доступ к подключенной к компьютеру камере.
- **Защита от атак на основе сценариев**: упреждающая защита от динамических атак на основе сценариев и необычных векторов атаки.
- **Высокая производительность и незначительное влияние на систему**: версия 10 обеспечивает защиту от новых типов угроз и при этом максимально эффективно использует системные ресурсов, позволяя вам наслаждаться производительностью своего компьютера.
- **Совместимость с Windows 10**: ESET полностью поддерживает ОС Microsoft Windows 10.

Для получения дополнительной информации о новых функциях ESET Smart Security, прочитайте статью базы знаний ESET:
Новые возможности продукта Home версии 10

1.2 Какой у меня продукт

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

- **ESET NOD 32 Antivirus;**
- **ESET Internet Security;**
- **ESET Smart Security;**
- **ESET Smart Security Premium.**

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

В приведенной ниже таблице описаны функции каждого из продуктов.

	ESET NOD 32 Antivirus	ESET Internet Security	ESET Smart Security	ESET Smart Security Premium
Защита от вирусов	✔	✔	✔	✔
Защита от шпионских программ	✔	✔	✔	✔
Блокировщик эксплойтов	✔	✔	✔	✔
Защита от атак на основе сценариев	✔	✔	✔	✔
Защита от фишинга	✔	✔	✔	✔
Защита от спама		✔	✔	✔
Персональный файервол		✔	✔	✔
Защита домашней сети		✔	✔	✔
Защита веб-камеры		✔	✔	✔
Защита от сетевых атак		✔	✔	✔
Защита от ботнетов		✔	✔	✔
Защита банковской оплаты		✔	✔	✔
Родительский контроль		✔	✔	✔
Антивор			✔	✔
ESET Password Manager				✔
ESET Secure Data				✔

1.3 Системные требования

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

Поддерживаемые процессоры:

Intel® или AMD x86–x64

Поддерживаемые операционные системы:

Microsoft® Windows® 10;
Microsoft® Windows® 8.1;
Microsoft® Windows® 8;
Microsoft® Windows® 7;
Microsoft® Windows® Vista;
Microsoft® Windows® Home Server 2011, 64-разрядная версия.

ПРИМЕЧАНИЕ.
ESET Антивор Не поддерживается в операционных системах Microsoft Windows Home Server.

1.4 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 своевременного обнаружения ThreatSense, тысячи новых уникальных заражений появляются ежедневно. Они пытаются обойти существующие меры безопасности и приносят доход их авторам за счет убытков других пользователей. Специалисты исследовательской лаборатории ESET ежедневно анализируют такие угрозы, подготавливают и выпускают обновления для непрерывного повышения уровня защиты пользователей. Для максимальной эффективности этих обновлений важно настроить их надлежащим образом на компьютере пользователя. Дополнительные сведения о настройке обновлений см. в главе Настройка обновлений.

Загружайте пакеты обновлений операционной системы и других программ

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

Резервное копирование важных данных

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. Рекомендуем 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. Установка

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

- Интерактивный установщик можно загрузить с веб-сайта ESET. Пакет установки подходит для всех языков (выберите свой язык). Сам интерактивный установщик представляет собой файл небольшого размера; другие необходимые для установки ESET Smart Security файлы загружаются автоматически.

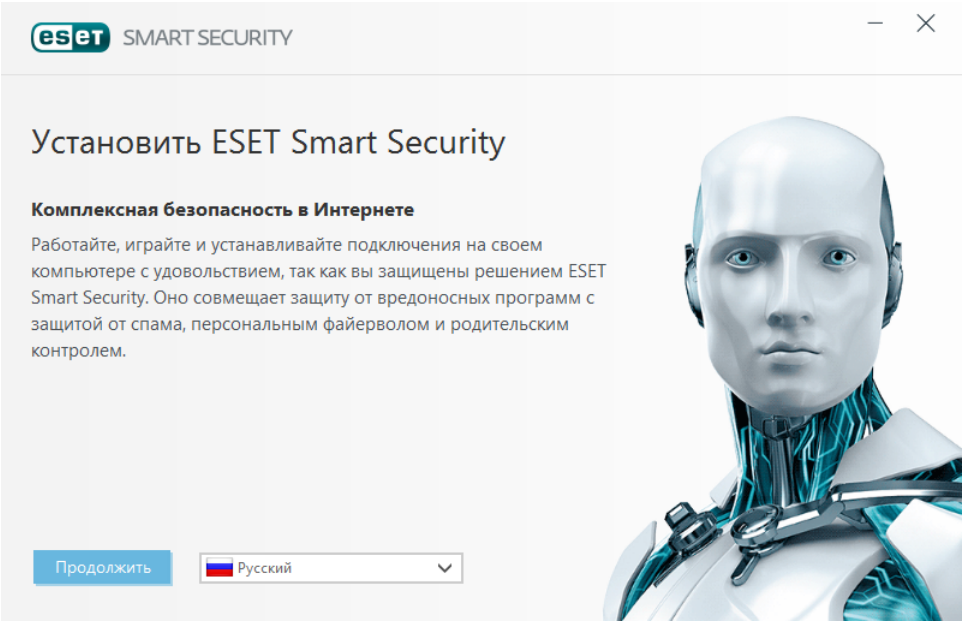
- Автономная установка: данный тип установки используется при установке программы с компакт-/DVD-диска. В рамках этого типа установки используется файл формата *EXE*, размер которого превышает размер файла интерактивного установщика, и не требуется подключение к Интернету или дополнительные файлы для завершения установки.

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

2.1 Интерактивный установщик

После загрузки пакета установки *интерактивного установщика* дважды щелкните файл установки и следуйте пошаговым инструкциям в окне установщика.

ВАЖНО!
Для использования этого типа установки необходимо подключение к Интернету.



Выберите нужный язык в раскрывающемся списке и нажмите кнопку **Продолжить**. Подождите некоторое время, пока не будут загружены установочные файлы.

После принятия **лицензионного соглашения** отобразится запрос относительно настройки **ESET LiveGrid®**. ESET LiveGrid® помогает обеспечить незамедлительное и непрерывное информирование ESET о появлении новых угроз, чтобы защитить пользователей. С помощью этой системы вы можете отправлять новые угрозы в исследовательскую лабораторию ESET, где они анализируются, обрабатываются и добавляются в базу данных сигнатур вирусов.

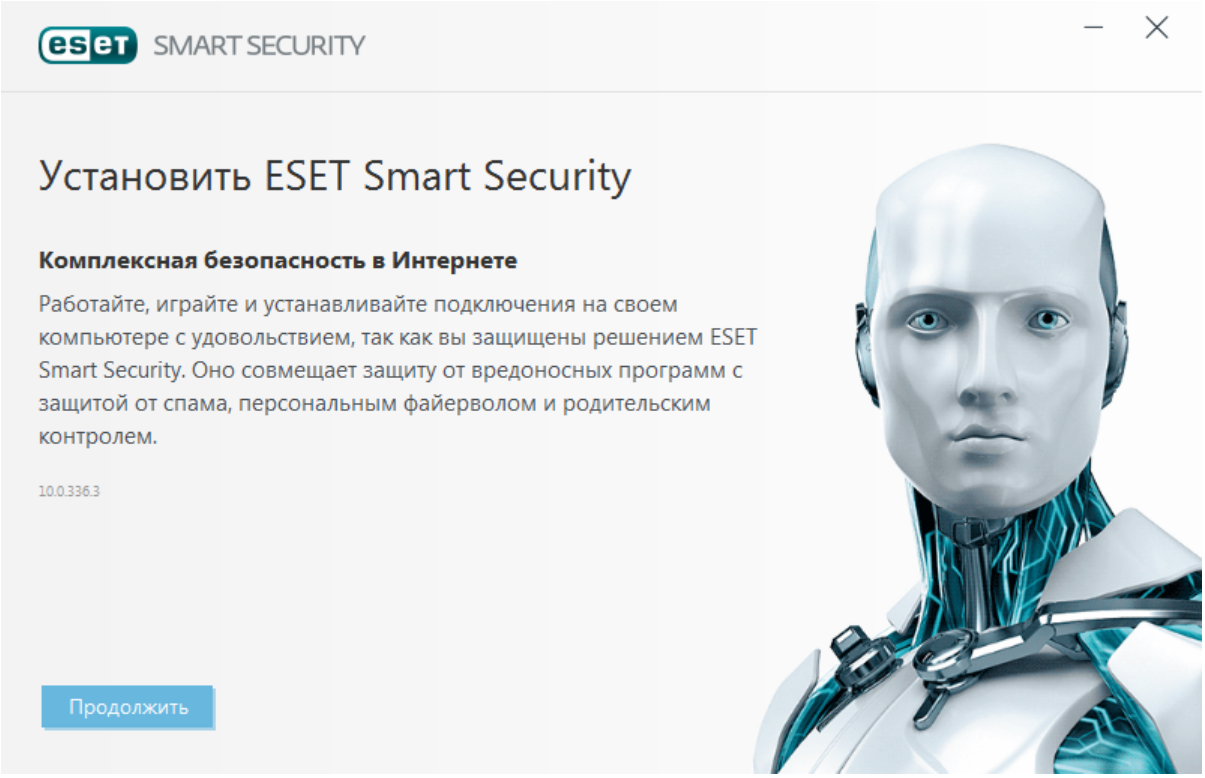
По умолчанию выбран вариант **Включить систему отзывов ESET LiveGrid® (рекомендуется)**, что приводит к активации данной функции.

Следующим действием при установке является настройка обнаружения потенциально нежелательных приложений. Потенциально нежелательные приложения не обязательно являются вредоносными, но могут негативно влиять на работу операционной системы. Дополнительные сведения см. в главе Потенциально нежелательные приложения.

Чтобы запустить процесс установки, нажмите кнопку **Установить**.

2.2 Автономная установка

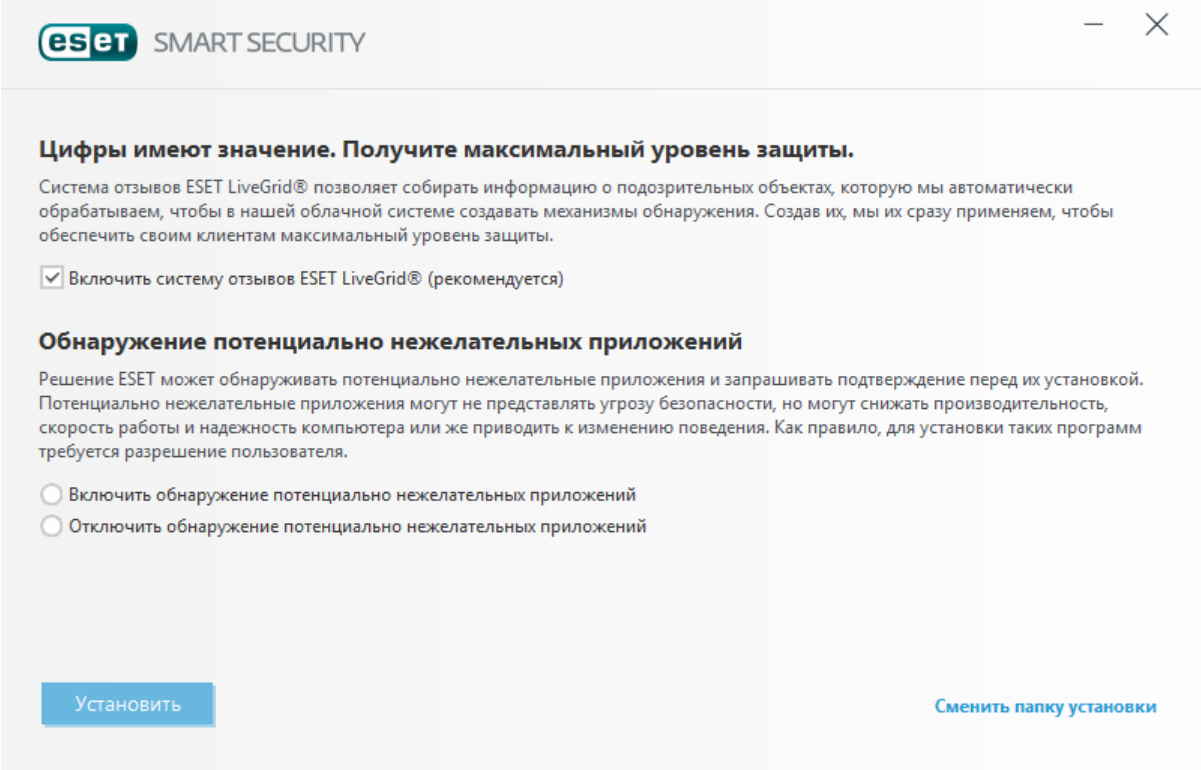
Когда вы инициируете автономную установку (запустите EXE-файл), мастер установки поможет установить программу.



Сначала программа проверяет наличие более новой версии ESET Smart Security. При обнаружении более новой версии вы будете уведомлены об этом на первом этапе установки. Если выбрать команду **Загрузить и установить новую версию**, будет загружена новая версия, после чего установка будет продолжена. Этот флажок отображается, если доступна более новая версия программы, чем та, которая устанавливается.

На следующем этапе на экран будет выведено лицензионное соглашение с конечным пользователем. Прочтите его и нажмите кнопку **Принять**, чтобы подтвердить свое согласие с условиями лицензионного соглашения с конечным пользователем. После принятия установка продолжится.

Дополнительные указания по поводу этапов установки, **ESET LiveGrid®** и **обнаружения потенциально нежелательных приложений** приведены в упомянутом выше разделе (см. раздел Интерактивный установщик).



2.2.1 Дополнительно

После выбора варианта **Сменить папку установки** необходимо выбрать папку для установки. По умолчанию программа устанавливается в указанную ниже папку.

C:\Program Files\ESET\ESET Smart Security

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

Для выполнения следующих этапов установки (**ESET LiveGrid®** и **Обнаружение потенциально нежелательных приложений**) следуйте инструкциям, которые содержатся в разделе «Интерактивный установщик» (см. раздел Интерактивный установщик).

Щелкните **Продолжить**, а затем — **Установить**, чтобы установить продукт.

2.3 Распространенные проблемы при установке

Если в процессе установки возникают какие-либо проблемы, см. наш список распространенных проблем при установке и их решений, чтобы найти решение для своей проблемы.

2.4 Активация программы

После завершения установки будет предложено активировать программный продукт.

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

- Если вы приобрели коробочную розничную версию программы, активируйте ее, используя **Лицензионный ключ**. Лицензионный ключ, как правило, расположен внутри упаковки продукта или на ее тыльной стороне. Для успешного выполнения активации лицензионный ключ необходимо ввести в том виде, в котором он предоставлен. Лицензионный ключ — это уникальная строка в формате XXXX-XXXX-XXXX-XXXX-XXXX или XXXX-XXXXXXXX, которая используется для идентификации владельца и активации лицензии.
- Если вы хотите оценить программу ESET Smart Security, прежде чем покупать ее, выберите вариант **Лицензия на бесплатную пробную версию**. Укажите свои адрес электронной почты и страну, чтобы активировать ESET Smart Security на ограниченный период времени. Тестовая лицензия будет отправлена вам по электронной почте. Каждый пользователь может активировать только одну пробную лицензию.
- Если у вас нет лицензии, но вы хотите купить ее, выберите вариант «Приобрести лицензию». В результате откроется веб-сайт местного распространителя ESET.

2.5 Ввод лицензионного ключа

Автоматические обновления важны для вашей безопасности. ESET Smart Security будет получать обновления после активации с использованием вашего **лицензионного ключа**.

Если не ввести лицензионный ключ после установки, продукт активирован не будет. Сменить лицензию можно в главном окне программы. Для этого щелкните элемент **Справка и поддержка**, затем **Активировать лицензию** и в окне «Активация программы» введите данные лицензии, полученные в комплекте с продуктом ESET.

При вводе **Лицензионного ключа** важно указывать его именно в том виде, в котором он получен.

- Лицензионный ключ — это уникальная строка в формате XXXX-XXXX-XXXX-XXXX-XXXX, которая используется для идентификации владельца и активации лицензии.

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

2.6 Обновление до новой версии

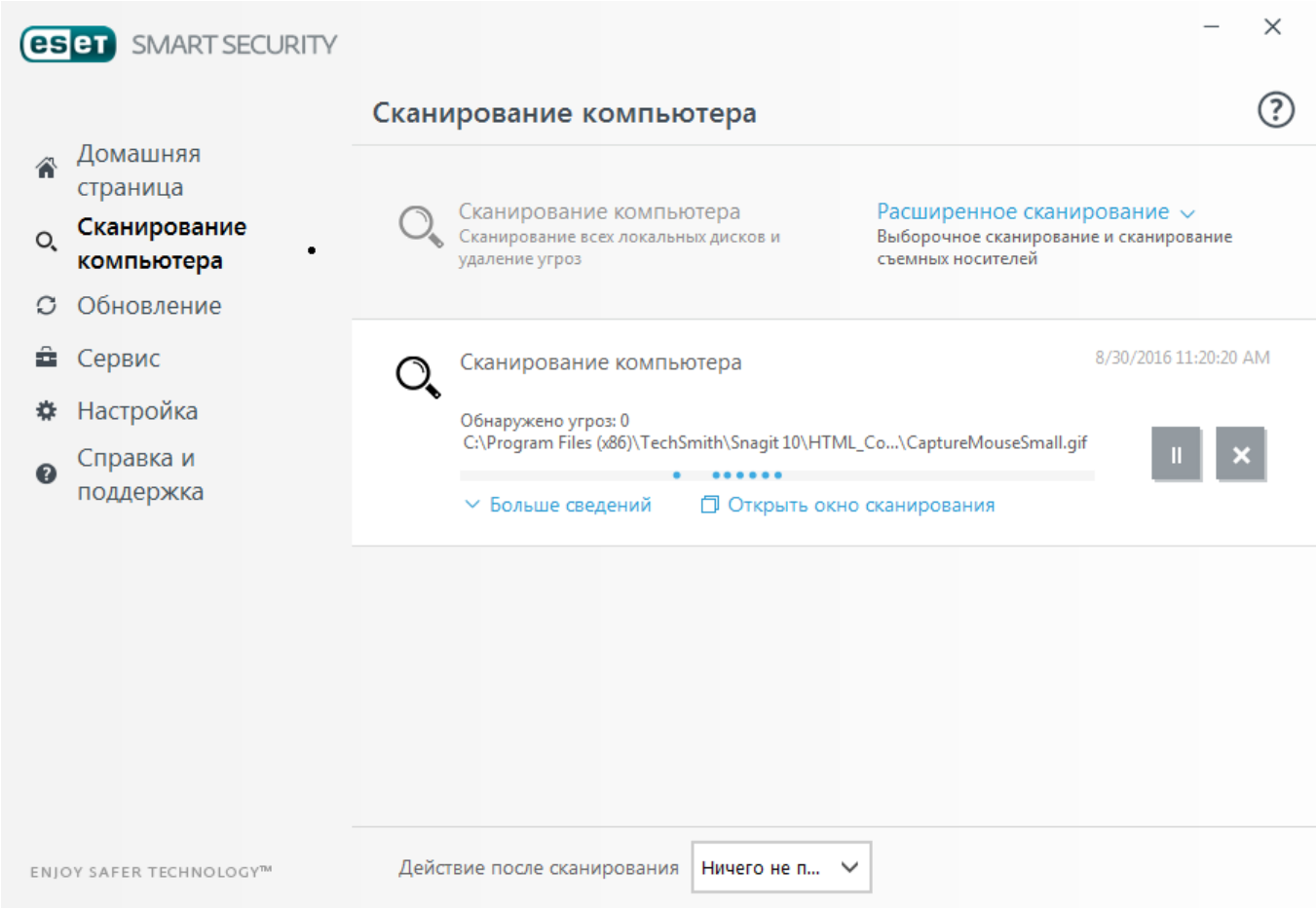
Новые версии ESET Smart Security выпускаются для реализации улучшений или исправления проблем, которые не могут быть устранены автоматическим обновлением модулей программы. Обновление до новой версии можно выполнить одним из нескольких способов.

1. Автоматически путем обновления программы.
   Поскольку обновления программы распространяются среди всех пользователей и могут повлиять на некоторые системные конфигурации, они выпускаются только после длительного тестирования с целью обеспечения бесперебойной работы на всех возможных конфигурациях. Чтобы перейти на новую версию сразу после ее выпуска, воспользуйтесь одним из перечисленных ниже способов.
2. Вручную в главном окне программы путем нажатия кнопки **Проверить наличие обновлений** в разделе **Обновление**.
3. Вручную путем загрузки и установки новой версии поверх предыдущей.

2.7 Первое сканирование после установки

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

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



3. Руководство для начинающих

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

3.1 Главное окно программы

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

Ниже описаны пункты главного меню.

Домашняя страница - этот пункт предоставляет информацию о состоянии защиты ESET Smart Security.

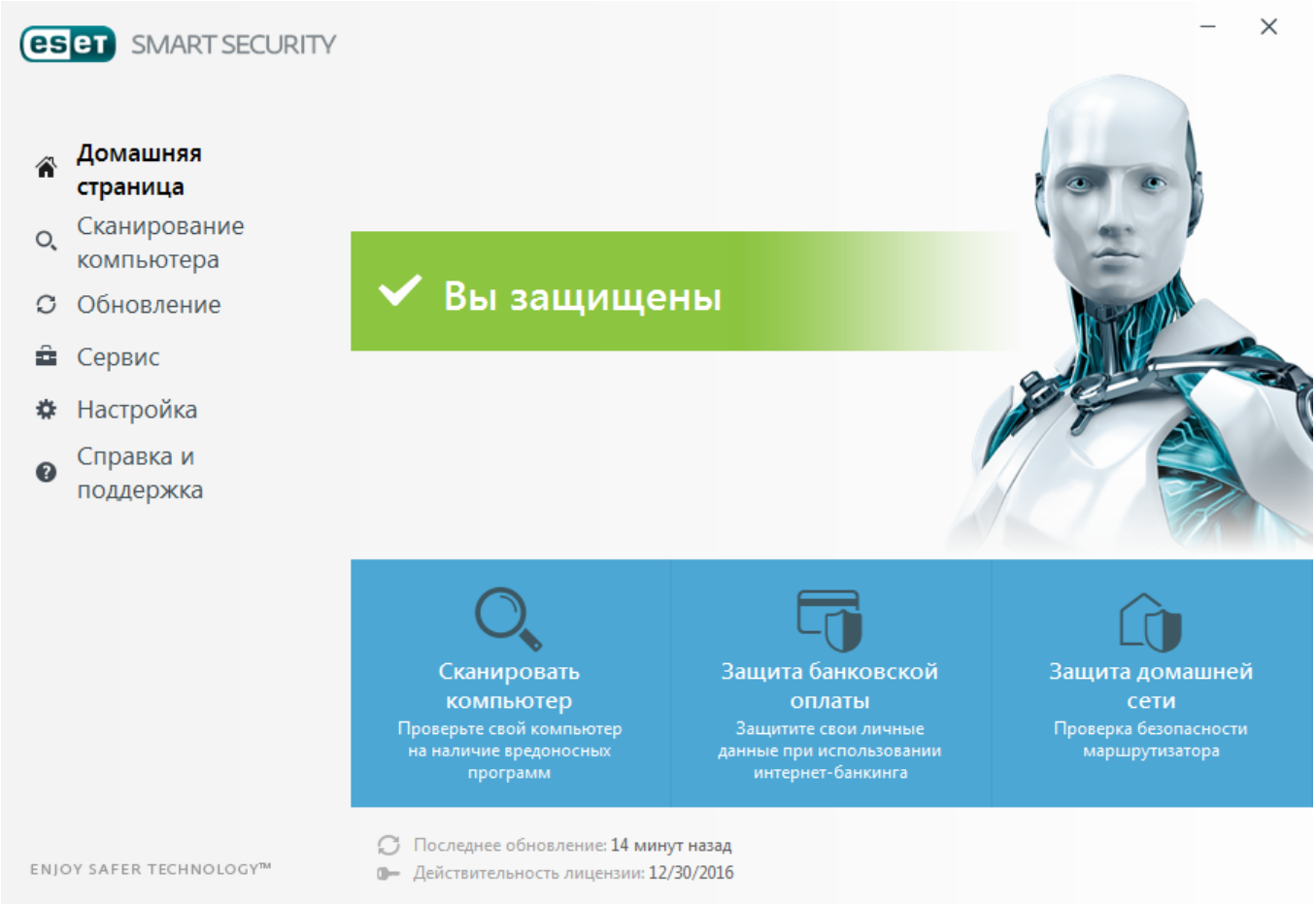
Сканирование компьютера: настройка и запуск сканирования компьютера или создание выборочного сканирования.

Обновление - выводит информацию об обновлениях базы данных сигнатур вирусов.

Сервис - позволяет открыть файлы журнала, статистику защиты, программу мониторинга, запущенные процессы, сетевые подключения, планировщик, ESET SysInspector и ESET SysRescue.

Настройка — с помощью этого параметра можно настроить уровень безопасности для компьютера, Интернета, защиты сети и средств безопасности.

Справка и поддержка — обеспечивает доступ к файлам справки, базе знаний ESET, веб-сайту ESET и ссылкам для отправки запросов в службу поддержки.

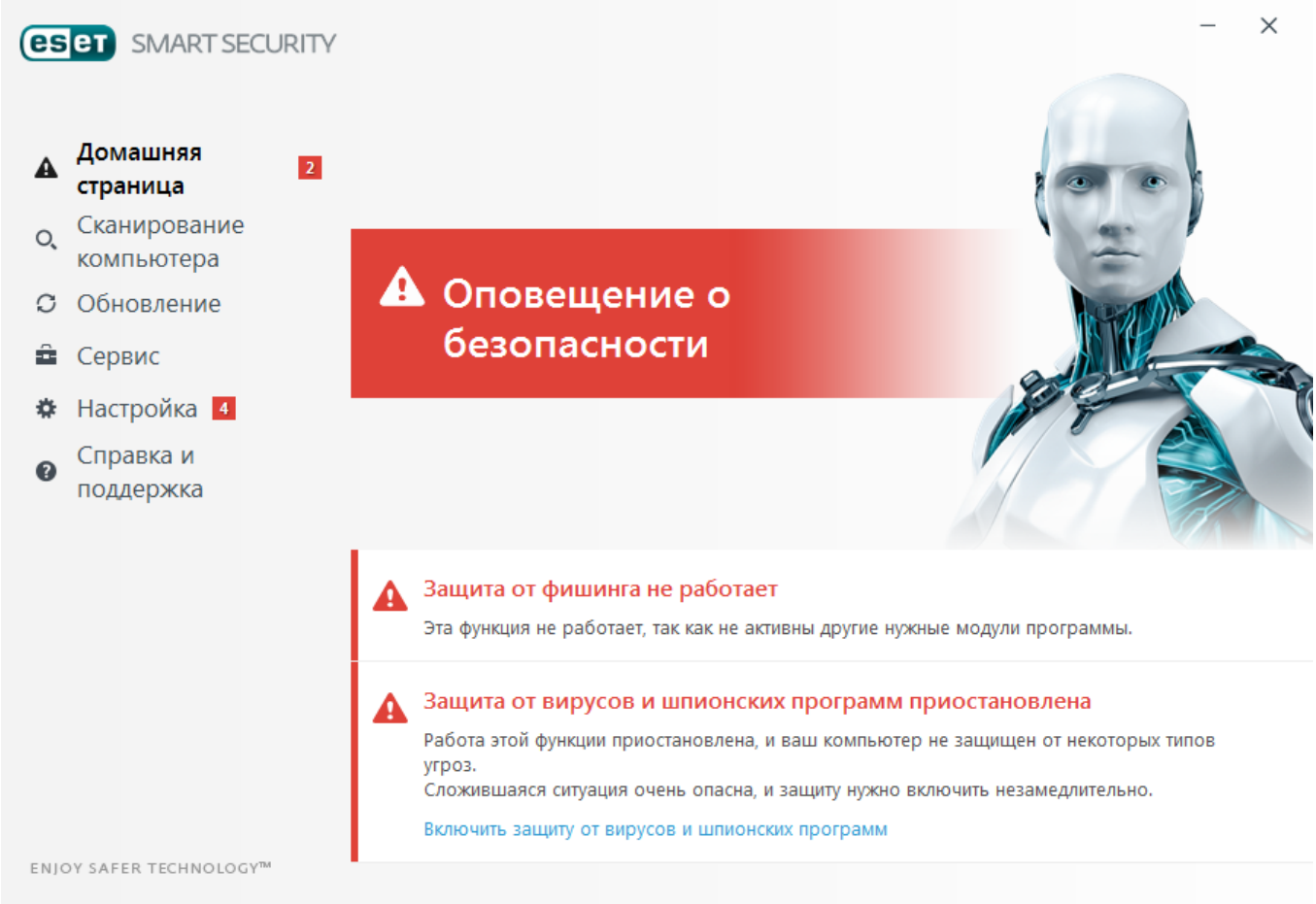


На экране **Домашняя страница** отображаются важные сведения о текущем уровне защиты компьютера. В окне состояния отображаются часто используемые функции ESET Smart Security. Здесь также указаны сведения о последнем обновлении и дата окончания срока действия программы.

Зеленый значок и зеленый статус **Максимальная защита** сообщают о максимальном уровне защиты.

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

Если модуль активной защиты работает правильно, значок состояния защиты будет зеленым. Красный восклицательный знак или оранжевый значок уведомления означает, что максимальная степень защиты не обеспечивается. В **Главном меню** будут отображаться дополнительные сведения о состоянии защиты каждого модуля и предложены решения для восстановления полной защиты. Для изменения состояния отдельного модуля щелкните **Настройка** и выберите необходимый модуль.



Красный значок и красная надпись «Максимальная защита» не обязательно сигнализируют о критических проблемах.
Для отображения такого состояния может быть несколько причин.

- **Программа не активирована**: можно активировать программу ESET Smart Securityна **Домашней странице**, выбрав **Активировать продукт** или **Купить сейчас** возле сведений о состоянии защиты.
- **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 сконфигурированные параметры подключения.
- **Модули защиты от вирусов и шпионских программ отключены**: можно снова включить защиту от вирусов и шпионских программ, щелкнув **Включить защиту от вирусов и шпионских программ**.
- **Персональный файервол ESET отключен**: об этой проблеме сигнализирует уведомление о защите на рабочем столе рядом с элементом **Сеть**. Чтобы повторно включить защиту сети, щелкните элемент **Включить файервол**.
- **Срок действия лицензии истек**: об этом сигнализирует красный значок состояния защиты. С этого момента программа больше не сможет выполнять обновления. Для продления лицензии следуйте инструкциям в окне предупреждения.

Оранжевый цвет значка указывает на то, что действует ограниченная защита. Например, существуют проблемы с обновлением программы или заканчивается срок действия лицензии.
Для отображения такого состояния может быть несколько причин.

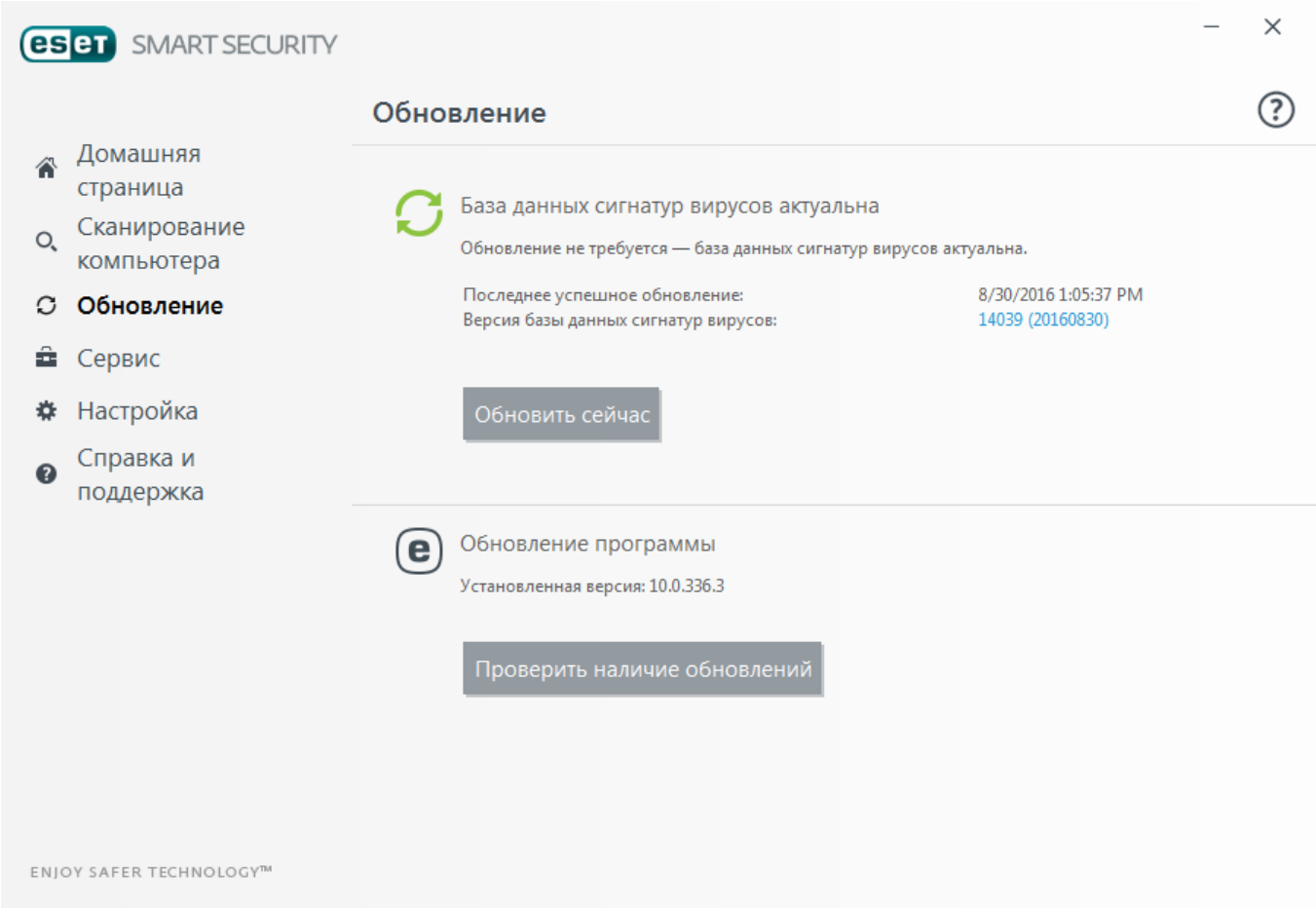
- **Предупреждение об оптимизации модуля «Антивор»**: это устройство не оптимизировано для модуля ESET Антивор. Например, на вашем компьютере может быть не создана фантомная учетная запись (функция системы защиты, автоматически включаемая, когда устройство помечается как отсутствующее). Фантомную учетную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

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

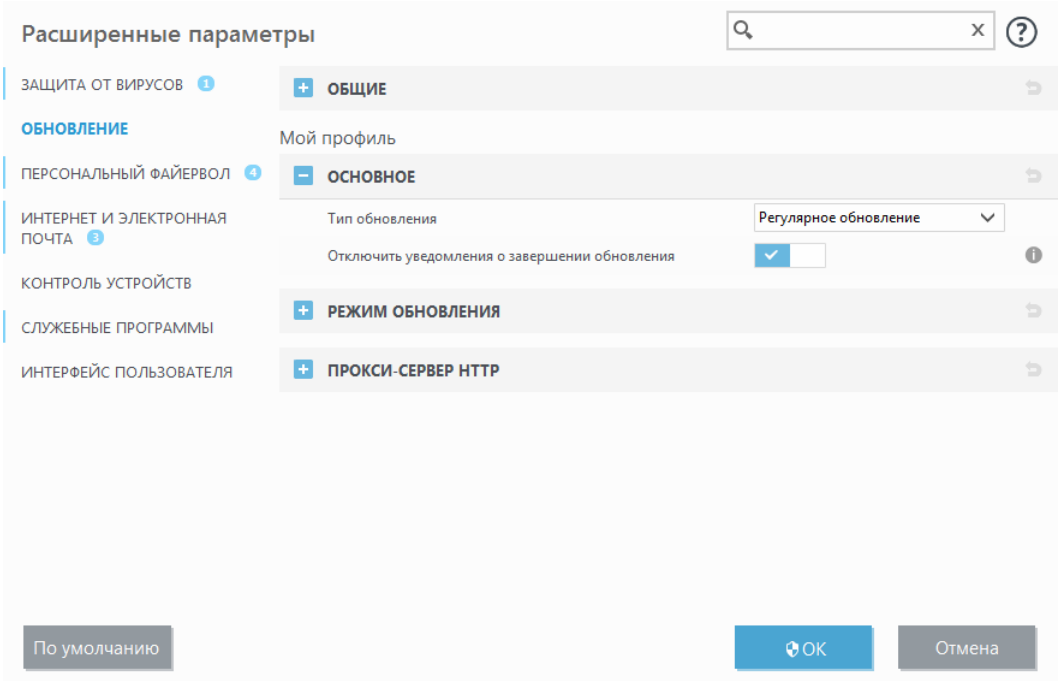
3.2 Обновления

Обновление базы данных сигнатур вирусов и компонентов программы является важной частью обеспечения защиты компьютера от вредоносного кода. Обратите особое внимание на их настройку и работу. В главном меню выберите пункт **Обновление**, а затем щелкните **Обновить сейчас**, чтобы проверить наличие обновлений базы данных сигнатур вирусов.

Если лицензионный ключ не был введен в процессе активации ESET Smart Security, на этом этапе будет предложено его ввести.



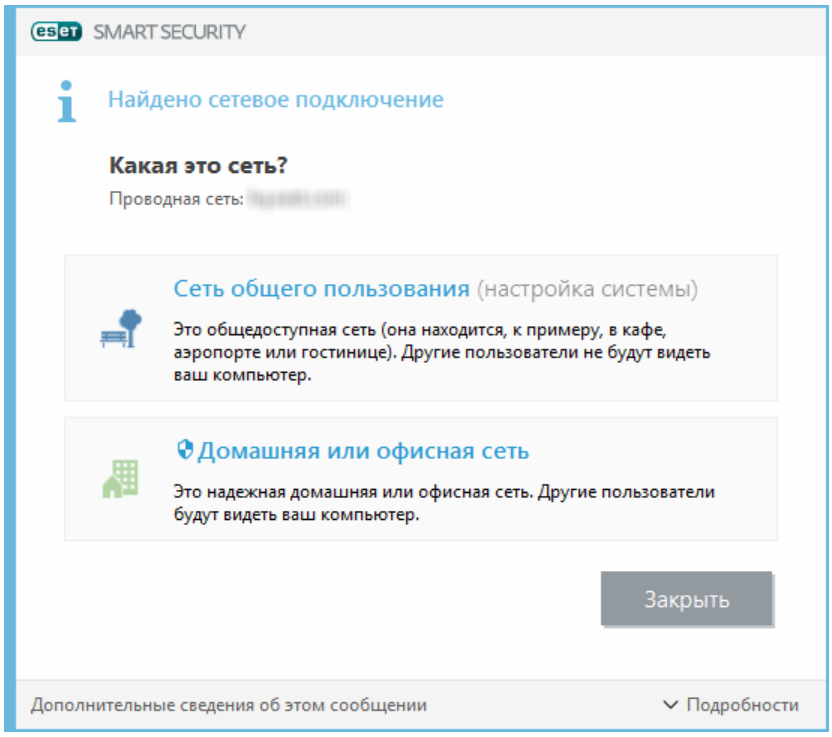
В окне **Дополнительные настройки** (выберите пункт **Настройка** в главном меню, после чего щелкните элемент **Дополнительные настройки** или нажмите клавишу F5) содержатся расширенные параметры обновления. Для настройки расширенных параметров обновления, таких как режим обновления, доступ через прокси-сервер и подключения к локальной сети, откройте соответствующую вкладку в окне **Обновление**.



3.3 Настройка доверенной зоны

Необходимо настроить доверенные зоны для защиты компьютера в сетевой среде. Настройка доверенных зон для разрешения общего доступа дает возможность предоставить доступ к компьютеру другим пользователям. Последовательно выберите элементы **Настройка** > **Защита сети** > **Подключенные сети** и щелкните ссылку рядом с подключенной сетью. На экран будет выведено окно, позволяющее выбрать нужный режим безопасности компьютера сети.

Обнаружение доверенных зон происходит после установки ESET Smart Security и при каждом подключении компьютера к новой сети. Таким образом, обычно нет необходимости задавать доверенные зоны. По умолчанию, если обнаруживается новая зона, появляется диалоговое окно, в котором пользователю будет предложено настроить уровень защиты для этой зоны.



ВНИМАНИЕ!
Неправильная настройка доверенной зоны может повлечь за собой снижение уровня безопасности компьютера.

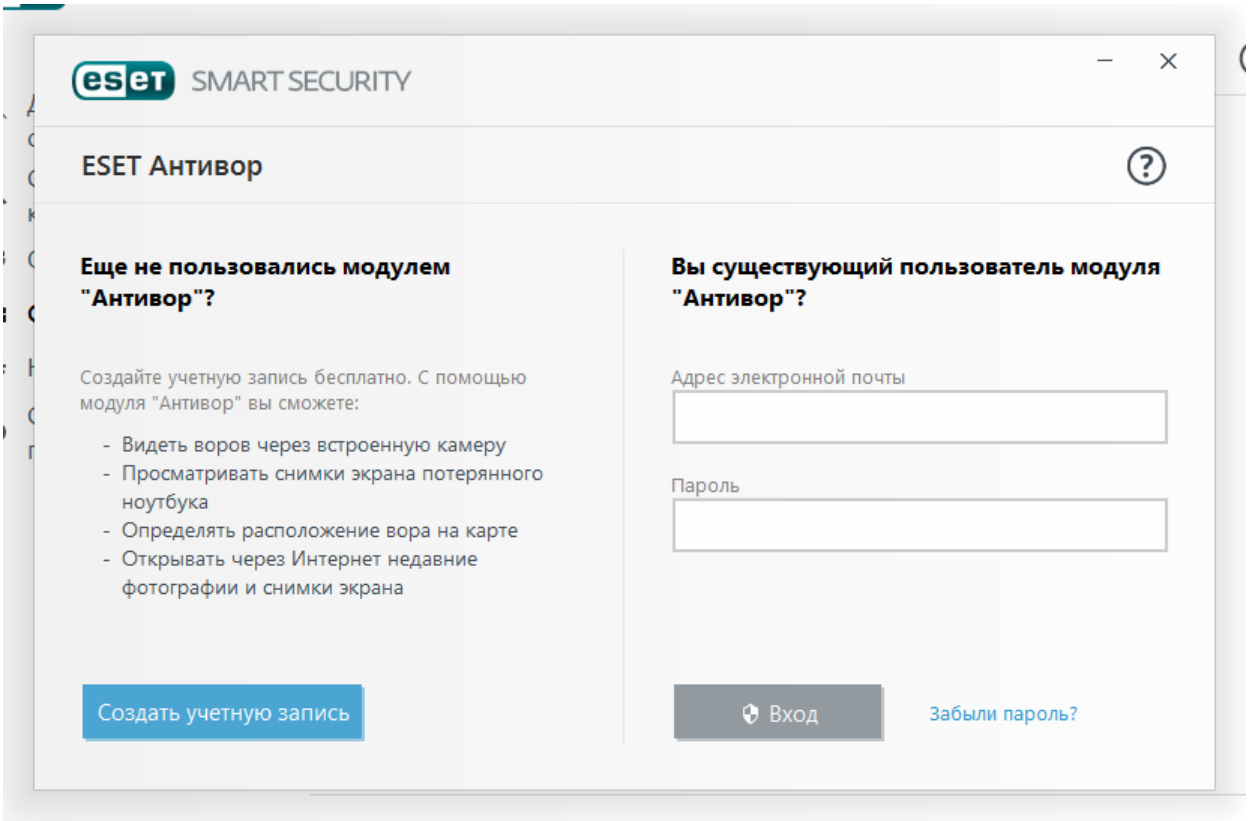
ПРИМЕЧАНИЕ.
По умолчанию рабочие станции из доверенной зоны получают доступ к файлам и принтерам, для которых открыт общий доступ, для них разрешены входящие соединения RPC, а также доступна служба удаленного рабочего стола.

Дополнительные сведения об этой функции см. в статье базы знаний ESET:
[В ESET Smart Security обнаружено новое сетевое подключение]

3.4 Антивор

Чтобы защитить компьютер от потери или кражи, выберите один из описанных ниже вариантов для регистрации компьютера в системе ESET Антивор.

1. После успешной активации выберите команду **Включить Антивор**, чтобы активировать функции ESET Антивор для только что зарегистрированного компьютера.



2. Если на панели **Главная** программы ESET Smart Security отображается сообщение о том, что модуль **ESET Антивор доступен**, рекомендуется активировать эту функцию на компьютере. Щелкните элемент **ВключитьESET Антивор**, чтобы зарегистрировать компьютер в системе ESET Антивор.

3. В главном окне программы последовательно выберите элементы **Настройка** > **Средства безопасности.** Щелкните элемент рядом с элементом **ESET Антивор** и следуйте инструкциям, приведенным в открывшемся окне.

ПРИМЕЧАНИЕ.
ESET Антивор Не поддерживается в операционных системах Microsoft Windows Home Server.

Дополнительные инструкции о связывании компьютера со службой ESET Антивор приведены в разделе Добавление нового устройства.

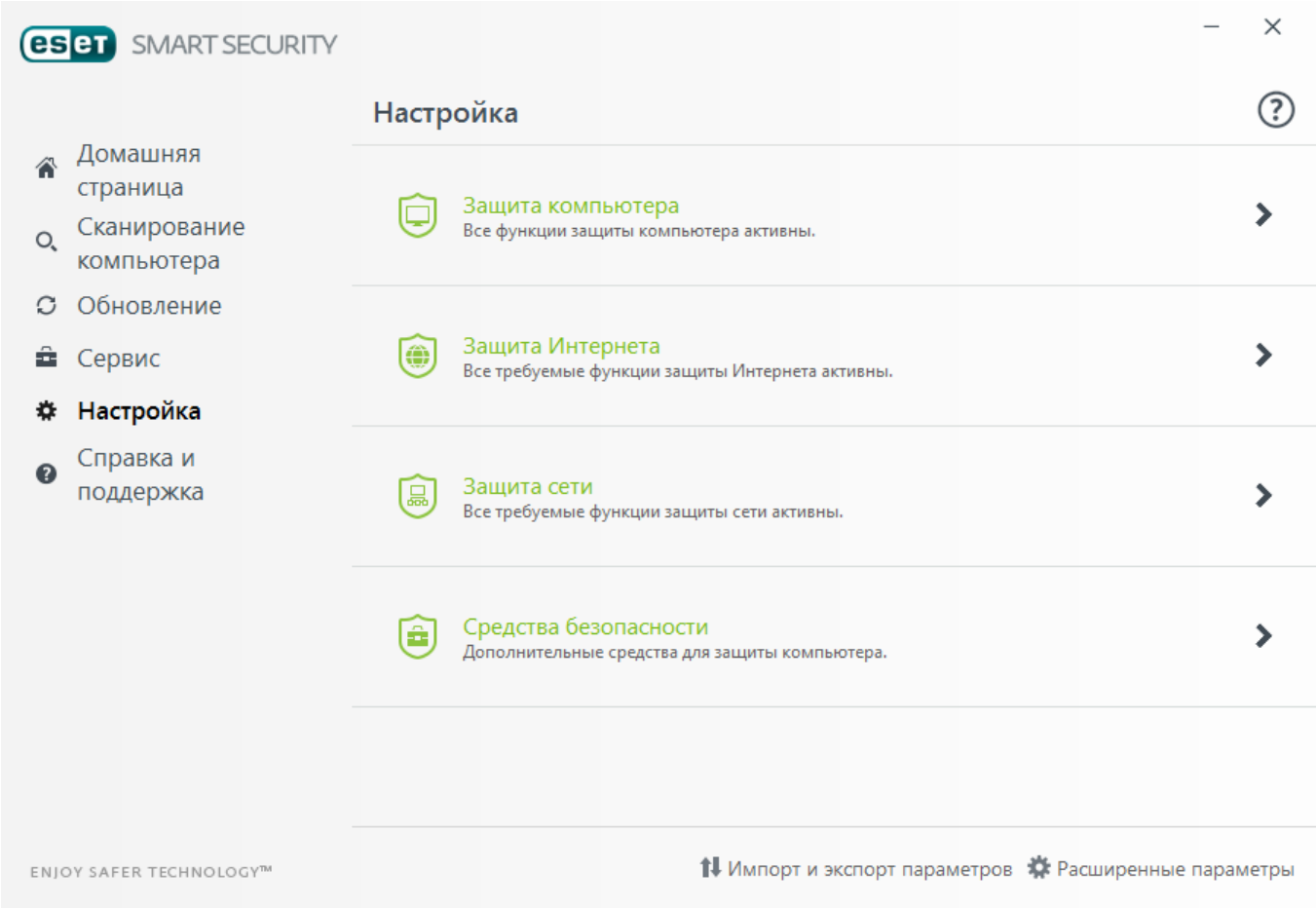
3.5 Средства родительского контроля

Если вы уже включили родительский контроль в ESET Smart Security, необходимо также настроить родительский контроль для нужных учетных записей пользователя, чтобы обеспечить правильную работу этой функции.

Если родительский контроль активирован, но учетные записи пользователя не настроены, на панели **Главная** главного окна программы отобразится сообщение **Функция родительского контроля не настроена**. Выберите команду **Настроить правила** и обратитесь к главе Родительский контроль за указаниями по созданию специальных ограничений для защиты детей от потенциально нежелательных материалов.

4. Работа с ESET Smart Security

Параметры настройки ESET Smart Security дают пользователю возможность настраивать уровни защиты компьютера и сети.



Меню **Настройка** содержит следующие разделы.

Защита компьютера

Защита в Интернете

Защита сети

Средства безопасности

Выберите компонент, чтобы настроить дополнительные параметры для соответствующего защитного модуля.

В настройках **защиты компьютера** можно включать и отключать следующие компоненты.

- **Защита файловой системы в режиме реального времени**: при открытии, создании или запуске любого файла на вашем компьютере выполняется сканирование на наличие вредоносного кода.
- **HIPS**: система предотвращения вторжений на узел отслеживает события в операционной системе и реагирует на них в соответствии с имеющимся набором правил.
- **Игровой режим**: включает или отключает игровой режим. После включения игрового режима на экран будет выведено предупреждение (о потенциальной угрозе безопасности), а для оформления главного окна будет применен оранжевый цвет.
- **Защита веб-камеры**: контролирует процессы и приложения, осуществляющие доступ к подключенной к компьютеру камере. Для получения дополнительных сведений щелкните здесь.

В настройках **защиты в Интернете** 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 спама**: сканируются нежелательные сообщения, т. е. спам.
- **Защита от фишинга**: обеспечивает фильтрацию веб-сайтов, заподозренных в распространении содержимого, которое предназначено для манипулирования пользователем, с тем чтобы получить от него конфиденциальную информацию.

Раздел **Защита сети** используется для включения или отключения Персонального файервола, защиты от сетевых атак (IDS) и Защиты от ботнетов.

Параметр **Средства безопасности** можно использовать для настройки следующих модулей.

- Защита банковской оплаты
- Родительский контроль
- Антивор

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

Для повторного включения отключенного компонента безопасности щелкните ползунок  таким образом, чтобы отобразился зеленый флажок.  .

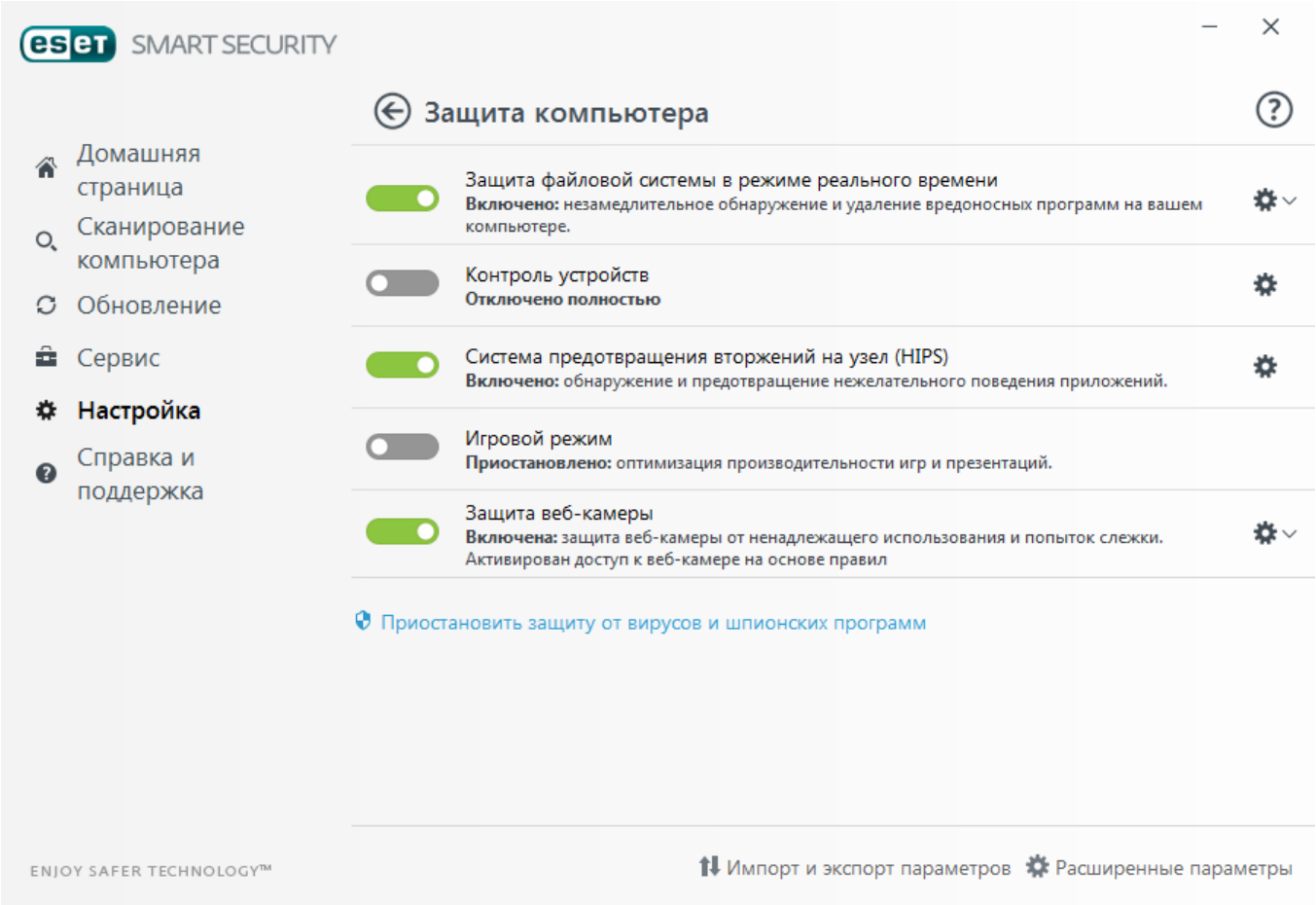
ПРИМЕЧАНИЕ.
При отключении защиты таким способом все отключенные модули защиты будут повторно включены после перезагрузки компьютера.

В нижней части окна настройки есть дополнительные параметры. Чтобы выполнить более подробную настройку параметров для каждого модуля, перейдите по ссылке **Дополнительные настройки**. Чтобы загрузить параметры настройки из файла конфигурации в формате *XML* или сохранить текущие параметры настройки в файл конфигурации, воспользуйтесь функцией **Импорт и экспорт параметров**.

4.1 Защита компьютера

В окне «Настройка» щелкните параметр «Защита компьютера», чтобы просмотреть общие сведения обо всех модулях защиты. Чтобы временно отключить тот или иной модуль, щелкните . Обратите внимание, что при этом будет ослаблена защита вашего компьютера. Щелкните элемент рядом с модулем защиты, чтобы получить доступ к дополнительным настройкам для него.

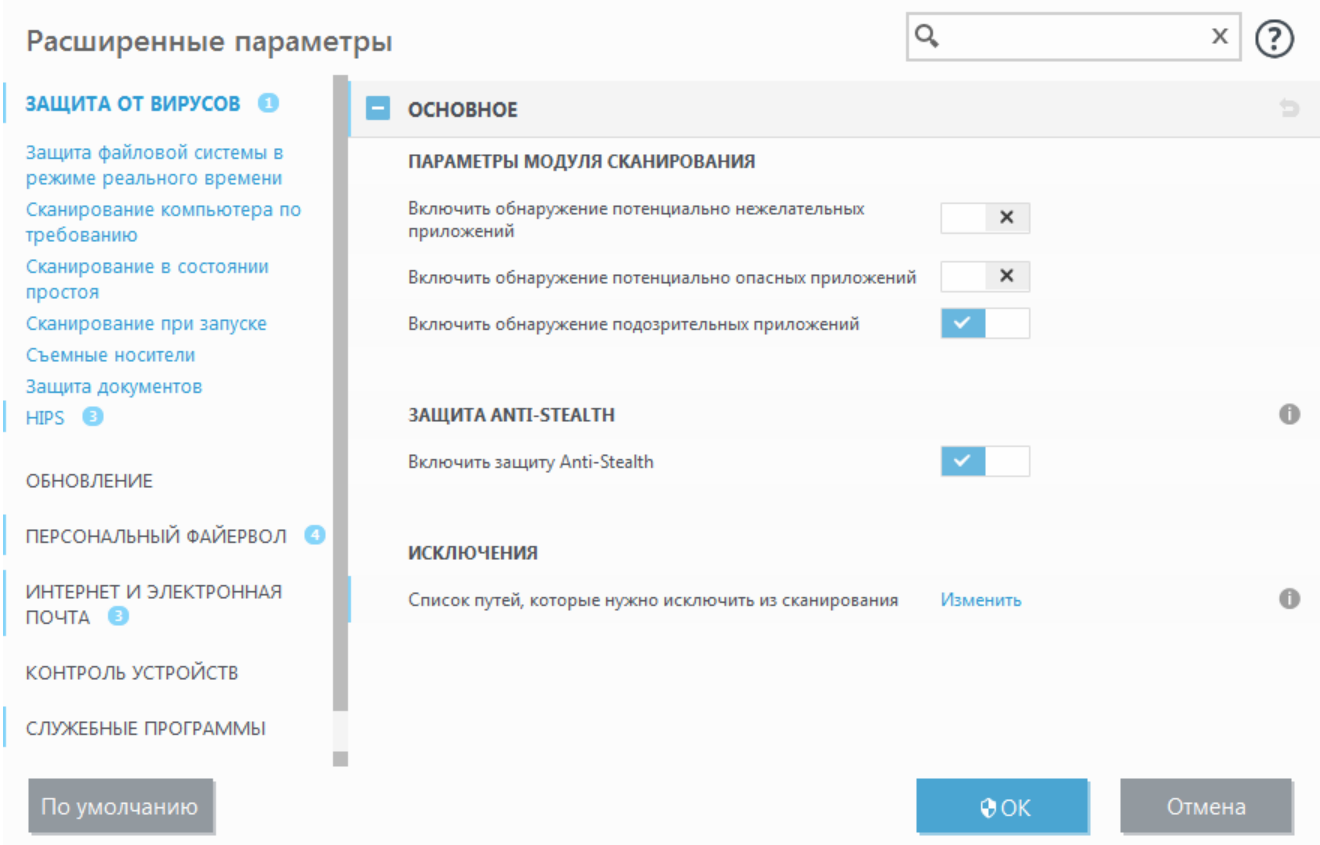
Щелкните элемент > **Изменить исключения** рядом с элементом**Защита файловой системы в режиме реального времени**, чтобы открыть окно настроек Исключение, в котором можно исключить файлы и папки из сканирования.



Приостановить защиту от вирусов и шпионских программ: отключение всех модулей защиты от вирусов и шпионских программ. При отключении защиты отображается соответствующее окно. С его помощью можно задать время, на которое будет отключена защита, выбрав значение в раскрывающемся меню **Время**. Нажмите кнопку **Применить** для подтверждения.

4.1.1 Защита от вирусов

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



Параметры модуля сканирования позволяют для всех модулей защиты (например, защиты файловой системы в режиме реального времени, защиты доступа в Интернет и т. д.) включить или отключить обнаружение следующих 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). Этот параметр по умолчанию 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.

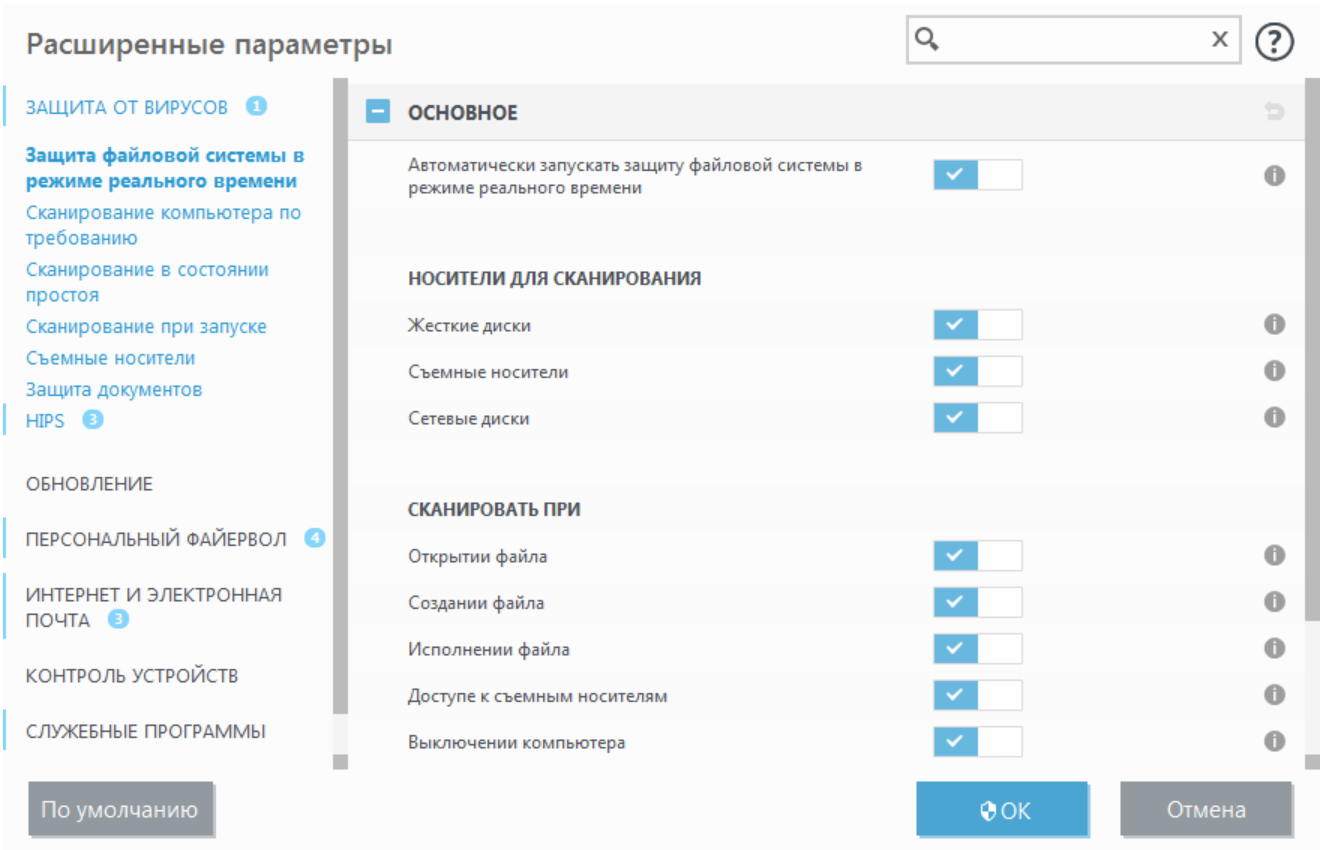
Технология Anti-Stealth является сложной системой, обеспечивающей обнаружение опасных программ, таких как руткиты, которые могут скрываться от операционной системы. Это значит, что такие программы невозможно обнаружить с помощью обычных методов тестирования.

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.

Включить расширенное сканирование с помощью AMSI: инструмент Microsoft Antimalware Scan Interface, позволяющий разработчикам приложений создавать новые средства защиты от вредоносного ПО (только Windows 10).

4.1.1.1 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. При открытии, создании или запуске файлов все они сканируются на наличие вредоносного кода. 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 реальном времени) защиту файловой системы в реальном времени можно выключить. Для этого нужно открыть окно **Дополнительные настройки** и в разделе **Защита файловой системы в реальном времени** > **Основное** снять флажок **Автоматически запускать защиту файловой системы в режиме реального времени**.

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 при каждом к ним доступе. Для изменения этого параметра откройте окно **Дополнительные настройки**, нажав клавишу **F5**, и перейдите к разделу **Защита от вирусов** > **Защита в режиме реального времени**. Последовательно щелкните элементы **Настройка параметров модуля ThreatSense** > **Другое** и снимите или установите флажок **Включить интеллектуальную оптимизацию**.

4.1.1.1.1 Дополнительные параметры ThreatSense

Дополнительные параметры ThreatSense для только что созданных и измененных файлов

Вероятность заражения только что созданных или измененных файлов выше по сравнению с аналогичным показателем для существующих файлов. Именно поэтому программа проверяет эти файлы с дополнительными параметрами сканирования. ESET Smart Security вместе с обычными методами сканирования, основанными на сигнатурах, применяет расширенную эвристики, что делает возможным обнаружение новых угрозеще до выпуска обновлений базы данных сигнатур вирусов В дополнение к только что созданным файлам выполняется также сканирование **самораспаковывающихся архивов** (.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**.

Дополнительные параметры ThreatSense для исполняемых файлов

Расширенный эвристический анализ при запуске файлов: по умолчанию при запуске файлов применяется расширенная эвристика. Если этот параметр включен, настоятельно рекомендуется включить оптимизацию Smart и ESET LiveGrid®, чтобы уменьшить воздействие на производительность системы.

Расширенная эвристика запуска файлов со съемных носителей: прежде чем разрешить запуск кода со съемного носителя, система расширенного эвристического анализа эмулирует код в виртуальной среде и оценивает его поведение.

4.1.1.1.2 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.

Обычная очистка — программа пытается автоматически очистить или удалить зараженный файл на основе предварительно заданного 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 («Обычная очистка») архив, в котором заражены все файлы, удаляется целиком. В режиме **Тщательная очистка** удаляется архив, в котором заражен хотя бы один файл, независимо от состояния остальных файлов.

4.1.1.1.3 Момент изменения конфигурации защиты в режиме реального времени

Защита в режиме реального времени является наиболее существенным элементом всей системы обеспечения безопасности. Необходимо быть внимательным при изменении ее параметров. Рекомендуется изменять параметры только в особых случаях.

После установки ESET Smart Security 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**).

4.1.1.1.4 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.

ПРИМЕЧАНИЕ.
Перед проверкой защиты в режиме реального времени необходимо отключить файервол. Если файервол включен, он обнаружит данный файл и предотвратит его загрузку.

4.1.1.1.5 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 в главном окне программы перейдите в раздел **Настройка** и нажмите **Защита компьютера** > **Защита файловой системы в режиме реального времени**.

Если защита файловой системы в режиме реального времени не запускается при загрузке системы, обычно это связано с тем, что отключен параметр **Автоматический запуск защиты файловой системы в режиме реального времени**. Чтобы включить этот параметр, перейдите в раздел **Дополнительные настройки** (**F5**) и последовательно выберите **Защита от вирусов** > **Защита 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. Если на компьютере установлено сразу две антивирусных программы, они могут конфликтовать между собой. Перед установкой ESET рекомендуется удалить с компьютера все прочие программы защиты от вирусов.

Защита 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.

4.1.1.2 Сканирование компьютера

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

Доступно два типа **сканирования ПК**. **Сканировать компьютер**: быстрое сканирование системы, не требующее уточнения параметров сканирования. **Выборочное сканирование** позволяет выбрать один из предварительно определенных профилей сканирования для проверки специальных папок, а также позволяет указывать конкретные объекты сканирования.

Сканировать компьютер

Функция «Сканировать компьютер» позволяет быстро запустить сканирование компьютера и очистить зараженные файлы без вмешательства пользователя. Преимущество такого сканирования заключается в том, что оно удобно в выполнении и не требует тщательной настройки сканирования. При таком сканировании 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 позволяет 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.

Сканирование съемных носителей

Подобно сканированию компьютера 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**.

Повторить последнее сканирование

Быстрый запуск последнего выполненного сканирования с использованием тех же настроек.

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

ПРИМЕЧАНИЕ

Рекомендуется запускать сканирование компьютера не реже одного раза в месяц. Можно настроить сканирование как запланированную задачу в меню **Служебные программы** > **Дополнительные средства** > **Планировщик**. Планирование еженедельного сканирования компьютера

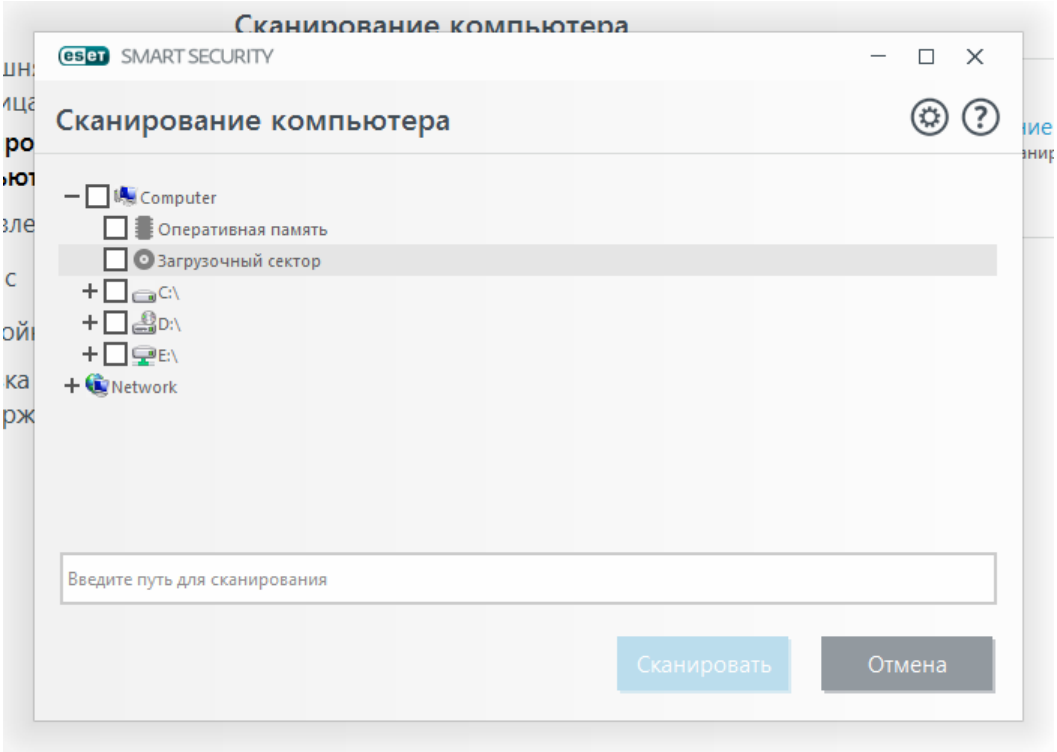
4.1.1.2.1 Средство запуска выборочного сканирования

Выборочное сканирование позволяет сканировать диск не целиком, а только определенные его части. Для этого последовательно щелкните элементы **Сканирование компьютера** > **Выборочное сканирование** и выберите один из вариантов в раскрывающемся списке **Объекты сканирования** либо конкретные объекты сканирования в древовидной структуре папок.

В раскрывающемся меню **Объекты сканирования** можно выбрать предварительно определенные объекты сканирования.

- **По параметрам профиля**: выбираются объекты сканирования, указанные в выбранном профиле сканирования.
- **Сменные носители**: выбираются дискеты, USB-устройства хранения, компакт- и DVD-диски.
- **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 или для добавления папки или файлов введите имя целевой папки в пустое 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 **Ничего не выбирать**.



Параметры очистки для сканирования можно настроить, последовательно выбрав элементы **Дополнительные настройки** > **Защита от вирусов** > **Сканирование компьютера по требованию** > Параметры **ThreatSense** > **Очистка.** Чтобы выполнить сканирование без очистки, выберите параметр **Сканировать без очистки**. История сканирования сохраняется в журнале сканирования.

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

В раскрывающемся меню **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

ThreatSense. Щелкните элемент **Настройка** для настройки пользовательского профиля сканирования. Параметры профиля сканирования описаны в разделе **Другое** параметров ThreatSense.

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

Кнопка **Сканировать с правами администратора** позволяет выполнять сканирование под учетной записью администратора. Воспользуйтесь этой функцией, если у текущего пользователя нет прав на доступ к файлам, которые следует просканировать. Данная кнопка недоступна, если текущий пользователь не может вызывать операции контроля учетных записей в качестве администратора.

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

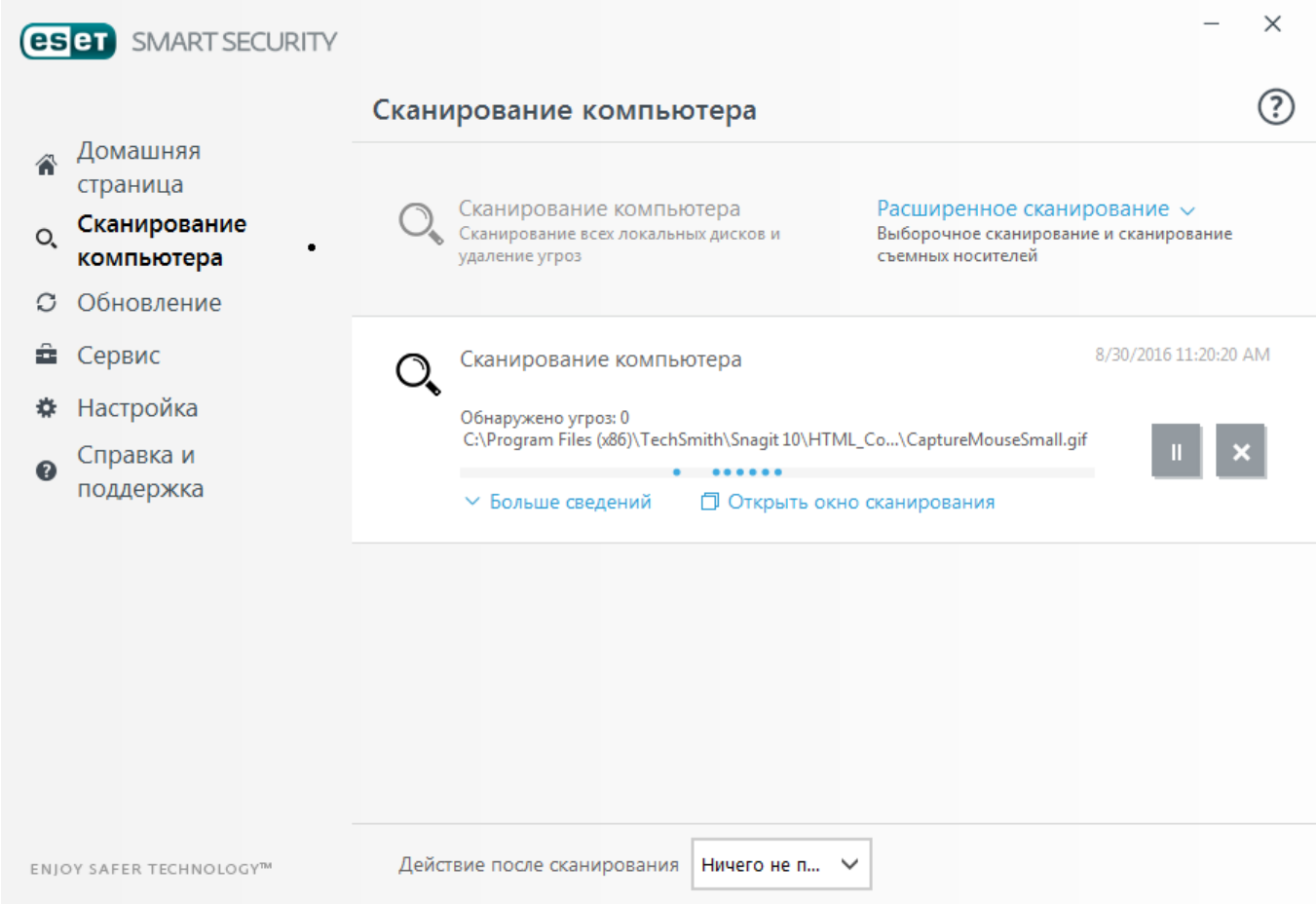
4.1.1.2.2 Ход сканирования

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

ПРИМЕЧАНИЕ.
Нормальной ситуацией является невозможность сканирования некоторых файлов, например защищенных паролем файлов или файлов, используемых исключительно операционной системой (обычно *pagefile.sys* и некоторых файлов журналов).

Ход сканирования: индикатор выполнения показывает состояние уже просканированных объектов по сравнению с объектами, ожидающими сканирования. Состояние выполнения сканирования формируется на основе общего количества объектов, включенных в сканирование.
Объект: имя и расположение объекта, который сканируется в настоящий момент.
Найдены угрозы: отображается общее количество просканированных файлов и угроз, обнаруженных и удаленных во время сканирования.
Пауза: приостановка сканирования.
Продолжить: этот параметр отображается после приостановки выполнения сканирования. Нажмите **Возобновить**, чтобы продолжить сканирование.
Остановить: прекращение сканирования.
Прокрутить журнал сканирования: если этот параметр активирован, журнал сканирования будет прокручиваться автоматически при добавлении новых записей, чтобы отображались самые свежие из них.

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



Действие после сканирования: выполнение запланированного завершения работы или перезагрузки по окончании сканирования компьютера. После завершения сканирования на экран будет выведено диалоговое окно подтверждения завершения работы. Оно будет активно в течение 60 секунд.

4.1.1.2.3 Профили сканирования

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** > **Основное** > **Список профилей**. В окне **Диспетчер профилей** есть раскрывающееся меню **Выбранный профиль**, в котором перечисляются существующие профили сканирования и есть возможность создать новый. Для создания профиля сканирования в соответствии с конкретными потребностями см. раздел Настройка параметров модуля ThreatSense, в котором описывается каждый параметр, используемый для настройки сканирования.

ПРИМЕЧАНИЕ.
Предположим, пользователю требуется создать собственный профиль сканирования, причем конфигурация **Сканировать компьютер** 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 **Выбранный профиль** и настройте остальные параметры в соответствии со своими требованиями, а затем нажмите кнопку **ОК**, чтобы сохранить новый профиль.

4.1.1.2.4 Журнал сканирования компьютера

В журнале сканирования компьютера содержатся общие сведения о сканировании, например такие:

- время завершения;
- общее время сканирования;
- количество обнаруженных угроз;
- количество просканированных объектов;
- просканированные диски, папки и файлы;
- дата и время сканирования;
- версия базы данных сигнатур вирусов.

4.1.1.3 Сканирование в состоянии простоя

Установите переключатель **Включить сканирование в состоянии простоя** в дереве **Дополнительные настройки** > **Антивирус** > **Сканирование в состоянии простоя** > **Основное**, чтобы разрешить автоматическое сканирование системы, когда компьютер не используется.

По умолчанию в состоянии простоя сканирование не работает, если компьютер (ноутбук) работает от батареи. Этот параметр можно переопределить, установив флажок **Сканировать даже в случае работы компьютера от аккумулятора**.

Включите параметр **Включить ведение журналов**, чтобы результаты сканирования компьютера регистрировались в разделе Файлы журналов: в главном окне программы последовательно щелкните элементы **Сервис** > **Файлы журналов**, после чего в раскрывающемся списке **Журнал** выберите элемент **Сканирование компьютера**.

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

- Заставка
- Блокировка компьютера
- Выход пользователя

Щелкните Параметры ThreatSense для изменения параметров сканирования в состоянии простоя (например, способов обнаружения).

4.1.1.4 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, исполняемых при запуске системы**. Для изменения его настроек выберите команду **Служебные программы** > **> Дополнительные средства** > > **Планировщик**, щелкните элемент **Автоматически проверять файлы при запуске системы**, а затем **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.

4.1.1.4.1 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 **Обычно используемые файлы** 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.

4.1.1.5 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. 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.

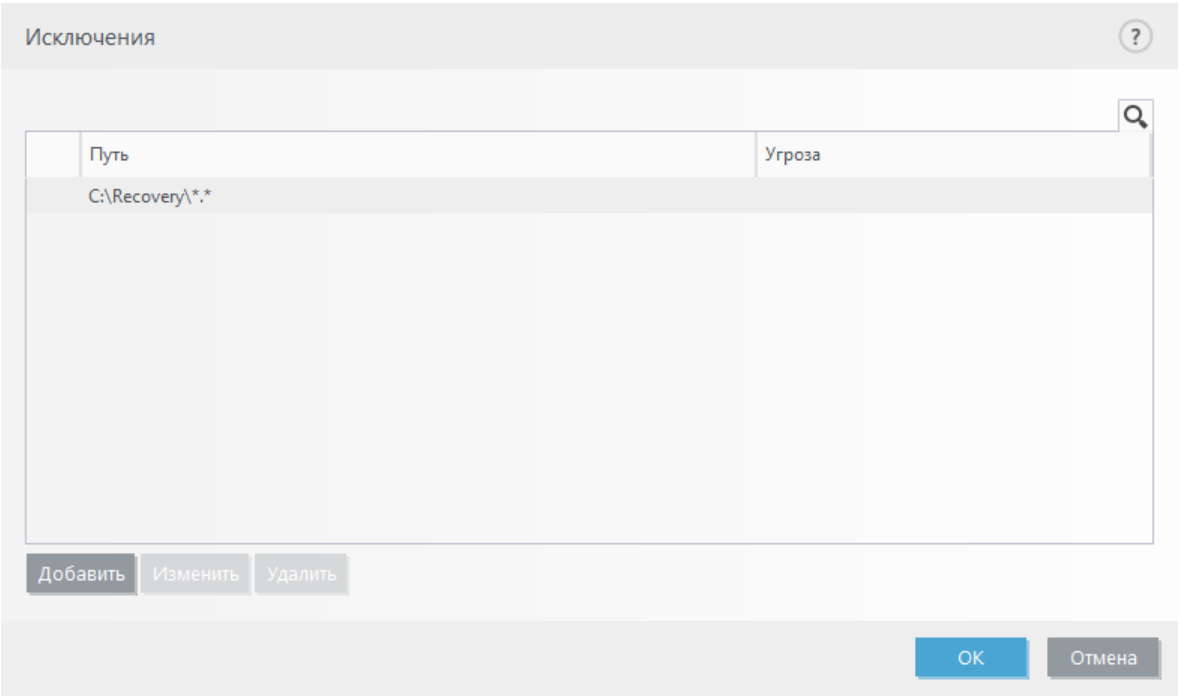
Для исключения объекта из сканирования выполните следующие действия.

1. Нажмите кнопку **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 вообще. Если этот файл позже окажется заражен другой вредоносной программой, модуль защиты от вирусов ее обнаружит. Исключения такого типа могут использоваться только с определенными типами заражений м могут создаваться в окне предупреждения об угрозе, в котором сообщается о заражении (последовательно щелкните элементы **Показать расширенные параметры** > **Исключить из обнаружения**). В качестве альтернативы для создания исключения выберите элементы **Служебные программы** > > **Дополнительные средства** > > **Карантин**, после чего щелкните правой кнопкой мыши находящийся в карантине файл и выберите в контекстном меню команду **Восстановить и исключить из обнаружения**.

Элементы управления

Добавить: исключение объектов из области сканирования.

Изменить: изменение выделенных записей.

Удалить: удаление выделенных записей.

4.1.1.6 Параметры ThreatSense

ThreatSense состоит из ряда сложных методов обнаружения угроз. Эта технология является упреждающей, т. е. защищает от новой угрозы уже в самом начале ее распространения. А сочетание анализа и моделирования кода, применения обобщенных сигнатур и сигнатур вирусов позволяет значительно повысить уровень безопасности компьютера. Модуль сканирования способен контролировать несколько потоков данных одновременно, благодаря чему максимизируются количество обнаруживаемых угроз и эффективность. ThreatSense обеспечивает к тому же успешное уничтожение руткитов.

Для модуля ThreatSense можно настроить несколько параметров сканирования:

- типы и расширения файлов, подлежащих сканированию;
- сочетание различных способов обнаружения;
- уровни очистки и т. д.

Чтобы открыть окно параметров, щелкните **Параметры ThreatSense** в окне «Дополнительные настройки» любого модуля, использующего технологию ThreatSense (см. ниже). Разные сценарии обеспечения безопасности могут требовать различных настроек. Поэтому технологию ThreatSense можно настроить отдельно для каждого из следующих модулей защиты:

- защита файловой системы в режиме реального времени;
- сканирование в состоянии простоя;
- сканирование при запуске;
- защита документов;
- защита почтового клиента;
- защита доступа в Интернет;
- сканирование компьютера.

ThreatSense может похвастаться параметрами, которые хорошо оптимизированы для каждого из модулей, причем 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, направленных на 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: это файлы архивов с расширением SFX, которые распаковываются самостоятельно.

Упаковщики: в отличие от архивов стандартных типов, запущенные упаковщики исполняемых файлов распаковываются прямо в оперативную 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 деятельности 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.

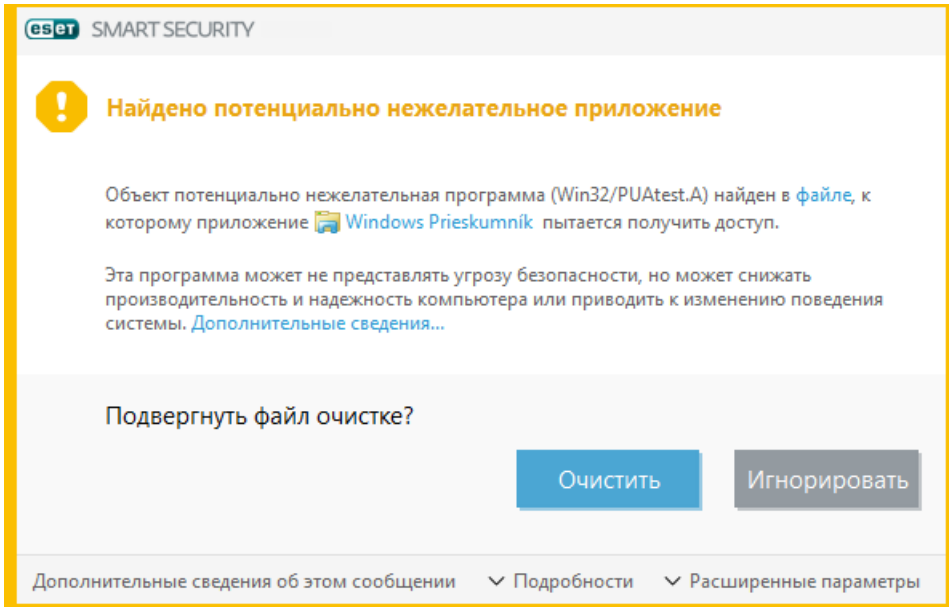
Расширенный эвристический анализ/сигнатуры распределенных сетевых атак: метод расширенной эвристики базируется на уникальном эвристическом алгоритме, разработанном компанией ESET, оптимизированном для обнаружения компьютерных червей и троянских программ и реализованном на языках программирования высокого 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 доступность 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 — это программа, которая содержит рекламу, устанавливает панели инструментов или выполняет другие неясные функции. В некоторых ситуациях может показаться, что преимущества такого потенциально нежелательного приложения перевешивают риски. Поэтому компания ESET помещает эти приложения в категорию незначительного риска, в отличие от других вредоносных программ, например троянских программ или червей.

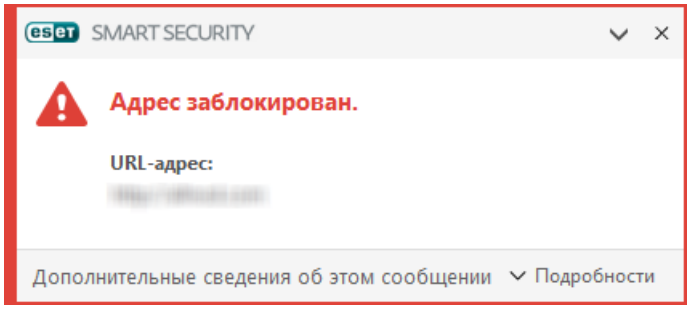
Предупреждение — обнаружена потенциальная угроза

Когда обнаруживается потенциально нежелательное приложение, можно решить, какое действие следует выполнить.

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

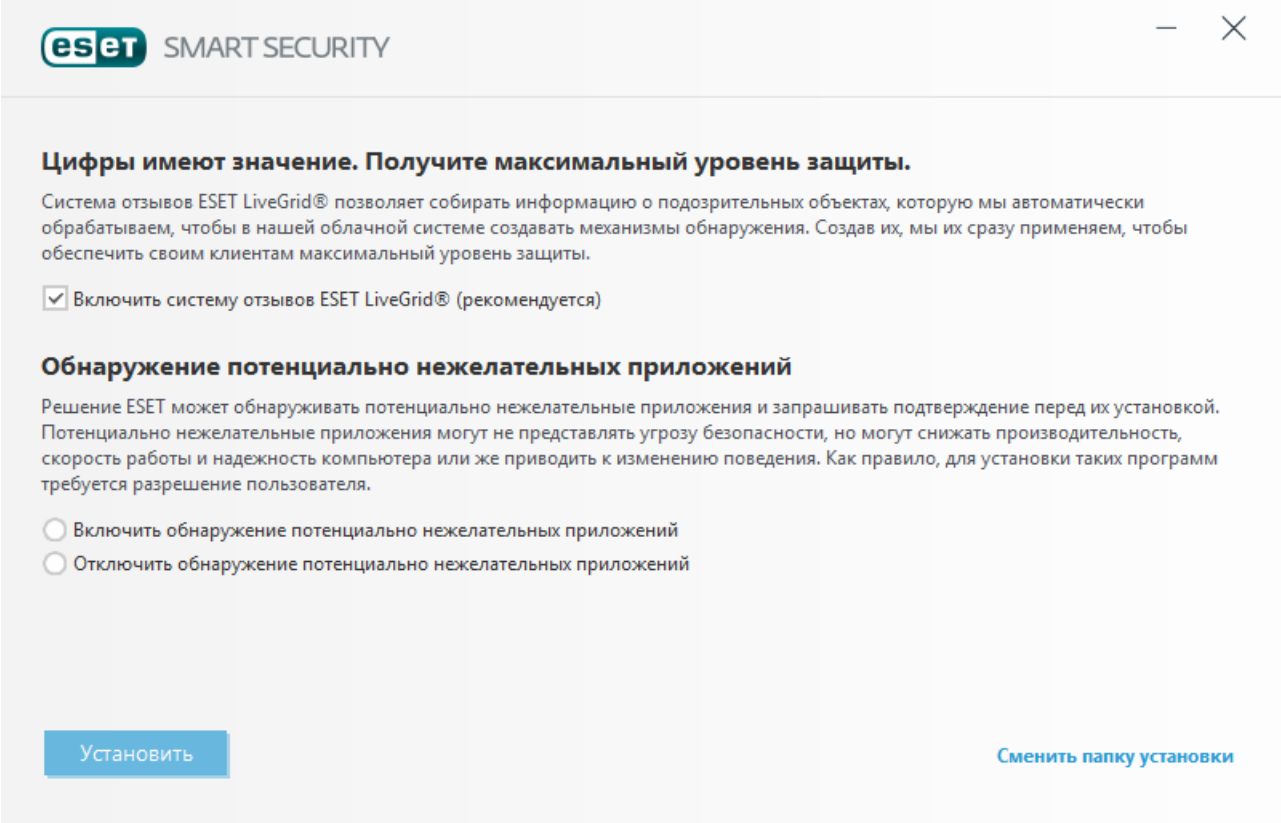


Если обнаруживается потенциально нежелательное приложение и его не удается очистить, отображается уведомление **Адрес заблокирован**. Для получения дополнительных сведений об этом событии перейдите из главного меню в раздел **Служебные программы** > **Дополнительные средства** > **Файлы журналов** > **Отфильтрованные веб-сайты**.



Потенциально нежелательные приложения — параметры

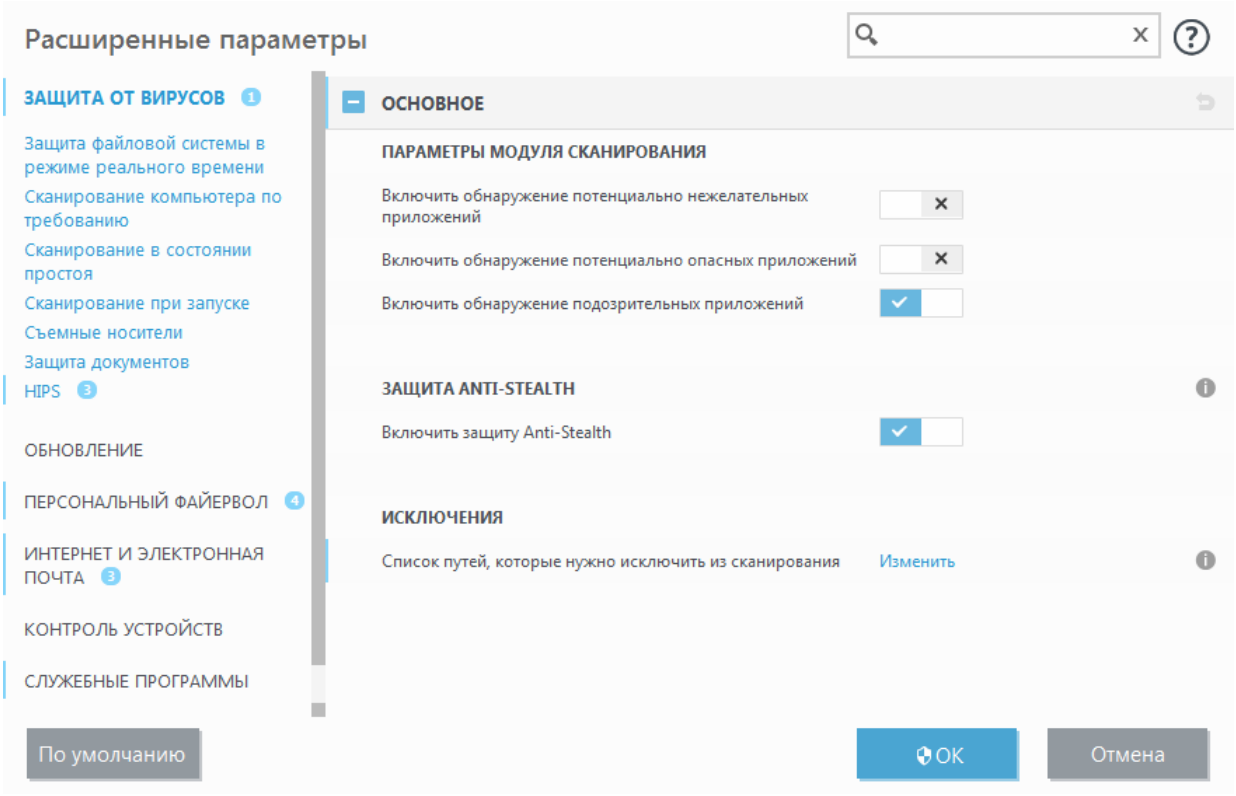
При установке программы ESET можно включить обнаружение потенциально нежелательных приложений (см. изображение ниже).



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 приведенным ниже инструкциям.

1. Откройте программу ESET. Как открыть программу ESET на моем компьютере?
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 рекламной программой, которые могут изменить домашнюю страницу браузера или параметры поиска. При этом файлообменные ресурсы часто не уведомляют поставщиков программного обеспечения или получателей загруженных файлов о внесенных изменениях и скрывают настройки, позволяющие от них отказаться. Именно поэтому компания ESET считает оболочки потенциально нежелательными приложениями и дает пользователям возможность отказаться от их загрузки.

Обновленную версию данной страницы справки см. в этой статье базы знаний ESET.

Потенциально опасные приложения. Потенциально опасные приложения — это обозначение для не являющихся вредоносными 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.

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

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 параметров модуля ThreatSense для сканирования компьютера по требованию также доступны описанные ниже параметры из раздела **Другое**.

Сканировать альтернативные потоки данных (ADS): альтернативные потоки данных, используемые файловой системой NTFS, — это связи файлов и папок, которые не обнаруживаются при использовании обычных методов сканирования. Многие заражения маскируются под альтернативные потоки данных, пытаясь избежать обнаружения.

Запускать фоновое сканирование с низким приоритетом: каждый процесс сканирования потребляет некоторое количество системных ресурсов. Если пользователь работает с ресурсоемкими программами, можно активировать фоновое сканирование с низким приоритетом и высвободить тем самым ресурсы для других приложений.

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 оптимизации Smart используются оптимальные параметры для обеспечения самого эффективного уровня сканирования с сохранением максимально высокой скорости. Разные модули защиты выполняют интеллектуальное сканирование, применяя отдельные методы для различных типов файлов. Если оптимизация Smart отключена, при сканировании используются только пользовательские настройки ядра ThreatSense каждого модуля.

Сохранить отметку о времени последнего доступа: установите этот флажок, чтобы 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 сканирования объекта. Если пользователь укажет здесь собственное значение, модуль защиты от вирусов прекратит сканирование объекта по истечении указанного времени вне зависимости от того, завершено ли сканирование. Значение по умолчанию: *не ограничено*.

Настройки сканирования архивов

Уровень вложенности архивов: определяет максимальную глубину сканирования архивов. Значение по умолчанию: *10*.

Максимальный размер файла в архиве: этот параметр позволяет задать максимальный размер подлежащих сканированию файлов в архиве (имеется в виду размер, который будут иметь извлеченные файлы). Значение по умолчанию: *не ограничено*.

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

4.1.1.6.1 Очистка

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

4.1.1.6.2 Исключенные из сканирования расширения файлов

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

По умолчанию сканируются все файлы независимо от их расширения. 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 файлов с определенными расширениями. Для добавления в список нового расширения нажмите кнопку **Добавить**, введите расширение в пустом поле и нажмите кнопку **ОК**. Выбрав вариант **Введите несколько значений**, можно добавить несколько расширений имен файлов, разделив их символами перевода строки, запятой или точки с запятой. Если разрешен ввод нескольких значений, расширения будут отображаться в виде списка. Чтобы удалить расширение из списка, выберите это расширение и нажмите кнопку **Удалить**. Для изменения выбранного расширения нажмите кнопку **Изменить**.

Специальные символы ? (вопросительный знак). Звездочка вопросительный знак — любой отдельный символ.

ПРИМЕЧАНИЕ.
Чтобы отобразить расширение файла (если оно есть) в операционной системе Windows, выберите **Панель управления** > **Параметры папок** > **Вид** (вкладка), снимите флажок **Скрывать расширения для зарегистрированных типов файлов**, а затем нажмите кнопку «Применить».

4.1.1.7 Действия при обнаружении заражения

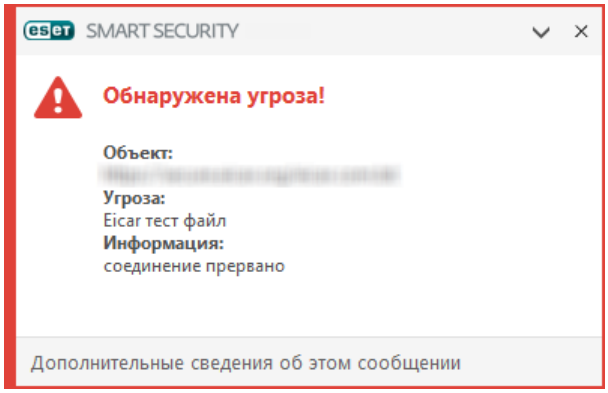
Заражения могут попасть на компьютер из различных источников, таких как веб-сайты, общие папки, электронная почта или съемные носители (накопители USB, внешние диски, компакт- или DVD-диски, дискеты и т. д.).

Стандартное поведение

Обычно ESET Smart Security обнаруживает заражения с помощью следующих модулей:

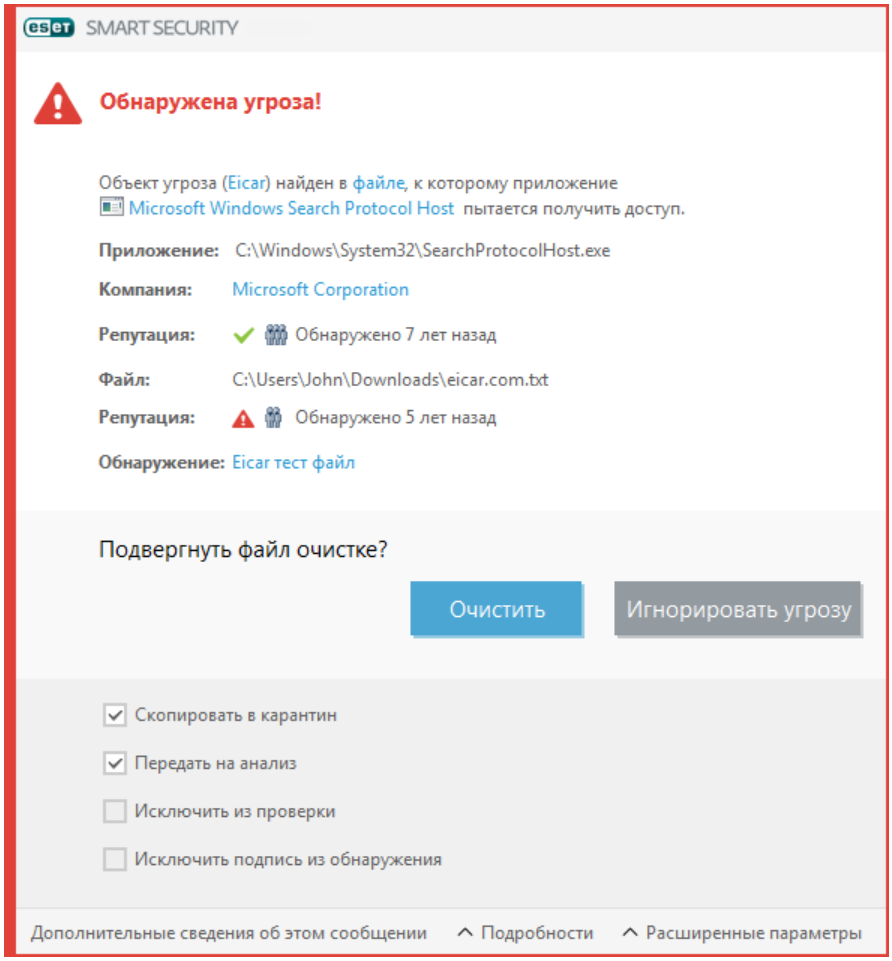
- защита файловой системы в режиме реального времени;
- защита доступа в Интернет;
- защита почтового клиента;
- сканирование компьютера по требованию.

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

Удаление файлов из архивов

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

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

- Откройте ESET Smart Security и выберите команду «Сканирование компьютера».
- Выберите вариант **Сканировать компьютер** (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.

4.1.1.8 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 еще один уровень безопасности в дополнение к функции защиты файловой системы в режиме реального времени. Чтобы улучшить производительность систем, где не осуществляется работа с большим количеством документов Microsoft Office, функцию защиты документов можно отключить.

Для включения функции защиты документов откройте окно **Дополнительные настройки** (нажмите клавишу F5), затем выберите элементы **Защита от вирусов** > **Защита документов** и установите переключатель **Интеграция с системой**.

ПРИМЕЧАНИЕ.
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).

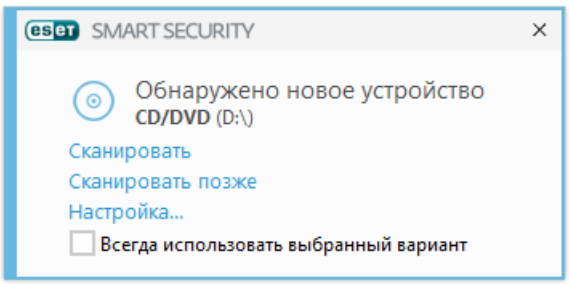
4.1.2 Съемные носители

ESET Smart Security 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 к компьютеру съемного носителя (компакт-диска, DVD-диска, USB-устройства). 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: отобразятся «Дополнительные настройки».

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

Кроме того, в ESET Smart Security есть модуль контроля устройств, позволяющий задавать правила использования внешних устройств на указанном компьютере. Дополнительные сведения об этом модуле см. в разделе Контроль устройств.

4.1.3 Контроль устройств

Контроль устройств

ESET Smart Security обеспечивает автоматическое управление устройствами (компакт- и DVD-дисками, USB-устройствами и т. п.). Данный модуль позволяет сканировать, блокировать и 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-принтер
- FireWire-хранилище
- Устройство Bluetooth
- Устройство чтения смарт-карт
- Устройство обработки изображений
- Модемы
- LPT/COM-порты
- Переносное устройство
- Микрофон
- Все типы устройств

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

Если активировать переключатель **\Интеграция с системой**, в программе ESET Smart Security 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 открыть окно Редактор правил.

ПРИМЕЧАНИЕ.
Можно создать разные группы устройств, к которым будут применяться разные правила. Группу, к которой применяется правило с действием **Чтение и запись** или **Только для чтения**, можно создать только одну. Благодаря этому, когда к компьютеру подключаются неопознанные устройства, функция контроля устройств их блокирует.

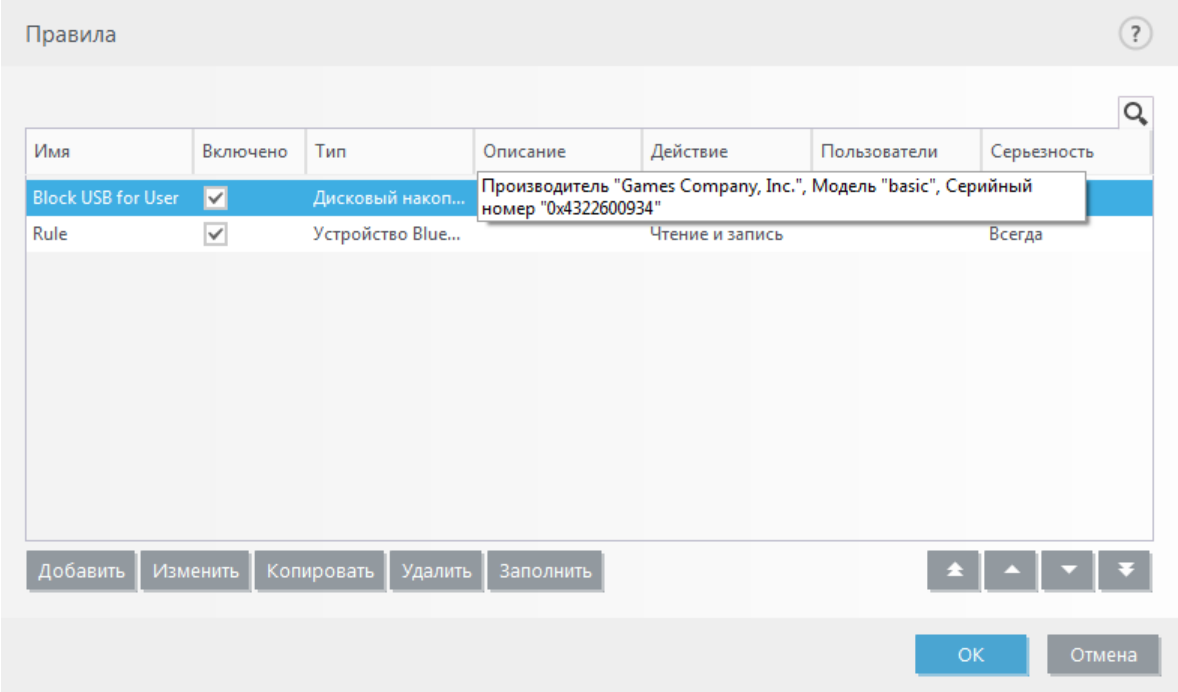
При подключении устройства, заблокированного существующим правилом, отобразится окно уведомления, и доступ к устройству будет заблокирован.

Защита веб-камеры

Включением переключателя, расположенного рядом с элементом **Интеграция с системой**, активируется функция «Защита веб-камеры» в решении ESET Smart Security. После включения функции «Защита веб-камеры» кнопка **Правила** станет активной и вы сможете открыть окно Редактор правил.

4.1.3.1 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.



Вы можете разрешить или заблокировать определенные устройства для конкретных пользователей или их групп, а также в соответствии с дополнительными параметрами, которые задаются в конфигурации правил. В списке правил для каждого правила отображается описание, включающее название и тип внешнего устройства, действие, выполняемое после его подключения к компьютеру, а также серьезность для журнала.

Для управления правилом используйте кнопки **Добавить** или **Изменить**. Чтобы создать правило с использованием заранее заданных параметров из другого правила, нажмите кнопку **Копировать**. XML-строки, которые отображаются, если щелкнуть правило, можно скопировать в буфер обмена. Кроме того, они могут помочь системным администраторам экспортировать или импортировать эти данные, а также использовать их, например, в ESET Remote Administrator.

Чтобы выделить несколько правил, щелкните их, удерживая нажатой клавишу CTRL. Затем их можно будет одновременно удалить либо переместить к началу или концу списка. Флажок **Включено** позволяет включить или отключить правило. Это может быть полезно, если вы не хотите полностью удалять правило, чтобы воспользоваться им позднее.

Управление основано на правилах, которые отсортированы по приоритету: правила с более высоким приоритетом находятся в начале.

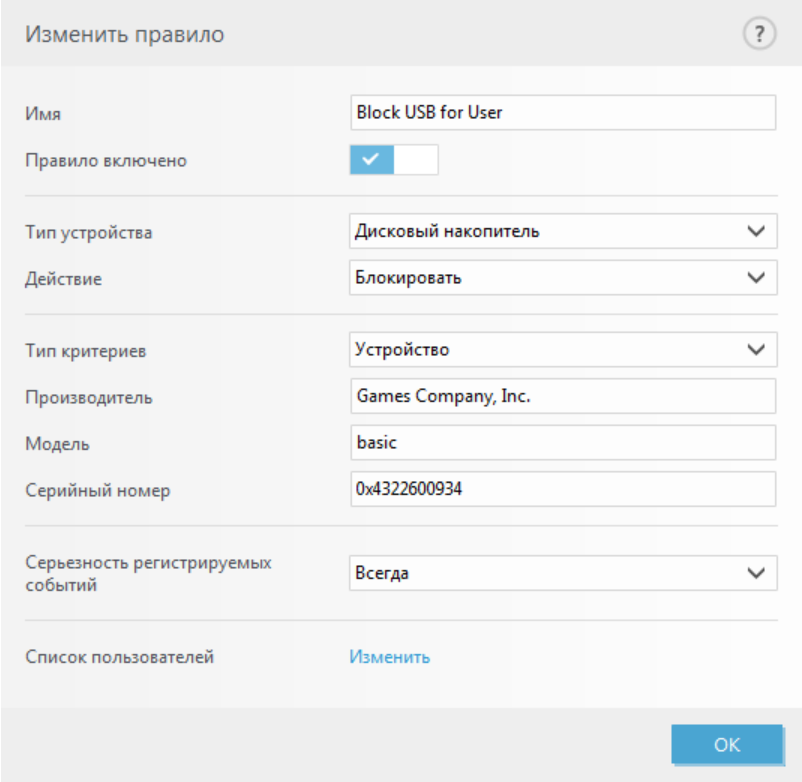
Записи журнала можно просмотреть в главном окне ESET Smart Security в разделе **Служебные программы** > **Дополнительные средства** > **Файлы журнала**.

В журнал контроля устройств записываются все случаи, когда срабатывает функция контроля устройств.

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

4.1.3.2 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 списке 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.

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 о том, разрешено это устройство или заблокировано, и при этом создается запись в журнале. Устройства не запоминаются. Уведомления отображаются при каждом повторном подключении одного и того же устройства.

Обратите внимание, что полный список действий (разрешений) доступен не для всех типов устройств. Если устройство относится к типу хранилищ, будут доступны все четыре действия. Если устройство не предназначено для хранения данных, будут доступны только три действия. Например, разрешение **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 (*, ?).

ПРИМЕЧАНИЕ.
Для просмотра сведений об этом устройстве создайте правило для соответствующего типа устройств, подключите устройство к компьютеру и ознакомьтесь со сведениями об устройстве в журнале контроля устройств.

Серьезность регистрируемых событий

Персональный файервол ESET Smart Security сохраняет данные обо всех важных событиях в файле журнала, который можно открыть из главного меню. Щелкните **Служебные программы** > **Дополнительные средства** > **Файлы журналов** и выберите в раскрывающемся списке **Журнал** элемент **Контроль устройств**.

- **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.
Все устройства можно фильтровать по пользовательским правилам (например, устройства обработки изображений предоставляют информацию только о действиях, но не о пользователях).

4.1.3.3 Редактор правил защиты веб-камеры

В этом окне отображаются имеющиеся правила и предоставляется возможность управлять приложениями и процессами, которые осуществляют доступ к веб-камере вашего компьютера, основываясь на совершенном вами действии.

Доступны перечисленные далее действия.

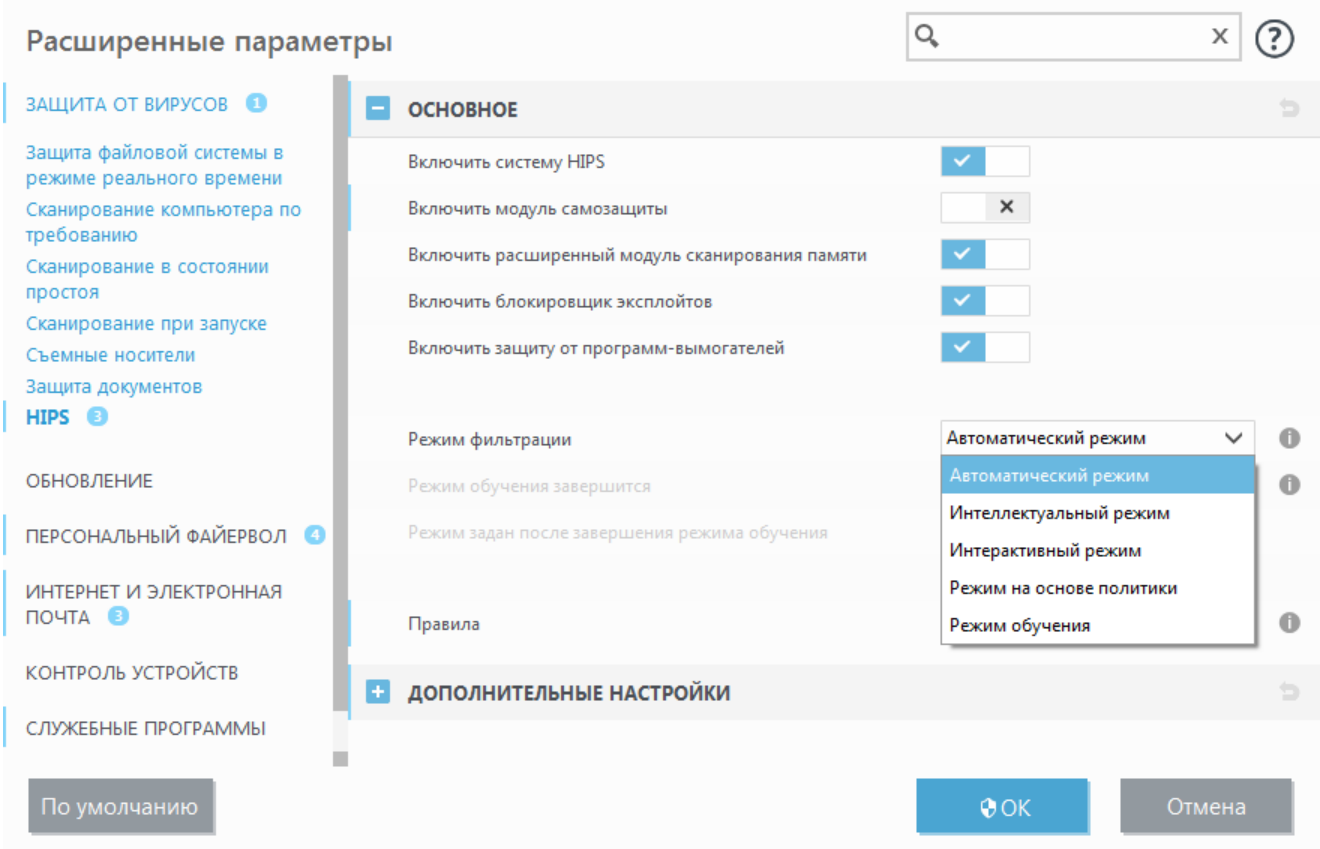
- **Заблокировать доступ**
- **Запросить**
- **Разрешить доступ**

4.1.4 Система предотвращения вторжений на узел (HIPS)

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) > **Защита от вирусов** > **Система предотвращения вторжений на узел** > **Основные**. Состояние HIPS (включено/отключено) отображается в главном окне программы ESET Smart Security, в разделе **Настройка** > **Защита компьютера**.



использует встроенную технологии **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.

Включить защищенную службу: включается защита на уровне ядра (Windows 8.1, 10).

Расширенный модуль сканирования памяти работает в сочетании с блокировщиком эксплойтов, чем обеспечивается усиленная защита 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.

Защита от программ-шантажистов — это еще один уровень защиты, функционирующий как часть компонента предотвращения вторжений на узел. Для работы модуля защиты от программ-шантажистов необходимо, чтобы система репутации LiveGrid была включена. Дополнительную информацию об этом типе защиты см. здесь.

Доступны четыре режима фильтрации.

Автоматический режим: включены все операции за исключением тех, что заблокированы посредством предварительно заданных правил, предназначенных для защиты компьютера.

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

Интерактивный режим: пользователю будет предлагаться подтверждать операции.

Режим на основе политики: операции блокируются.

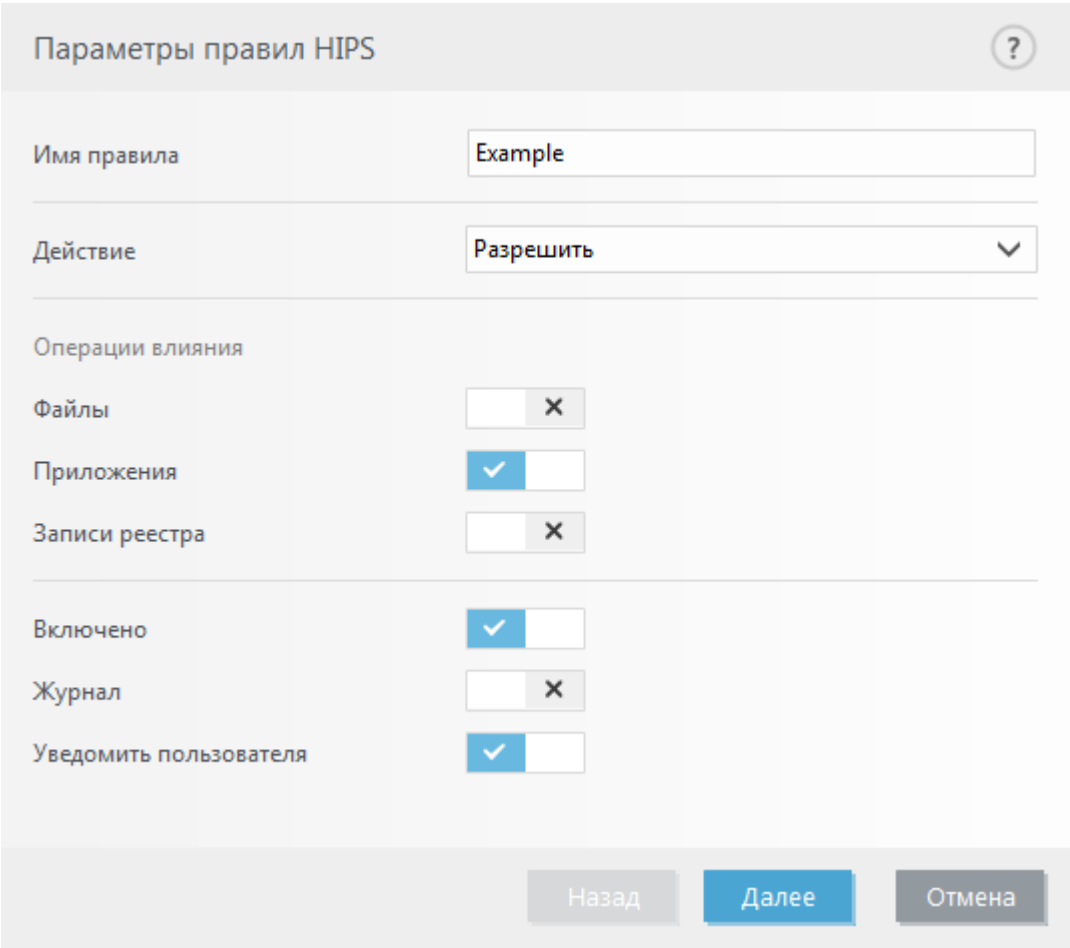
Режим обучения: операции включены, причем после каждой операции создается правило. Правила, создаваемые в таком режиме, можно просмотреть в редакторе правил, но их приоритет ниже, чем у правил, создаваемых вручную или в автоматическом режиме. Если в раскрывающемся списке режимов фильтрации HIPS выбран режим обучения, становится доступным параметр **Режим обучения завершится**. Выберите длительность использования режима обучения. Максимальная длительность — 14 дней. Когда указанный период завершится, вам будет предложено изменить правила, созданные системой HIPS в режиме обучения. Кроме того, можно выбрать другой режим фильтрации или отложить решение и продолжить использовать режим обучения.

Режим задан после завершения режима обучения: выберите режим фильтрации, который будет действовать по окончании использования режима обучения.

Система предотвращения вторжений на узел отслеживает события в операционной системе и реагирует на них на основе правил, аналогичных правилам персонального файервола. Нажмите кнопку **Изменить**, 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 операцию, 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 по программе, 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.



4.1.4.1 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 явно посредством пользовательского правила.

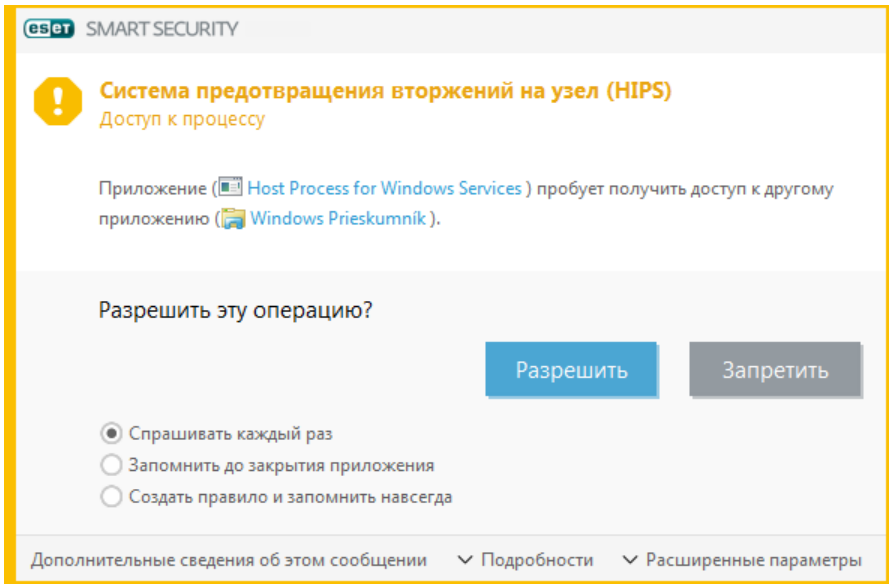
Регистрировать все заблокированные операции: все заблокированные операции будут записываться в журнал системы предотвращения вторжений на узел.

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.

4.1.4.2 Интерактивное окно HIPS

Если для правила по умолчанию установлено действие **Запросить**, то при каждом запуске правила будет отображаться диалоговое окно. В нем можно **запретить** или **разрешить** операцию. Если пользователь не выбирает действие в течение определенного времени, на основе правил выбирается новое действие.

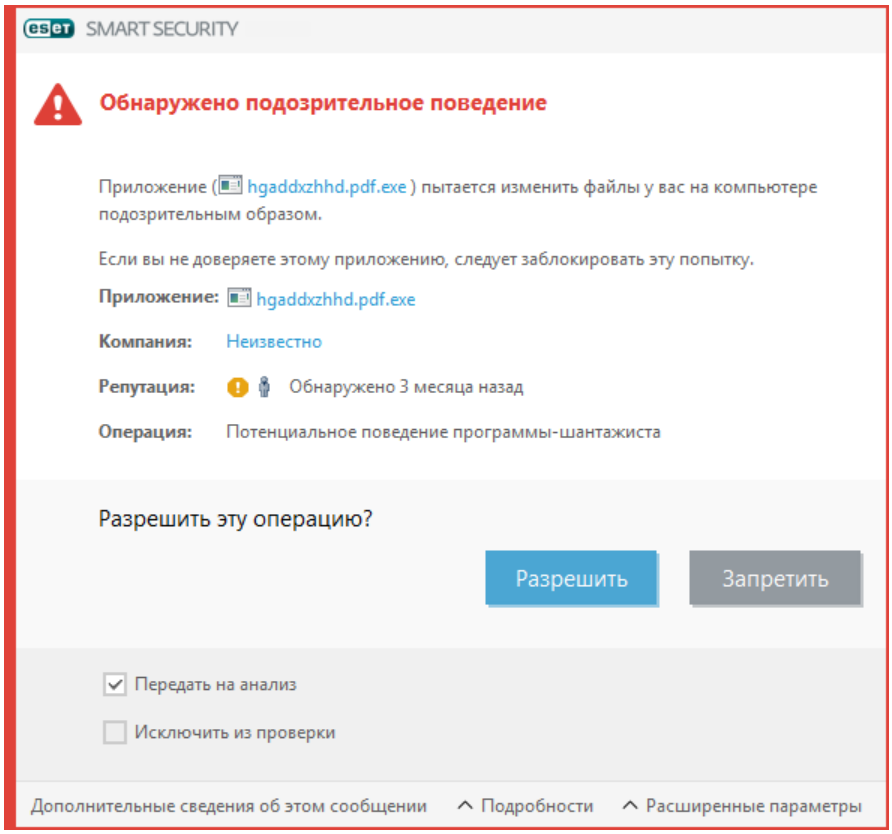


В диалоговом окне можно создать правило на основе нового действия, обнаруживаемого системой HIPS, а затем определить условия, в соответствии с которыми это действие будет разрешено или запрещено. Отдельные параметры можно настроить, щелкнув элемент **Дополнительные сведения**. Правила, создаваемые таким 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.

Временно запомнить это действие для данного процесса — если выбрать эту установку, действие (**Разрешить/Запретить**) будет использоваться до тех пор, пока не изменятся 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.

4.1.4.3 Обнаружено потенциальное поведение программы-шантажиста

При обнаружении потенциального поведения, характерного для программы-шантажиста, отображается диалоговое окно. В нем можно **запретить** или **разрешить** операцию.



Данное диалоговое окно позволяет **отправить файл на анализ** или **исключить из проверки**. Нажмите кнопку **Сведения**, чтобы просмотреть конкретные параметры обнаружения.

4.1.5 Игровой режим

Игровой режим — это функция для тех, кто стремится избежать перерывов в работе программного обеспечения и появления отвлекающих всплывающих окон, а также желает свести к минимуму нагрузку на процессор. Его также можно использовать во время презентаций, которые нельзя прерывать деятельностью модуля защиты от вирусов. При включении этой функции отключаются все всплывающие окна, а работа планировщика полностью останавливается. Защита системы по-прежнему работает в фоновом режиме, но не требует какого-либо вмешательства со стороны пользователя.

Включение и отключение игрового режима осуществляется в главном окне программы, в области, открываемой командой **Настройка** > **Защита компьютера** или щелчком на пиктограмме  рядом с **Игровой режим**. Включая игровой режим, вы подвергаете систему угрозе, поэтому значок состояния защиты на панели задач станет оранжевого цвета, чтобы тем самым предупредить вас. Кроме того, данное предупреждение отобразится в главном окне программы, где оранжевым цветом будет отмечено **Игровой режим активен**.

Выберите элемент **Автоматически включать игровой режим при выполнении приложений в полноэкранном режиме** в разделе **Дополнительные настройки** (F5) > **Служебные программы**, чтобы игровой режим включался при запуске любого приложения в полноэкранном режиме и выключался при выходе из приложения.

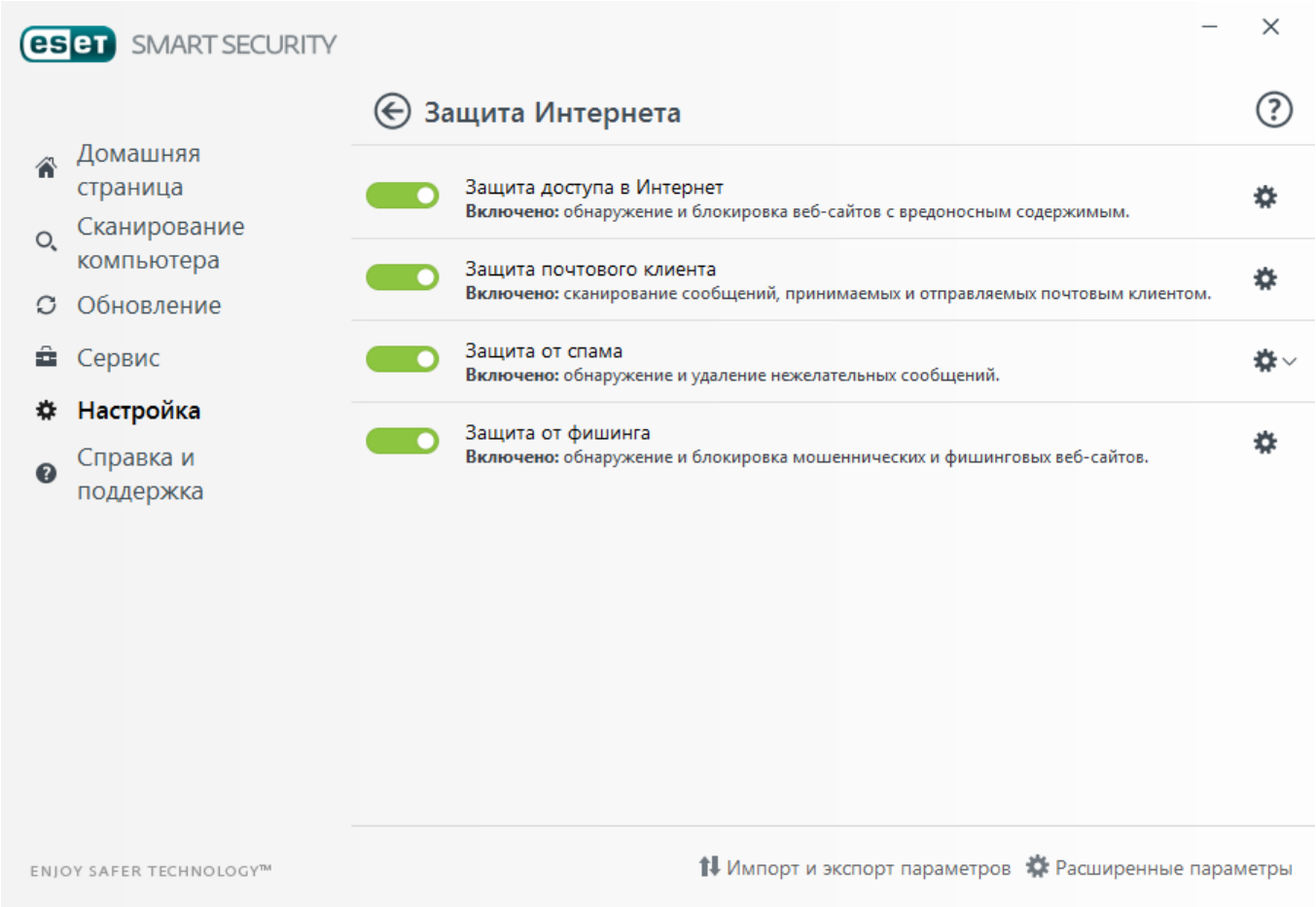
Выберите параметр **Автоматически отключать игровой режим через**, чтобы задать время, спустя которое игровой режим будет автоматически отключаться.

ПРИМЕЧАНИЕ.
Если персональный файервол работает в интерактивном режиме и включен игровой режим, возможны проблемы при подключении к Интернету. Это может представлять сложности, если запускается игра, в

которой используется подключение к Интернету. Обычно пользователю предлагается подтвердить нужное действие (если не задано никаких правил или исключений для подключения), но в игровом режиме взаимодействие с пользователем невозможно. Чтобы разрешить сетевое взаимодействие, определите правило подключения для каждого приложения, которое может его осуществлять, или используйте другой Режим фильтрации в персональном файерволе. Также следует помнить о том, что при включенном игровом режиме может быть заблокирован переход на веб-страницу или использование приложения, которые способны представлять угрозу для безопасности, но при этом на экран не будет выведено никакого пояснения или предупреждения, поскольку взаимодействие с пользователем отключено.

4.2 Защита в Интернете

Конфигурация параметров Интернета и электронной почты доступна на панели **Настройка**, которая появляется при нажатии параметра **Защита в Интернете**. В этом окне предоставляется доступ к более подробным настройкам программы.



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

Щелкните , чтобы открыть параметры защиты в Интернете/защиты электронной почты/защиты от фишинга/защиты от спама в разделе «Дополнительные настройки».

Защита почтового клиента обеспечивает контроль обмена данными электронной почты по протоколам POP3 и IMAP. При использовании подключаемого модуля для почтового клиента ESET Smart Security позволяет контролировать весь обмен данными, осуществляемый почтовым клиентом (по протоколам POP3, MAPI, IMAP, HTTP).

Функция **защиты от спама** отфильтровывает нежелательные сообщения, поступающие по электронной почте.

Если щелкнуть значок шестеренки рядом с элементом **Защита от спама**, станут доступными следующие параметры.

Настроить...: переход к дополнительным параметрам защиты почтового клиента от спама.

Белый список/**черный список**/**список исключений пользователя**: отображение диалогового окна, в котором можно добавлять, изменять или удалять адреса электронной почты, которые считаются безопасными или опасными. В соответствии с указанными здесь правилами электронные письма с этих адресов не будут сканироваться или будут считаться спамом. Щелкните элемент **Список исключений пользователя**, чтобы добавить, изменить или удалить адреса электронной почты, которые могут быть подделаны и использованы для отправки спама. Сообщения электронной почты, полученные с адресов, присутствующих в списке исключений, всегда будут сканироваться на предмет наличия спама.

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

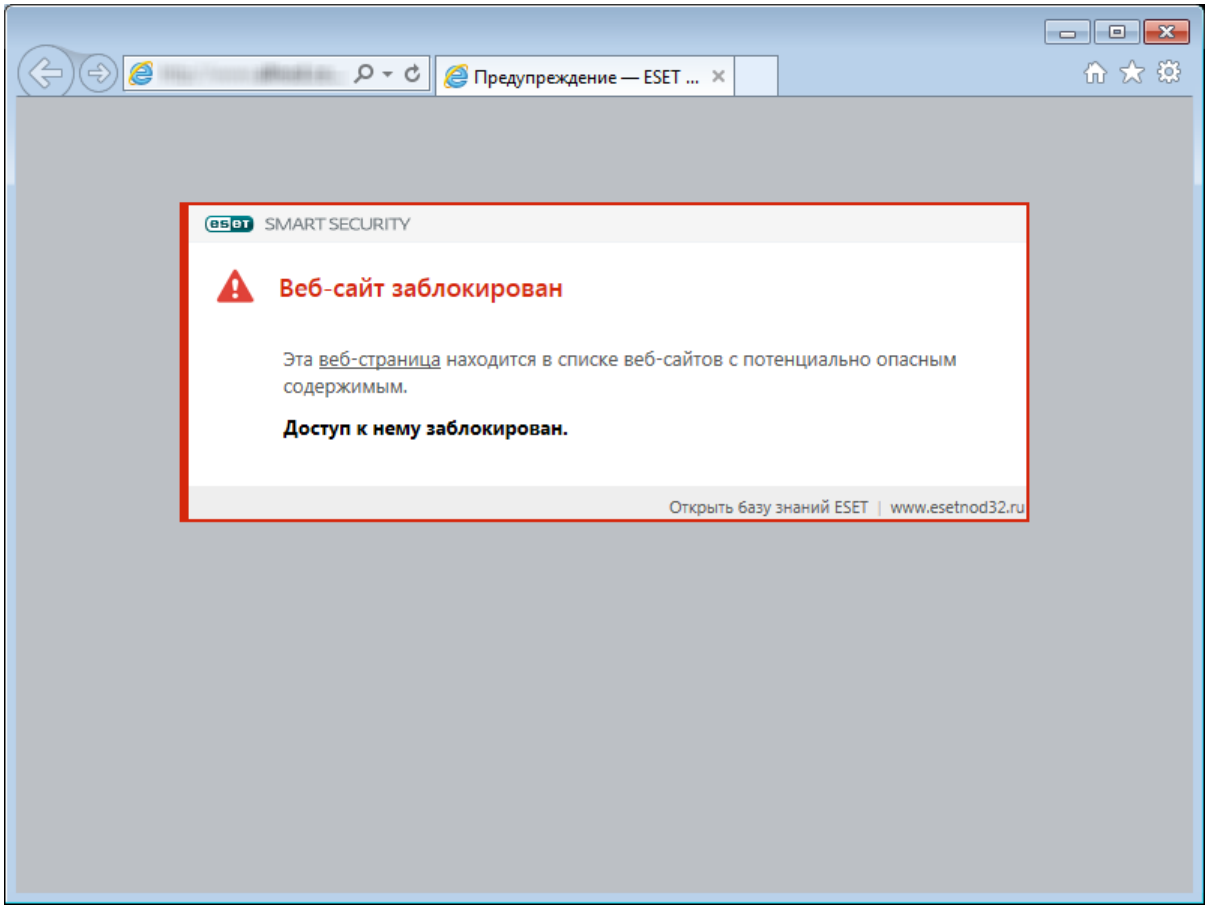
Вы можете отключить модули защиты от фишинга, /защиты от спама защиты в Интернете/защиты электронной почты на некоторое время, щелкнув пункт .

4.2.1 Защита доступа в Интернет

Подключение к Интернету стало стандартной функцией персонального компьютера. К сожалению, Интернет также стал и основной средой распространения вредоносного кода. Защита доступа в Интернет работает путем отслеживания соединений между веб-браузерами и удаленными серверами в соответствии с правилами протоколов HTTP и HTTPS.

Доступ к веб-страницам, которые содержат заведомо вредоносное содержимое, блокируется до его загрузки. Все остальные веб-страницы при загрузке сканируются модулем сканирования ThreatSense и блокируются в случае обнаружения вредоносного содержимого. Защита доступа в Интернет предполагает два уровня: блокировка на основании «черного» списка и блокировка на основании содержимого.

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



В разделе **Дополнительные настройки** (F5) > **Интернет и электронная почта** > **Защита доступа в Интернет** доступны следующие параметры.

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

4.2.1.1 Основное

Включить защиту доступа в Интернет: когда этот параметр отключен, защита доступа в Интернет и защита от фишинга не осуществляются.

Включить расширенное сканирование сценариев браузера: когда этот параметр включен, все программы на языке JavaScript, выполняемые браузерами, будут проверяться антивирусным сканером.

> **ПРИМЕЧАНИЕ**
> Настоятельно рекомендуется не отключать защиту доступа в Интернет.

4.2.1.2 Веб-протоколы

По умолчанию ESET Smart Security настроен на отслеживание протокола HTTP, используемого большинством интернет-браузеров.

Настройка модуля сканирования HTTP

В Windows Vista и более поздних версиях, HTTP-трафик отслеживается для всех портов и приложений. В операционной системе Windows XP можно вносить изменения в параметр **Порты, используемые протоколом HTTP** в окне, открываемом с помощью команды **Дополнительные настройки** (F5) > **Интернет и электронная почта** > **Защита доступа в интернет** > **Веб-протоколы**. HTTP-трафик всех приложений отслеживается по указанным портам для всех приложений и по всем портам для приложений, помеченных как веб-клиенты и почтовые клиенты.

Настройка модуля сканирования HTTPS

также поддерживает проверку протокола HTTPS. В этом типе соединения для передачи информации между сервером и клиентом используется зашифрованный канал. Программа ESET Smart Security проверяет соединения, использующие методы шифрования SSL и TLS. Программа осуществляет сканирование только тех портов, которые помечены как **Порты, используемые протоколом HTTPS**, вне зависимости от версии операционной системы.

Зашифрованные соединения не будут сканироваться. Чтобы включить сканирование зашифрованного обмена данными и просмотреть настройки модуля сканирования, перейдите к параметрам SSL/TLS в разделе «Дополнительные настройки», щелкните **Интернет и электронная почта** > **SSL/TLS** и установите флажок **Включить фильтрацию протоколов SSL/TLS**.

4.2.1.3 Управление URL-адресами

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

Посещение веб-сайтов, включенных в **Список заблокированных адресов невозможно**, кроме случаев, когда их адреса также включены в **Список разрешенных адресов**. Веб-сайты, добавленные в **Список адресов, для которых отключена проверка**, загружаются без проверки на наличие вредоносного кода.

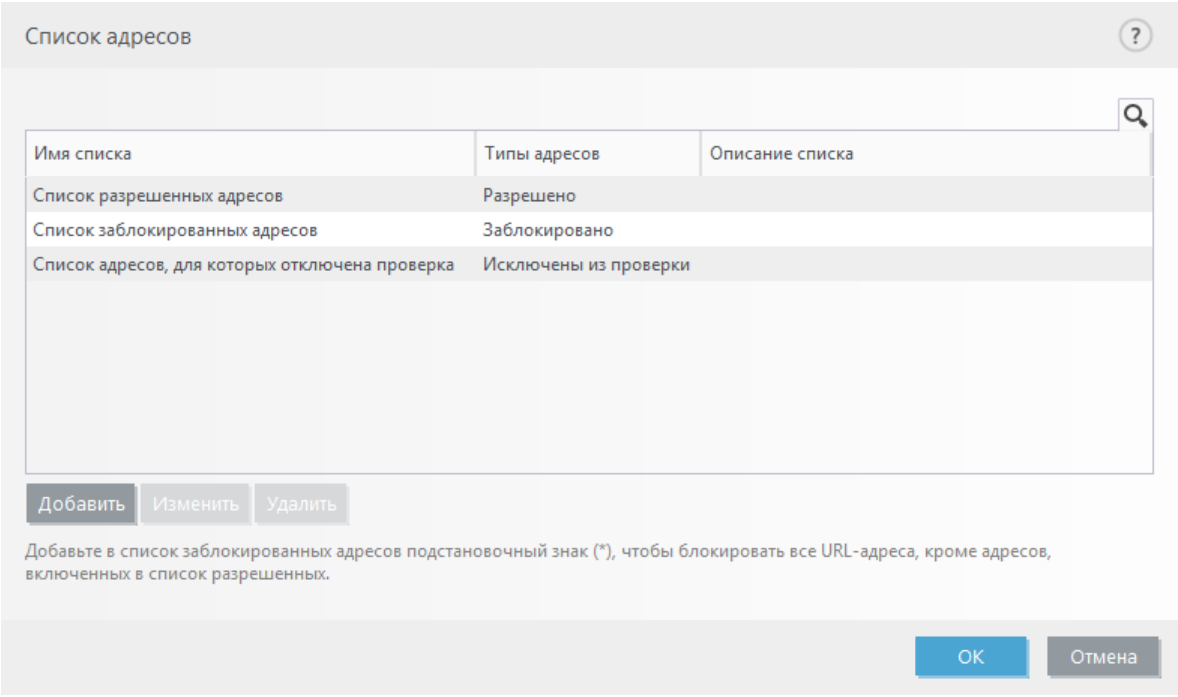
Включить фильтрацию протоколов SSL/TLS — это установка, предусмотренная на случай, когда кроме HTTP-сайтов требуется также фильтровать сайты, использующие протокол HTTPS. В противном случае в список будут добавлены только посещенные вами домены HTTPS-сайтов, а не полный URL-адрес.

Если добавить URL-адрес в **Список адресов, для которых отключена фильтрация**, этот адрес будет исключен из процесса сканирования. Также можно разрешать или блокировать определенные адреса, добавляя их соответственно в **Список разрешенных адресов** или в **Список заблокированных адресов**.

Если вы хотите заблокировать все HTTP-адреса, кроме адресов, включенных в активный **Список разрешенных адресов**, добавьте символ «*» в активный **Список заблокированных адресов**.

В списках можно использовать такие специальные символы, как «*» (звездочка) и «?» (вопросительный знак). Символ звездочки заменяет любую последовательность символов, а вопросительный знак — любой символ. Особое внимание следует уделить указанию адресов, исключенных из проверки, поскольку в этот список должны входить только доверенные и надежные 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**.

ПРИМЕЧАНИЕ.
Функция управления URL-адресами позволяет также блокировать или разрешать открытие файлов определенных типов при просмотре веб-страниц. Например, если не требуется открывать исполняемые файлы, выберите в раскрывающемся списке список, в котором хотите блокировать эти файлы, и введите маску «**.exe».



Элементы управления

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 списков. Используйте эту установку для добавления или удаления адресов.

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

4.2.2 Защита почтового клиента

4.2.2.1 Почтовые клиенты

Интеграция ESET Smart Security с вашим почтовым клиентом повышает уровень активной защиты от вредоносного кода в сообщениях электронной почты. Если используемый почтовый клиент поддерживается, в ESET Smart Security можно настроить интеграцию. Если интеграция активирована, панель инструментов ESET Smart Security добавляется непосредственно в почтовый клиент, обеспечивая более эффективную защиту электронной почты (панель инструментов для последних версий Почты Windows Live не добавляется). Параметры интеграции доступны в разделе **Дополнительные настройки** (F5) > **Интернет и электронная почта** > **Защита клиента электронной почты** > **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 **Не выполнять проверку при изменении содержимого папки "Входящие"**, если при работе с MS Outlook наблюдается замедление функционирования системы. 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 работает.
Полученные сообщения: включение или отключение проверки входящих сообщений.
Отправленные сообщения: включение или отключение проверки отправленных сообщений.
Прочитанные сообщения: включение или отключение проверки прочитанных сообщений.

Действие, применяемое к зараженному сообщению

Ничего не предпринимать: программа будет выявлять зараженные вложения, но не станет выполнять никаких действий с сообщениями электронной почты.
Удалить сообщение: программа будет уведомлять пользователя о заражениях и удалять сообщение.
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, куда будут перемещаться обнаруженные зараженные сообщения электронной почты.

Повторить сканирование после обновления: включение или отключение повторного сканирования 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.
Рекомендуется включить параметры **Включить защиту электронной почты с помощью подключаемых модулей клиента** и **Включить защиту электронной почты с помощью фильтрации протоколов**. Эти параметры доступны в разделе Дополнительные настройки (F5) > Интернет и электронная почта > Защита почтового клиента > Протоколы электронной почты).

4.2.2.2 Протоколы электронной почты

IMAP и POP3 — самые распространенные протоколы, используемые для получения электронной почты в почтовых клиентах. IMAP — это интернет-протокол для получения электронной почты, IMAP имеет определенные преимущества перед POP3. Например, сразу несколько клиентов могут одновременно подключаться к одному и тому же почтовому ящику и поддерживать сведения о состоянии сообщения, в частности о том, было ли сообщение прочитано, удалено или на него был написан ответ. ESET Smart Security обеспечивает защиту этих протоколов вне зависимости от используемого почтового клиента и без необходимости перенастраивать почтовый клиент.

Модуль защиты, обеспечивающий такой контроль, автоматически запускается при запуске системы и остается активным в памяти. Проверка протокола IMAP осуществляется автоматически без дополнительной настройки почтового клиента. По умолчанию сканируются все данные, проходящие через порт 143, но при необходимости можно добавить и другие порты. Номера портов следует разделять запятыми.

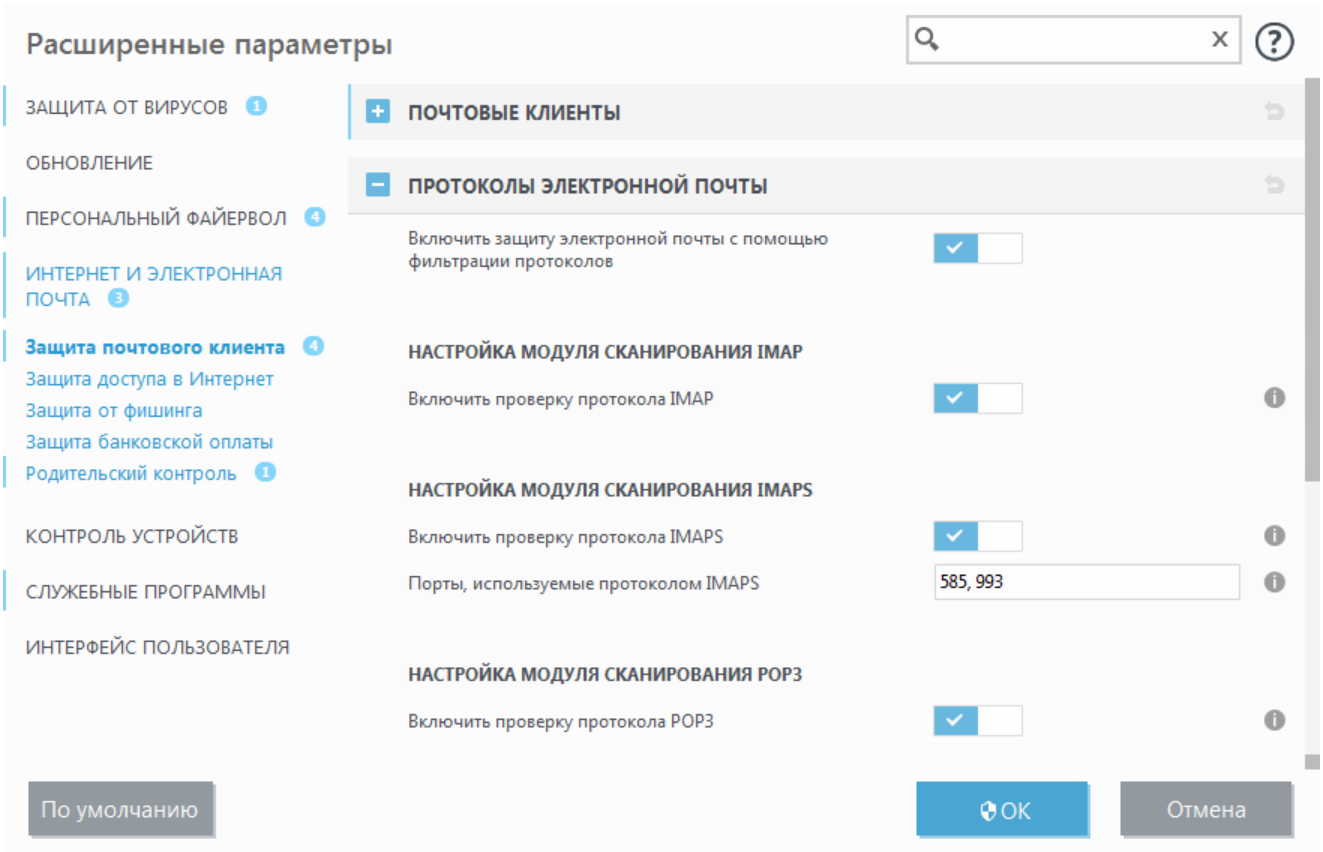
Настроить проверку протоколов IMAP/IMAPS и POP3/POP3S можно в области дополнительных настроек. Для доступа к этим настройкам последовательно выберите элементы **Интернет и электронная почта** > **Защита почтового клиента** > **Протоколы электронной почты**.

Включить защиту электронной почты с помощью фильтрации протоколов: включение проверки 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**. Кроме того, все порты сканируются для приложений, отмеченных как Веб-клиенты и почтовые клиенты.

Программа ESET Smart Security также поддерживает сканирование протоколов IMAPS и POP3S, которые для передачи информации между сервером и клиентом используют зашифрованный канал. Программа ESET Smart Security проверяет соединения, использующие методы шифрования SSL и TLS. Программа будет выполнять сканирование трафика только для портов, указанных как **Порты, используемые протоколом IMAPS или POP3S**, вне зависимости от версии операционной системы.

Зашифрованные соединения не будут сканироваться. Чтобы включить сканирование зашифрованного обмена данными и просмотреть настройки модуля сканирования, перейдите к параметрам SSL/TLS в разделе «Дополнительные настройки», щелкните **Интернет и электронная почта** > **SSL/TLS** и установите флажок **Включить фильтрацию протоколов SSL/TLS**.



4.2.2.3 Предупреждения и уведомления

Защита электронной почты обеспечивает контроль безопасности обмена данными по протоколам POP3 и IMAP. Используя подключаемый модуль для Microsoft Outlook и других почтовых клиентов, ESET Smart Security обеспечивает контроль всего обмена данными, осуществляемого 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 области **Дополнительные настройки**, раздел **Интернет и электронная почта** > **Защита почтового клиента** > **Предупреждения и уведомления**.

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 указанные ниже варианты.

- **Никогда**: уведомления не добавляются.
- **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 подсистема защиты электронной почты добавляла предупреждения о вирусах в тему зараженных сообщений. Эта функция позволяет осуществлять простую фильтрацию зараженных сообщений по теме (если поддерживается почтовым клиентом). Она также повышает уровень доверия для получателя. Если обнаружено заражение, данная функция предоставляет ценную информацию об уровне угрозы письма или отправителя.

Шаблон, добавляемый к теме зараженного письма: 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.

4.2.2.4 Интеграция с почтовыми клиентами

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

В настоящий момент поддерживаются следующие почтовые клиенты: Microsoft Outlook, Outlook Express, почта Windows, почта Windows Live. Полный список поддерживаемых почтовых клиентов и их версий см. в статье базы знаний ESET.

Установите флажок **Отключить проверку при изменении содержимого папки "Входящие"**, если при работе с почтовым клиентом наблюдается замедление работы системы. Это возможно при извлечении сообщения электронной почты из хранилища Kerio Outlook Connector Store.

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

4.2.2.4.1 Конфигурация защиты почтового клиента

Модуль защиты электронной почты поддерживает следующие почтовые клиенты: Microsoft Outlook, Outlook Express, почта Windows, 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.

4.2.2.5 Фильтр POP3, POP3S

POP3 — самый распространенный протокол, используемый для получения электронной почты в почтовых клиентах. ESET Smart Security обеспечивает защиту этого протокола вне зависимости от используемого почтового клиента.

Модуль защиты, обеспечивающий эту функцию, автоматически инициируется при запуске операционной системы и остается активным в оперативной памяти. Для нормальной работы модуля убедитесь в том, что он включен. Проверка протокола POP3 осуществляется автоматически без необходимости в настройке почтового клиента. По умолчанию сканируются все соединения по порту 110, однако при необходимости могут быть добавлены и другие порты. Номера портов следует разделять запятыми.

Зашифрованные соединения не будут сканироваться. Чтобы включить сканирование зашифрованного обмена данными и просмотреть настройки модуля сканирования, перейдите к параметрам SSL/TLS в разделе «Дополнительные настройки», щелкните **Интернет и электронная почта** > **SSL/TLS** и установите флажок **Включить фильтрацию протоколов SSL/TLS**.

В этом разделе можно конфигурировать проверку протоколов POP3 и POP3S.

Включить проверку писем: при включении этого параметра весь трафик, проходящий по протоколу POP3, проверяется на предмет наличия вредоносных программ.

Порты, используемые протоколом POP3: перечень портов, используемых протоколом POP3 (110 по умолчанию).

ESET Smart Security также поддерживает проверку протокола POP3S. В этом типе соединения для передачи информации между сервером и клиентом используется зашифрованный канал. ESET Smart Security проверяет соединения, использующие методы шифрования SSL и TLS.

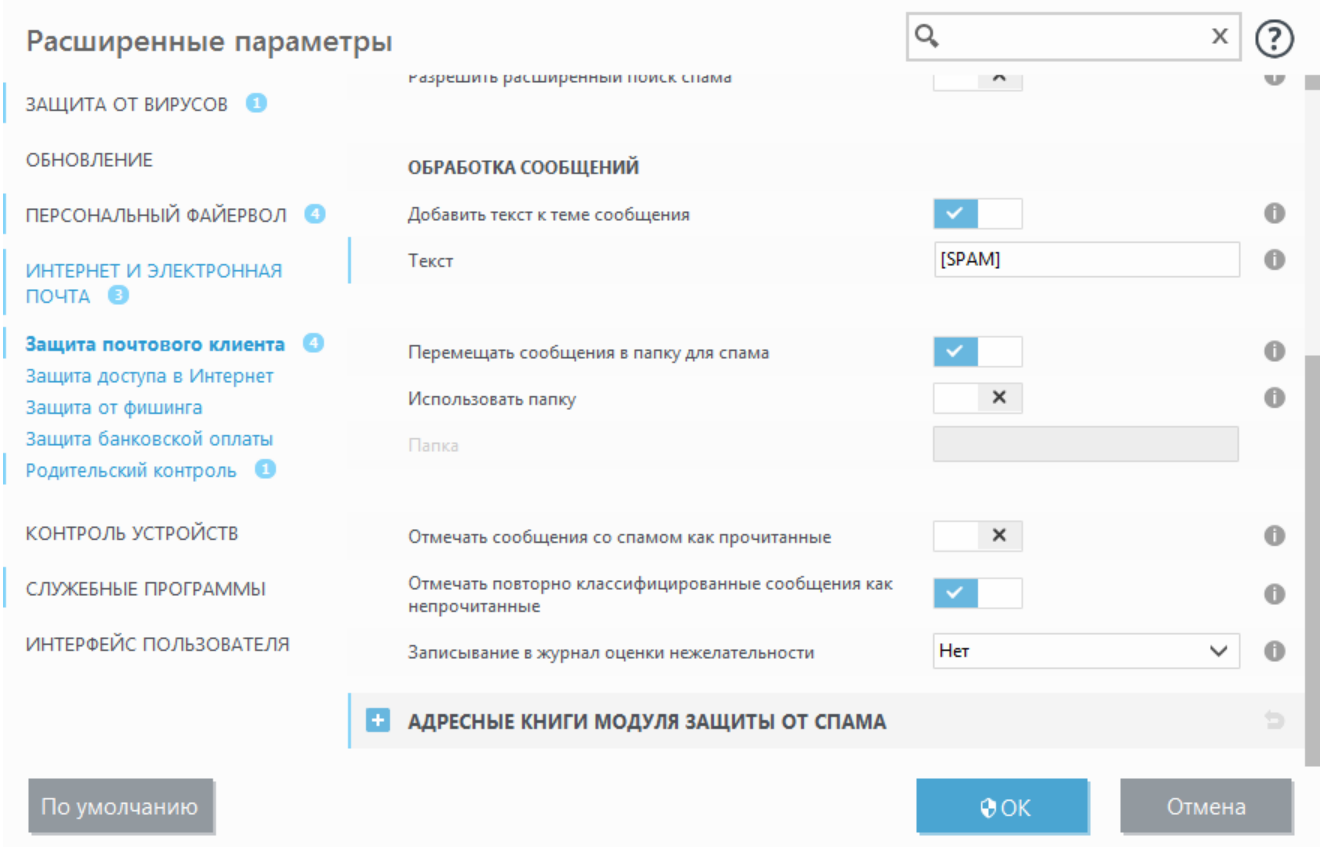
Не проверять протокол POP3S: зашифрованные соединения не будут проверяться.

Проверять протокол POP3S на указанных портах: соединения по протоколу POP3S проверяются только на портах, указанных в параметре **Используемые протоколом POP3S порты**.

Используемые протоколом POP3S порты: перечень портов, используемых протоколом POP3S, которые следует проверять (995 по умолчанию).

4.2.2.6 Защита от спама

Нежелательные сообщения, также называемые спамом, являются одной из самых серьезных проблем современных телекоммуникационных технологий. Доля спама в общем объеме передаваемых по электронной почте сообщений составляет около 80 %. Защита от спама ограждает от этой проблемы. Используя несколько принципов защиты электронной почты, модуль защиты от спама обеспечивает превосходную фильтрацию и не пропускает в папку входящих сообщений нежелательную почту.



Одним из важнейших принципов обнаружения спама является его распознавание на основе предварительно определенных списков доверенных («белый» список) и нежелательных («черный» список) адресов. Все адреса, найденные в адресной книге почтового клиента, автоматически попадают в «белый» список, а остальные адреса должны быть помечены пользователем как безопасные.

Основным методом, используемым для обнаружения спама, является сканирование свойств сообщения. Полученные сообщения сканируются на основные критерии защиты от спама (определения сообщения, статистические эвристики, алгоритмы распознавания и другие уникальные методы). Результатом работы этих методов является значение индекса, по которому можно с высокой степенью достоверности определить, является ли сообщение спамом.

Автоматически запускать модуль защиты почтового клиента от нежелательной почты: если этот флажок установлен, защита от спама будет автоматически активироваться при загрузке компьютера.

Разрешить расширенный поиск спама: периодически будут загружаться дополнительные данные, которые повышают эффективность защиты от спама.

Защита от спама в ESET Smart Security позволяет задать другие параметры для работы со списками рассылки. Доступны следующие параметры.

Обработка сообщений

Добавить текст к теме сообщения: позволяет добавлять настраиваемую строку префикса в поле темы сообщений, которые классифицированы как спам. Строка по умолчанию — [SPAM].

Перемещать сообщения в папку для спама: если этот флажок установлен, сообщения со спамом будут перемещаться в стандартную папку для нежелательной почты, а сообщения, повторно классифицированные как не являющиеся спамом, — в папку со входящей почтой. Если щелкнуть сообщение правой кнопкой мыши и выбрать в контекстном меню пункт ESET Smart Security, появится возможность выбрать один из нескольких вариантов действий.

Использовать эту папку: этот параметр позволяет перемещать спам в папку, указанную пользователем.

Отмечать сообщения со спамом как прочитанные: установите этот флажок, чтобы автоматически помечать нежелательные сообщения как прочитанные. Это помогает сосредоточиться на «чистых» сообщениях.

Отмечать повторно классифицированные сообщения как непрочитанные: сообщения, первоначально классифицированные как спам, а затем помеченные как «чистые», будут отображаться как непрочитанные.

Регистрация оценки нежелательности Модуль защиты от спама ESET Smart Security присваивает каждому просканированному сообщению оценку нежелательности. Данное сообщение будет записано в журнал защиты от спама (**ESET Smart Security** > **Служебные программы** > **Файлы журнала** > **Защита от спама**).

- **Нет**: оценка, полученная в результате сканирования на предмет спама, не вносится в журнал.
- **Реклассифицировано и помечено как спам**: если выбран этот параметр, оценки нежелательности всех сообщений, помеченных как спам, будут записываться в журнал.
- **Все**: в журнал будут записываться все сообщения вместе с оценкой нежелательности.

ПРИМЕЧАНИЕ
Если в папке нежелательной почты выделить сообщение и выбрать команду **Классифицировать выбранные сообщения как НЕ спам**, это сообщение будет перемещено в папку входящей почты. Если в папке входящих сообщений выделить сообщение, которые вы считает нежелательным, и выбрать команду **Классифицировать сообщения как спам**, сообщение будет перемещено в папку спама. Это же действие можно выполнить сразу с несколькими выделенными сообщениями.

ПРИМЕЧАНИЕ.
ESET Smart Security обеспечивает защиту от спама в таких почтовых приложениях: Microsoft Outlook, Outlook Express, Почта Windows и Почта Windows Live.

4.2.3 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/TLS**.

Включить фильтрацию содержимого, передаваемого по протоколам приложений: может использоваться для отключения фильтрации протоколов. Учтите, что многие компоненты ESET Smart Security (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, если фильтрация протоколов вызывает проблемы совместимости.

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

Веб-клиенты и почтовые клиенты: используется только в операционных системах Windows XP и позволяет выбирать приложения, трафик которых будет подвергаться фильтрации протоколов, вне зависимости от используемого порта.

4.2.3.1 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.

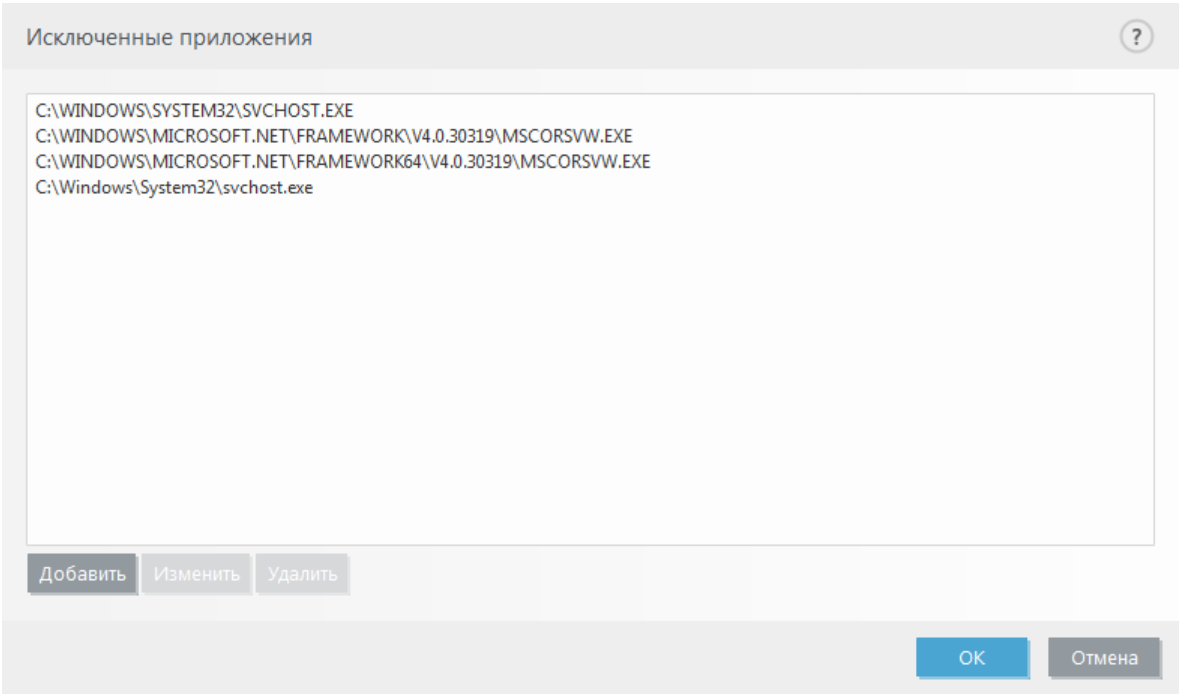
В условиях перенасыщенности Интернета вредоносными программами безопасное посещение веб-страниц является важным аспектом защиты компьютера. Уязвимости веб-браузеров и мошеннические ссылки позволяют вредоносным программам незаметно проникать в систему. Именно поэтому в программном обеспечении ESET Smart Security основное внимание уделяется обеспечению безопасности веб-браузеров. Каждое приложение, обращающееся к сети, может быть помечено как веб-браузер. Флажок имеет два состояния.

- **Не установлен**: подключения приложений фильтруются только для указанных портов.
- **Установлен**: подключения всегда фильтруются (даже если задан другой порт).

4.2.3.2 Исключенные приложения

Для исключения соединений определенных сетевых приложений из фильтрации содержимого выделите их в списке. Соединения выделенных приложений по протоколам HTTP/POP3/IMAP не будут проверяться на наличие угроз. Рекомендуется использовать эту возможность только для тех приложений, которые работают некорректно, если их соединения проверяются.

Запуск приложений и служб будет доступен автоматически. Нажмите кнопку **Добавить**, чтобы вручную выбрать приложение, отсутствующее в списке фильтрации протоколов.

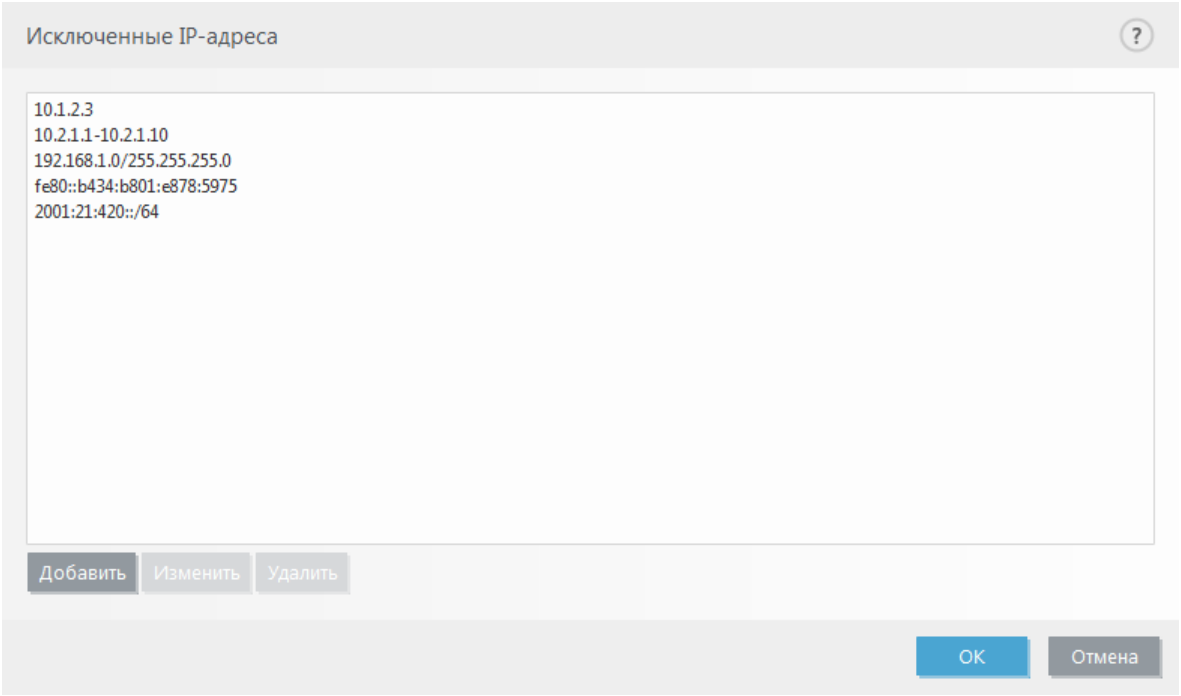


4.2.3.3 Исключенные IP-адреса

Записи в 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.

Нажмите кнопку **Добавить**, чтобы исключить IP-адрес, диапазон адресов или подсеть удаленного узла, не отображаемого в списке фильтрации протокола.

Нажмите кнопку **Удалить**, чтобы удалить выделенные записи из списка.



4.2.3.3.1 Добавить адрес IPv4

Этот функция позволяет добавить IP-адрес, диапазон адресов или маску подсети удаленной конечной точки, к которой должно быть применено правило. Интернет-протокол версии 4 (IPv4) — это устаревшая версия, но она до сих пор широко используется.

Отдельный адрес: добавляет IP-адрес отдельного компьютера, для которого должно быть применено правило (например, *192.168.0.10*).

Диапазон адресов: введите начальный и конечный IP-адреса, чтобы задать тем самым диапазон IP-адресов (или несколько компьютеров), к которым следует применить правило (например, от *192.168.0.1* до *192.168.0.99*).

Подсеть: подсеть (группа компьютеров), заданная IP-адресом и маской.

Например, *255.255.255.0* — это маска сети для префикса *192.168.1.0/24*, который означает диапазон адресов от *192.168.1.1* до *192.168.1.254*.

4.2.3.3.2 Добавить адрес IPv6

Этот функция позволяет добавить IPv6-адрес или маску подсети удаленной конечной точки, к которой должно быть применено правило. Это новейшая версия интернет-протокола, и в будущем она заменит более старую версию 4.

Отдельный адрес: добавляет IP-адрес отдельного компьютера, для которого должно быть применено правило (например, *2001:718:1c01:16:214:22ff:fec9:ca5*).

Подсеть: подсеть (группа компьютеров), заданная IP-адресом и маской (например, *2002:c0a8:6301:1::1/64*).

4.2.3.4 SSL/TLS

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 протокола SSL: если фильтрация протокола отключена, программа не сканирует обмен данными по протоколу SSL.

Режим фильтрации протоколов SSL/TLS доступен со следующими параметрами.

Автоматический режим: используемый по умолчанию режим, в котором сканируются только соответствующие приложения, такие как браузеры и почтовые клиенты. Его можно переопределить, выбрав приложения, для которых будет сканироваться передача данных.

Интерактивный режим: при выполнении входа на новый защищенный SSL-сайт (с неизвестным сертификатом) на экран выводится диалоговое окно выбора действия. Этот режим позволяет создавать список сертификатов SSL и приложений, исключаемых из сканирования.

Режим политики: выберите этот вариант, чтобы сканировать все защищенные SSL-соединения, кроме тех, что защищены исключенными из проверки сертификатами. Если устанавливается новое соединение, использующее неизвестный заверенный сертификат, пользователь не получит уведомления, а само соединение автоматически будет фильтроваться. При доступе к серверу с ненадежным сертификатом, который помечен пользователем как доверенный (добавлен в список доверенных сертификатов), соединение с этим сервером разрешается, а содержимое канала связи фильтруется.

Список приложений, отфильтрованных с помощью SSL: позволяет настраивать поведение ESET Smart Security для заданных приложений.

Список известных сертификатов: позволяет настроить поведение ESET Smart Security в отношении конкретных сертификатов SSL.

Исключить обмен данными, защищенный с помощью сертификатов высокой надежности (EV): когда этот параметр включен, обмен данными с таким типом сертификата SSL будет исключен из проверки. SSL-сертификаты высокой надежности гарантируют, что осуществляется просмотр именно требуемого сайта, а не идентично выглядящего поддельного (обычно поддельными бывают фишинговые сайты).

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

Корневой сертификат

Добавить корневой сертификат в известные браузеры: для нормальной работы SSL-подключений в браузерах и почтовых клиентах необходимо добавить корневой сертификат ESET в список известных корневых сертификатов (издателей). При включении этого параметра ESET Smart Security автоматически добавляет 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 последовательно выберите элементы **Просмотреть сертификат** > **Дополнительно** > **Копировать в файл...**, а затем вручную импортируйте этот сертификат 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 центров сертификации. 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 недопустимая подпись. В этом случае рекомендуется выбрать **Блокировать соединения, использующие сертификат**.

4.2.3.4.1 Сертификаты

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, 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.

В некоторых случаях сертификат невозможно проверить с помощью хранилища доверенных корневых сертификатов сертифицирующих органов (например, VeriSign). 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. На экране отобразится диалоговое окно для выбора действия, в котором можно принять решение о том, что следует сделать: пометить сертификат как доверенный или как исключенный. Если сертификат отсутствует в списке хранилища доверенных корневых сертификатов сертифицирующих органов, для оформления окна используется красный цвет. Если же сертификат есть в этом списке, окно будет оформлено зеленым цветом.

Можно выбрать вариант **Блокировать соединения, использующие сертификат**, чтобы всегда разрывать зашифрованные соединения с сайтом, использующим непроверенный сертификат.

Если этот сертификат недействителен или поврежден, это значит, что истек срок действия сертификата или же используется неверное собственное заверение. В этом случае рекомендуется блокировать соединения, использующие данный сертификат.

4.2.3.4.1.1 Зашифрованный сетевой трафик

Если компьютер сканирует соединения, использующие протокол SSL, при попытке установить зашифрованное соединение (с использованием неизвестного сертификата) на экран может быть выведено диалоговое окно, предлагающее выбрать действие.

Это диалоговое окно содержит следующие данные:

- имя приложения, которое инициировало обмен данными;
- имя используемого сертификата;
- выполняемое действие: нужно выбрать, сканировать ли зашифрованное соединение и запоминать ли действие для приложения либо сертификата.

Если сертификат не находится в хранилище доверенных корневых центров сертификации, он считается ненадежным.

4.2.3.4.2 Список известных сертификатов

Список известных сертификатов позволяет настроить поведение ESET Smart Security в отношении конкретных сертификатов SSL, а также настроить запоминание действий пользователя, если в режиме **Фильтрация 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**.

В окне **Список известных сертификатов** имеются перечисленные ниже элементы.

Столбцы

Имя: имя сертификата.

Издатель сертификата: имя создателя сертификата.

Субъект сертификата: в этом поле указывается субъект, которому принадлежит открытый ключ, содержащийся в поле открытого ключа субъекта.

Доступ: в качестве значения параметра **Действие доступа** выберите установку **Разрешить** или **Заблокировать**, чтобы разрешить или заблокировать обмен данными, защищенный этим сертификатом, вне зависимости от его надежности. Выберите установку **Автоматически**, чтобы разрешать доверенные сертификаты и предлагать варианты действий для ненадежных. Выберите **Запрашивать**, чтобы всегда запрашивать действия пользователя.

Сканировать: чтобы сканировать или игнорировать соединение, защищенное сертификатом, выберите значение **Сканировать** или **Пропустить для параметра Действие сканирования**. Выберите установку **Автоматически**, чтобы сканирование выполнялось в автоматическом режиме, а запрос действия — в интерактивном. Чтобы программа всегда запрашивала у пользователя, какое действие следует выполнить, выберите установку **Запрашивать**.

Элементы управления

Добавить — выбор нового сертификата и настройка его параметров, связанных с доступом и сканированием.

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

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

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

4.2.3.4.3 Список приложений, отфильтрованных с помощью SSL/TLS

Список приложений, отфильтрованных с помощью SSL/TLS, может использоваться для настройки поведения ESET Smart Security в отношении конкретных приложений, а также запоминания выбранных действий, если в режиме **Фильтрация протоколов SSL/TLS** выбран **интерактивный режим**. Список можно просмотреть и отредактировать, последовательно выбрав элементы **Дополнительные настройки** (F5) > **Интернет и электронная почта** > **SSL/TLS** > **Список приложений, отфильтрованных с помощью SSL/TLS**.

В окне **Список приложений, отфильтрованных с помощью SSL/TLS** имеются перечисленные ниже элементы.

Столбцы

Приложение: имя приложения.

Действие сканирования: Выберите **Сканировать** или **Пропустить**, чтобы сканировать или игнорировать обмен данными. Выберите установку **Автоматически**, чтобы сканирование выполнялось в автоматическом режиме, а запрос действия — в интерактивном. Чтобы программа всегда запрашивала у пользователя, какое действие следует выполнить, выберите установку **Запрашивать**.

Элементы управления

Добавить: добавление фильтрованных приложений.

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

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

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

4.2.4 Защита от фишинга

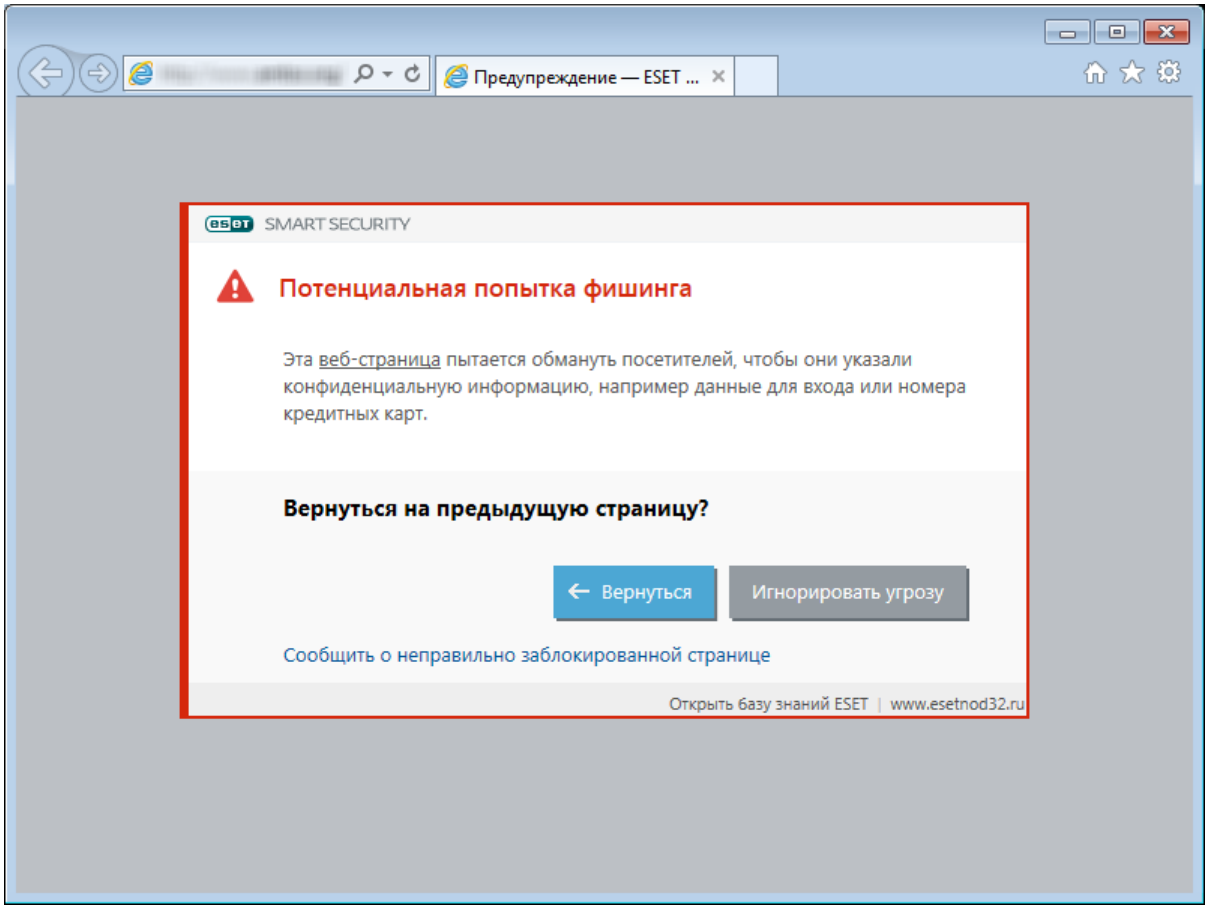
Термин «фишинг» обозначает преступную деятельность, в рамках которой используется социальная инженерия (манипулирование пользователями, направленное на получение конфиденциальной информации). Фишинг часто используется для получения доступа к конфиденциальным сведениям, таким как номера банковских счетов,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

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

В статье нашей базы знаний приведены дополнительные сведения о защите от фишинга в программе ESET Smart Security.

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 **Игнорировать угрозу** (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:

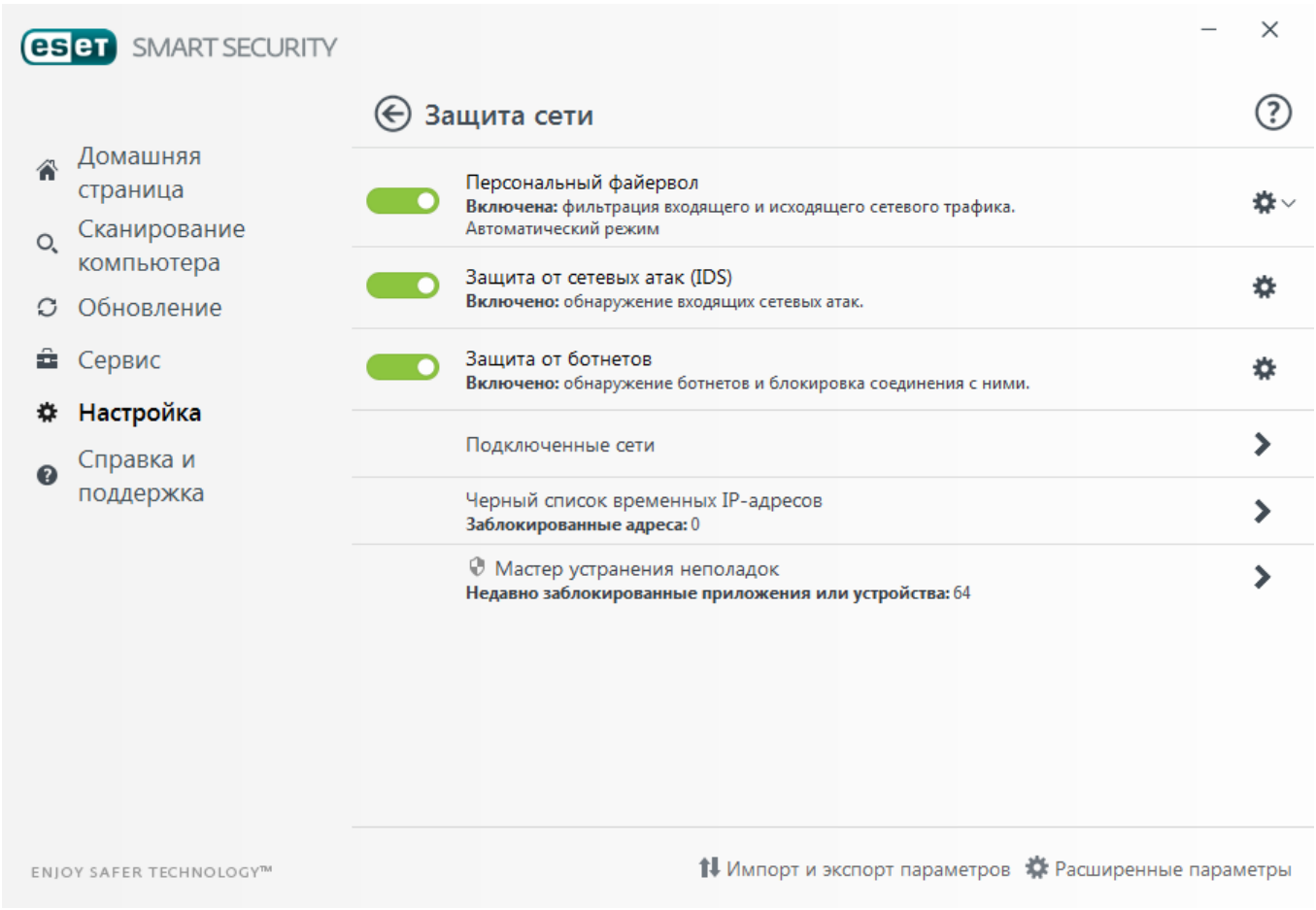
- веб-сайт совсем не обнаруживается;
- веб-сайт неправильно обнаруживается как угроза. В таком случае можно сообщить о ложной метке фишингового сайта.

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.).

4.3 Защита сети

Персональный файервол управляет всем сетевым трафиком компьютера в обоих направлениях. Процесс основан на разрешении или запрете отдельных сетевых соединений в соответствии с правилами фильтрации. Персональный файервол обеспечивает противодействие сетевым атакам со стороны удаленных компьютеров и разрешает блокирование некоторых служб. Кроме того, он обеспечивает защиту от вирусов при обмене данными по протоколам HTTP, POP3 и IMAP. Функционально модуль является очень важным элементом в системе компьютерной безопасности.

Конфигурация персонального файервола доступна в области **Настройка** в меню **Защита сети**. Здесь можно изменять режим фильтрации, правила и дополнительные параметры. Также можно получить доступ к дополнительным настройкам, щелкнув значок шестеренки > **Настроить...** рядом с элементом **Персональный файервол** или нажав клавишу **F5**, которая вызывает меню Дополнительные настройки.



Щелкните значок шестеренки ⚙ рядом с элементом **Персональный файервол**, чтобы открыть следующие настройки.

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

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

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

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

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

Защита от сетевых атак (IDS) анализ содержимого сетевого трафика и защита от сетевых атак. Трафик, который расценивается как опасный, блокируется.

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

Подключенные сети: отображение сетей, к которым подключены сетевые адаптеры. После нажатия ссылки, расположенной под именем сети, вам будет предложено выбрать тип защиты (максимальная или разрешенная) для сети, к которой вы подключены с помощью сетевого адаптера. Этим параметром определяется возможность доступа других компьютеров сети к вашему устройству.

Временный черный список IP-адресов: отображение списка IP-адресов, которые были обнаружены как источники атак и добавлены в черный список для блокировки соединения в течение определенного периода времени. Чтобы получить дополнительную информацию, выберите этот параметр, а затем нажмите F1.

Мастер устранения неполадок: помощь в устранении проблем с подключением, вызванных персональным файерволом ESET. Для получения дополнительных сведений см. раздел Мастер устранения неполадок.

4.3.1 Персональный файервол

Персональный файервол управляет всем входящим и исходящим сетевым трафиком компьютера. Процесс основан на запрете или разрешении отдельных сетевых соединений в соответствии с определенными правилами. Персональный файервол обеспечивает защиту от атак со стороны удаленных компьютеров и может блокировать потенциально опасные службы. Он также предоставляет защиту от вирусов для протоколов HTTP, POP3 и IMAP.

Основная информация

Включить персональный файервол: рекомендуется оставить эту функцию включенной, чтобы обеспечить защиту системы. При включенном файерволе сетевой трафик сканируется в обоих направлениях.

Включить защиту от сетевых атак (IDS) анализ содержимого сетевого трафика и защита от сетевых атак. Любой трафик, который расценивается как опасный, блокируется.

Включить защиту от ботнетов. Обнаружение и блокирование подключений, связанных со вредоносными командами и управляющими серверами путем распознавания шаблонов, указывающих, что компьютер инфицирован и бот пытается подключаться осуществить сетевое взаимодействие.

Включить защиту домашней сети: защищает компьютеры от входящих сетевых (Wi-Fi) угроз.

Уведомлять о новых сетевых устройствах: уведомляет вас, когда в сети обнаруживается новое устройство.

Дополнительно

Режим фильтрации: поведение персонального файервола зависит от режима фильтрации. Кроме того, от выбранного режима фильтрации зависит степень участия пользователя в процессе. Персональный файервол ESET Smart Security поддерживает следующие режимы фильтрации.

Автоматический режим: режим по умолчанию. Этот режим подходит для пользователей, которым нравится простота и удобство использования персонального файервола, а также отсутствие необходимости создавать правила. В режиме по умолчанию можно создавать пользовательские правила, однако это не необходимо. В автоматическом режиме разрешен весь исходящий трафик системы и блокируется большая часть входящего трафика — кроме некоторого трафика из доверенной зоны (как указано в разделе IDS и расширенные параметры/Разрешенные службы) и ответов на недавний исходящий трафик.

Интерактивный режим: позволяет создать собственную конфигурацию персонального файервола. Если обнаружено соединение, на которое не распространяется ни одно из существующих правил, на экран выводится диалоговое окно с уведомлением о неизвестном подключении. В этом окне можно запретить или разрешить соединение, а также на основе этого решения создать правило для применения в будущем. Если принимается решение о создании нового правила, в соответствии с этим правилом все будущие соединения этого типа будут разрешены или запрещены.

Режим на основе политики: блокируются все соединения, не удовлетворяющие ни одному из ранее определенных разрешающих правил. Этот режим предназначен для опытных пользователей, которые могут создавать правила, разрешающие только нужные и безопасные соединения. Все прочие неуказанные соединения будут блокироваться персональным файерволом.

Режим обучения: правила создаются и сохраняются автоматически. Этот режим лучше всего подходит для первоначальной настройки персонального файервола, но его не следует оставлять надолго. Участие пользователя не требуется, потому что ESET Smart Security сохраняет правила согласно предварительно настроенным параметрам. Во избежание рисков для безопасности режим обучения следует использовать лишь до тех пор, пока не будут созданы все необходимые для сетевого взаимодействия правила.

Профили можно использовать для настройки поведения персонального файервола ESET Smart Security, указывая разные наборы правил для разных ситуаций.

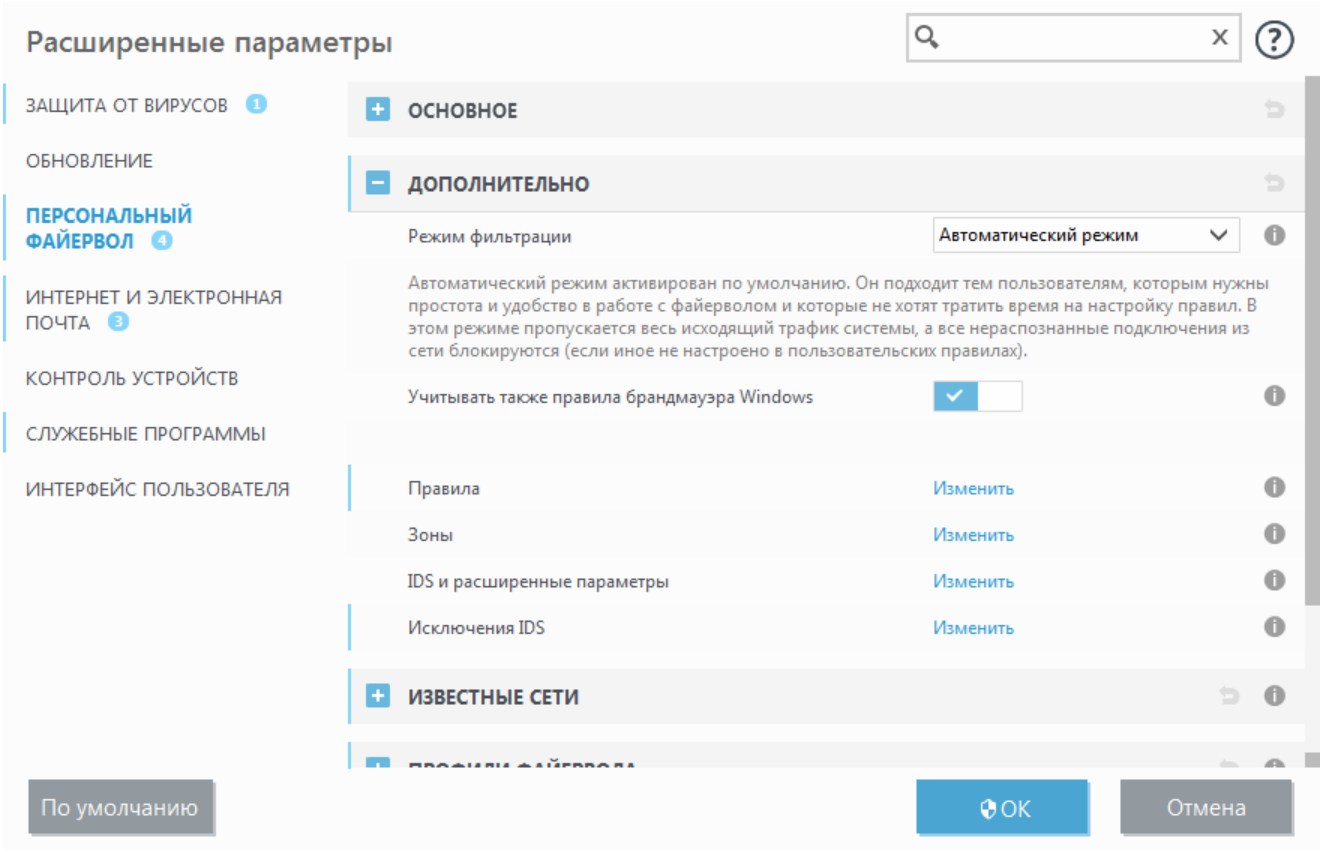
Учитывать также правила брандмауэра windows: если этот параметр включен, то в автоматическом режиме разрешен входящий трафик, разрешенный файерволом Windows и не заблокированный правилами персонального файервола.

Правила: добавление правил и управление тем, как персональный файервол обрабатывает сетевой трафик.

Зоны: создание зон, включающих один или более надежных IP-адресов.

IDS и расширенные параметры: настройка расширенных параметров фильтрации и функциональности системы IDS (используется для обнаружения некоторых типов атак и эксплойтов).

Исключения IDS: добавление исключений IDS и настройка способов реагирования на вредоносные действия.



ПРИМЕЧАНИЕ.
Если ботнет атакует ваш компьютер, можно создать исключение IDS. Исключение можно изменить в окне **Дополнительные настройки** (F5) > **Персональный файервол** > **Дополнительно** > **Исключения IDS**, нажав кнопку **Изменить**.

4.3.1.1 Настройки режима обучения

В режиме обучения правила для каждого соединения, установленного системой, создаются и сохраняются автоматически. Участие пользователя не требуется, потому что ESET Smart Security сохраняет правила согласно предварительно настроенным параметрам.

Использование этого режима может представлять риск для системы, и его рекомендуется использовать только для первоначальной настройки персонального файервола.

Для отображения настроек режима обучения активируйте его в разделе **Дополнительные настройки** (F5) > **Персональный файервол** > **Настройки режима обучения**. В этом разделе представлены следующие параметры.

ВНИМАНИЕ!
В режиме обучения персональный файервол не фильтрует соединения. Разрешены все исходящие и входящие соединения. В этом режиме компьютер защищен персональным файерволом не полностью.

Тип соединения: настройка отдельных параметров создания правил для каждого типа соединений. Существует четыре типа соединений.

- **Трафик, входящий из доверенной зоны**: примером входящего соединения в доверенной зоне является удаленный компьютер, находящийся в пределах доверенной зоны, который пытается установить соединение с приложением, запущенном на локальном компьютере.

- **Трафик, исходящий в доверенную зону**: приложение на локальном компьютере пытается установить соединение с другим компьютером в пределах локальной сети или сети в доверенной зоне.

- **Входящий интернет-трафик**: удаленный компьютер пытается установить соединение с приложением, запущенным на локальном компьютере.

- **Исходящий интернет-трафик**: приложение на локальном компьютере пытается установить соединение с другим компьютером.

В каждом разделе определяются параметры, которые будут добавляться к новым правилам.

Добавить локальный порт: включает номер локального порта сетевого соединения. Для исходящих соединений обычно создаются случайные номера, поэтому данный параметр рекомендуется включать только для входящих соединений.

Добавить приложение: включает имя локального приложения. Данный параметр предназначен для использования в будущих правилах на уровне приложений (правилах, определяющих соединения для всего приложения). Например, можно разрешить соединения только для веб-браузера или почтового клиента.

Добавить удаленный порт: включает номер удаленного порта сетевого соединения. Например, можно разрешить или запретить соединение для определенной службы по стандартному порту (HTTP — 80, POP3 — 110 и т. д.).

Добавить удаленный IP-адрес / доверенную зону: IP-адрес удаленного узла или имя зоны могут использоваться в качестве параметра при создании новых правил, определяющих все сетевые соединения между локальной системой и соответствующим удаленным узлом или зоной. Этот параметр используются при определении действия для конкретного компьютера или группы сетевых компьютеров.

Максимальное количество разных правил для одного приложения: для приложения, обменивающегося данными через разные порты, с различными IP-адресами и т. п., в режиме обучения файервола создается соответствующее количество правил. Данный параметр позволяет ограничить число правил, которые могут быть созданы для одного приложения.

4.3.2 Профили файервола

Использование профилей позволяет контролировать поведение персонального файервола ESET Smart Security. Создавая или изменяя правила персонального файервола, можно назначать их отдельному профилю или применять ко всем профилям. При выборе определенного профиля действуют только глобальные правила (правила без указания профиля) и правила, назначенные этому профилю. Возможность создать несколько профилей с разными правилами для сетевых адаптеров или сетей позволят с легкостью изменять поведение файервола.

Нажмите кнопку **Изменить**, расположенную рядом с элементом Список профилей. Откроется окно **Профили файервола**, в котором можно вносить изменения в профили.

Сетевой адаптер можно настроить таким образом, чтобы при подключении к конкретной сети он использовал сконфигурированный для нее профиль. Кроме того, можно указать конкретный профиль, который будет использоваться для определенной сети, для чего следует выбрать элементы **Дополнительные настройки** (F5) > **Персональный файервол** > **Известные сети**. Выберите сеть из списка **Известные сети** и щелкните **Изменить**, чтобы назначить профиль файервола для конкретной сети из раскрывающегося меню **Профиль файервола**. С сетями, для которых не был назначен профиль, будет использоваться профиль адаптера по умолчанию. Если адаптер не настроен на использование профиля сети, будет использоваться его профиль по умолчанию вне зависимости от того, к какой сети он подключен. Если в настройках сети или адаптера не указан профиль, применяется глобальный профиль по умолчанию. Чтобы назначить профиль сетевому адаптеру, выберите этот адаптер и нажмите кнопку **Изменить**, расположенную рядом с элементом **Профили, назначаемые**

сетевым адаптерам, затем отредактируйте сведения о выбранном адаптере и выберите профиль в раскрывающемся списке **Профиль файервола по умолчанию**.

При переключении профилей персонального файервола в правом нижнем углу экрана рядом с системными часами появляется соответствующее уведомление.

4.3.2.1 Профили, назначаемые сетевым адаптерам

Переключая профили, можно быстро изменять поведение файервола. Для определенных профилей могут быть установлены и применяться пользовательские правила. Записи для всех сетевых адаптеров компьютера автоматически добавляются в список **Сетевые адаптеры**.

Столбцы

Имя: имя сетевого адаптера.

Профиль файервола по умолчанию: профиль по умолчанию используется при подключении к сети, для которой отсутствует настроенный профиль или отключено использование сетевого профиля адаптером.

Предпочитаемый профиль сети: если параметр **Предпочитаемый профиль сети** включен, сетевой адаптер по возможности использует профиль файервола, назначенный для подключенной сети.

Элементы управления

Добавить: добавление нового сетевого адаптера.

Изменить: изменение существующего сетевого адаптера.

Удалить: выберите сетевой адаптер и щелкните **Удалить**, чтобы удалить его из списка.

ОК/Отмена: нажмите кнопку **ОК**, чтобы сохранить изменения, или кнопку **Отмена**, чтобы их отменить.

4.3.3 Настройка и использование правил

Правило содержит набор параметров и условий, которые позволяют целенаправленно проверять сетевые соединения и выполнять необходимые действия в соответствии с этими условиями. С помощью правил персонального файервола можно задать действия, которые выполняются при установке сетевых соединений различных типов. Для того чтобы настроить правило фильтрации, перейдите в окно **Дополнительные настройки** (F5) > **Персональный файервол** > **Основное**. Некоторые предопределенные правила связаны с флажками из **разрешенных служб** (IDS и расширенные функции) и не могут быть отключены напрямую, вместо этого для их отключения необходимо снять связанные с ними флажки.

В отличие от предыдущей версии ESET Smart Security, правила обрабатываются сверху вниз. Действие, определяемое первым соответствующим правилом, используется для каждого обрабатываемого сетевого соединения. Это важное изменение в поведении по сравнению с предыдущей версией продукта, где приоритет определялся автоматическим и был выше у более специфических правил, чем у более общих.

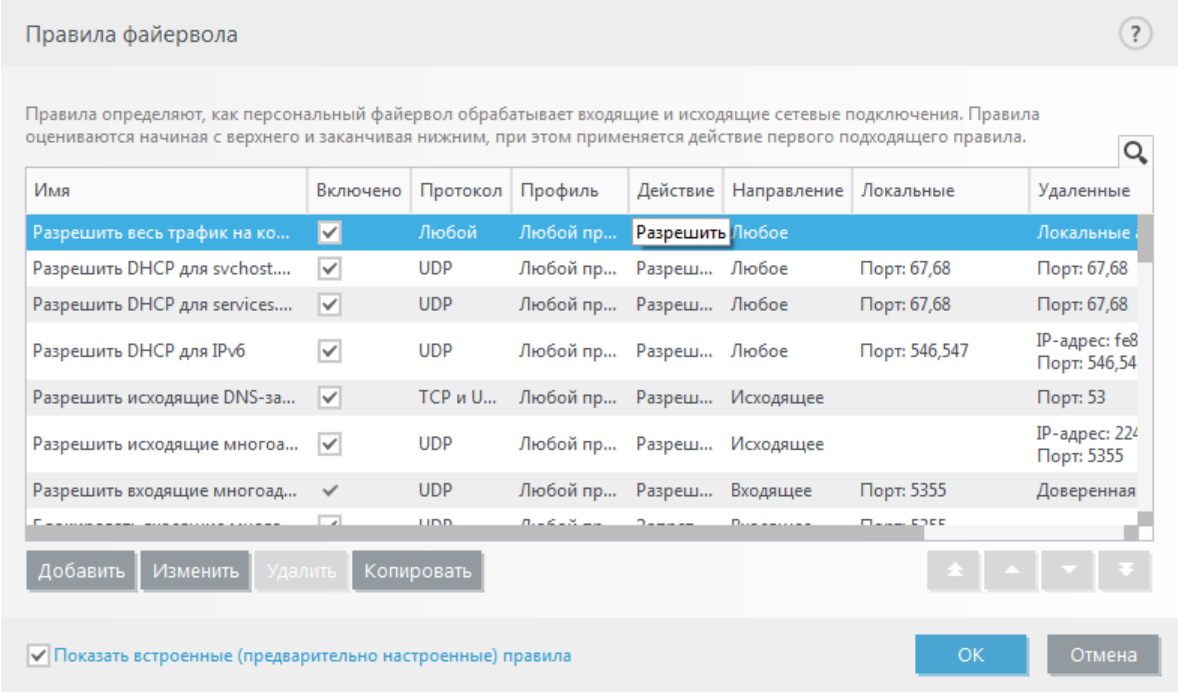
Подключения можно разделить на входящие и исходящие. Входящие подключения инициируются удаленным компьютером, который пытается подключиться к локальной системе. При исходящим соединении, наоборот, локальный компьютер пытается подключиться к удаленному.

При возникновении неизвестного соединения пользователь должен разрешить или запретить его. Нежелательные, небезопасные или неизвестные соединения несут угрозу безопасности для компьютера. При установлении такого соединения рекомендуется обратить особое внимание на удаленный компьютер и приложение, которые пытаются установить это соединение с компьютером. Многие типы заражений пытаются получить и отправить личные данные или загрузить другие злонамеренные приложения на компьютер. Персональный файервол дает пользователю возможность обнаружить и разорвать такие подключения.

4.3.3.1 Правила файервола

На вкладке **Основные сведения** рядом с элементом **Правила** нажмите кнопку **Изменить**, чтобы открыть окно **Правила файервола**, в котором представлен список всех правил. **Добавить**, **Изменить** и **Удалить** — это кнопки для добавления, настройки и удаления правил. Изменить уровень приоритета правила можно с помощью кнопок **В начало/Вверх/Вниз/В конец**.

ПОДСКАЗКА. Поле **Поиск** служит для поиска правил по имени, протоколу или порту.



Столбцы

Имя: имя правила.

Включено: сведения о том, включены ли правила. Для активации правила необходимо установить соответствующий флажок.

Протокол: сведения о протоколе, для которого используется данное правило.

Профиль: сведения о профиле файервола, для которого используется данное правило.

Действие: сведения о состоянии подключения (блокировать/разрешить/спрашивать).

Направление: направление соединения (входящее/исходящее/оба).

Локальный: IP-адрес и порт локального компьютера.

Удаленный: IP-адрес и порт удаленного компьютера.

Приложение: указывает на приложение, к которому применяется правило.

Элементы управления

Добавить: создание нового правила.

Изменить: позволяет изменять существующие правила.

Удалить: служит для удаления правил.

Показать встроенные (предварительно настроенные) правила: предварительно настроенные правила для ESET Smart Security, с помощью которых можно разрешать или блокировать определенные соединения. Эти правила можно отключить, но не удалить.

В начало/Вверх/Вниз/В конец: настройка уровней приоритета правил (правила выполняются по очереди сверху вниз).

4.3.3.2 Работа с правилами

После каждого изменения отслеживаемых параметров необходимо обновить правила. Если после внесения изменений правило не может отвечать требованиям и указанное действие не может выполняться, в подключении может быть отказано. Это может привести к проблемам в работе приложения, для которого создавалось правило. Примером может быть изменение сетевого адреса или номера порта удаленного компьютера.

Верхняя часть диалогового окна содержит три вкладки.

- **Общие**: выбор имени правила, направления подключения, действия (**Разрешить**, **Запретить**, **Запросить**), протокола и профиля, к которому будет применяться правило.
- **Локальный**: на экран выводится информация о локальном компьютере, участвующем в подключении, с указанием номера локального порта или диапазона портов и названия приложения, которое установило подключение. Позволяет также с помощью кнопки **Добавить** добавлять сюда предварительно заданную или созданную зону с диапазоном IP-адресов.
- **Удаленный**: на этой вкладке приводится информация об удаленном порте (диапазоне портов). Также здесь можно указать список удаленных IP-адресов или зон для конкретного правила. Позволяет также с помощью кнопки **Добавить** добавлять сюда предварительно заданную или созданную зону с диапазоном IP-адресов.

При создании нового правила необходимо ввести его имя в поле **Имя**. Направление подключения, к которому применяется правило, выбирается в раскрывающемся списке **Направление**, а действие, которое должно выполняться, когда подключение удовлетворяет параметрам правила, — в раскрывающемся списке **Действие**.

Протокол: протокол передачи данных, используемый для правила. Выберите в раскрывающемся списке протокол, который следует использовать для данного правила.

Тип/код ICMP: определяемое числом сообщение ICMP (например, 0 означает ответ проверки связи).

По умолчанию все правила включены с со сферой применения **Любой профиль**. При необходимости можно выбрать в раскрывающемся списке **Профили** пользовательский профиль файервола.

Если включить параметр **Журнал**,, действия, связанные с данным правилом, будут записываться в журнал. **Уведомить пользователя**: вывод сообщения в случае применения правила.

ПРИМЕЧАНИЕ
Ниже приведен пример создания правила, разрешающего веб-браузеру доступ к сети. Необходимо настроить такие параметры.

- На вкладке **Общие** включите исходящие подключения по протоколам TCP и UDP.
- Добавьте процесс браузера (для браузера Internet Explorer — iexplore.exe) на вкладке **Локальный**.
- На вкладке **Удаленный** включите порт 80, если следует разрешить стандартные действия, связанные с посещением веб-страниц.

ПРИМЕЧАНИЕ.
Обратите внимание, что возможности изменения предварительно заданных правил ограничены.

4.3.4 Настройка зон

Зона — набор сетевых адресов, объединенных в логическую группу. Возможность создания зон предусмотрена для случаев, когда один и тот же набор адресов необходимо использовать в нескольких правилах. Каждому адресу в группе присваивается аналогичное правило, которое определено для всей группы в целом. Примером такой группы является **доверенная зона**. Доверенная зона представляет собой группу сетевых адресов, не блокируемых персональным файерволом. Зоны можно настроить в разделе **Дополнительные настройки** > **Персональный файервол** > **Дополнительно**, нажав кнопку **Изменить**, расположенную рядом с элементом **Зоны**. Чтобы добавить новую зону, нажмите кнопку **Добавить**, в поле **Имя** введите имя зоны, в поле **Описание** — ее описание, а затем в поле **Адрес удаленного компьютера (IPv4, IPv6, диапазон, маска)** укажите IP-адрес удаленного компьютера.

В окне настроек **Зоны файервола** можно задать имя зоны, ее описание и список сетевых адресов (см. также раздел Редактор известных сетей).

4.3.5 Известные сети

Если вы часто подключаете компьютер к сетям общего пользования или сетям, находящимся вне вашей обычной домашней или рабочей сети, мы рекомендуем проверять надежность новых сетей, к которым выполняется подключение. После определения сетей ESET Smart Security может определять доверенные (домашние или рабочие) сети, используя параметры сети, заданные в конфигурации **Сетевая идентификация**. Портативные компьютеры часто входят в сети с IP-адресами, похожими на адрес доверенной сети. В таких случаях ESET Smart Security может отнести неизвестную сеть к доверенным (домашним или рабочим). Во избежание этого рекомендуется использовать **Сетевую аутентификацию**.

Когда сетевой адаптер подключается к сети или происходит изменение его сетевой конфигурации, ESET Smart Security проверяет наличие новой сети в списке известных сетей. Если **Сетевая идентификация** и **Сетевая аутентификация** (необязательный параметр) совпадают, сеть помечается как подключенная к данному интерфейсу. Если сеть не найдена среди известных, на основе конфигурации сетевой идентификации создается новое сетевое подключение, на основании которого определяется эта сеть при следующем подключении к ней. По умолчанию для нового сетевого подключения используется тип защиты **Сеть общего пользования**. В диалоговом окне **Обнаружено новое сетевое подключение** вам будет предложено выбрать тип защиты: **Сеть общего пользования**, **Домашняя или офисная сеть** либо **Использовать параметр Windows**. Если сетевой адаптер подключен к известной сети, помеченной как **Домашняя или офисная сеть**, то локальные подсети адаптера будут добавлены в доверенную зону.

Тип защиты новых сетей: выберите один из следующих параметров: **Использовать параметр Windows**, **Спросить пользователя** либо **Отметить как общедоступ.**. Этот параметр будет использоваться для новых сетей по умолчанию.

ПРИМЕЧАНИЕ
Когда выбрана установка **Использовать параметр Windows**, диалоговое окно не отображается и сеть, к которой вы подключены, автоматически помечается согласно вашим настройкам ОС Windows. В результате для новых сетей будут доступны некоторые функции (например, обмен файлами и удаленный рабочий стол).

Настройку новых сетей можно осуществить вручную из окна Редактор известных сетей.

4.3.5.1 Редактор известных сетей

Настройку известных сетей вручную можно выполнить, выбрав **Дополнительные настройки** > **Персональный файервол** > **Известные сети** и нажав кнопку **Изменить**.

Столбцы

Имя: имя известной сети.

Тип защиты: этот элемент отображается, если для сети выбрана установка **Домашняя или офисная сеть**, **Сеть общего пользования** либо **Использовать параметр Windows**.

Профиль файервола: выберите профиль в раскрывающемся списке **Показывать правила, используемые в этом профиле**, чтобы отобразить используемые в нем правила фильтрования.

Элементы управления

Добавить: создание новой известной сети.

Изменить: изменение существующей известной сети.

Удалить: выберите сеть и нажмите кнопку **Удалить**, чтобы удалить ее из списка известных сетей.

Вверх/Поднять/Опустить/Вниз: настройка уровня приоритета известных сетей (оценка сетей осуществляется сверху вниз).

Параметры конфигурации сети размещаются на следующих вкладках:

Сеть

Здесь можно определить **имя сети** и выбрать для нее **тип защиты** («Сеть общего пользования», «Домашняя или офисная сеть» либо «Использовать параметр Windows»). Раскрывающийся список **Профиль файервола** служит для выбора профиля сети. Если для сети выбран тип защиты **Домашняя или офисная сеть**, все подключенные к ней напрямую подсети автоматически считаются доверенными. Например, если сетевой адаптер подключен к такой сети с IP-адресом 192.168.1.5 и маской подсети 255.255.255.0, подсеть 192.168.1.0/24 будет добавлена в доверенную зону адаптера. Если у адаптера имеется больше адресов или подсетей, все они будут считаться доверенными вне зависимости от конфигурации параметра **Сетевая идентификация** известной сети.

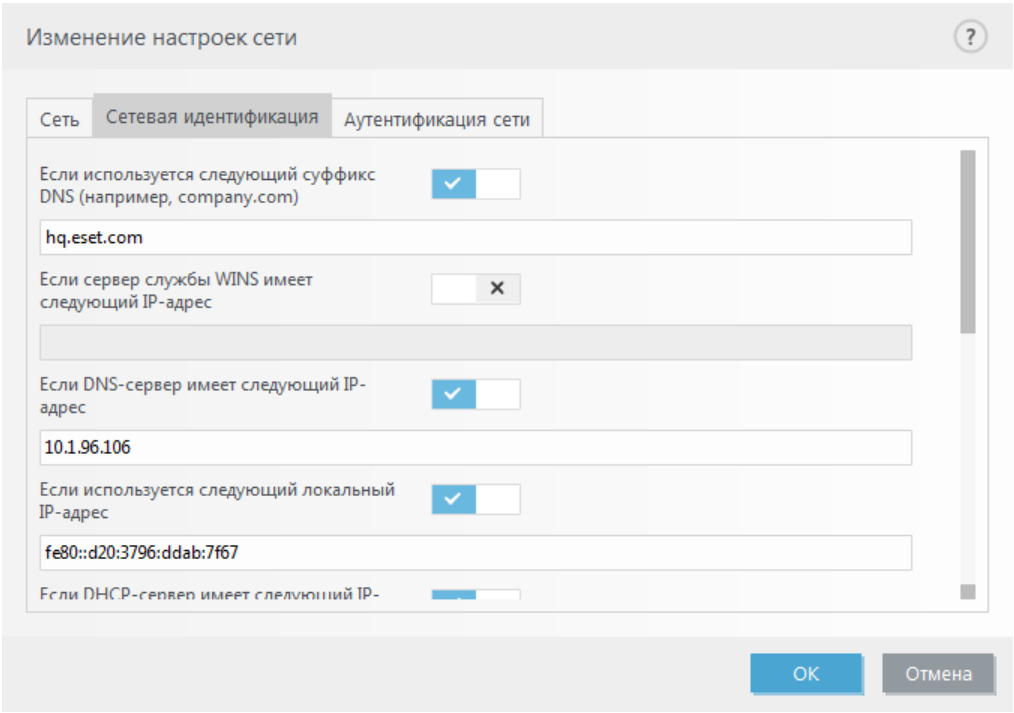
Кроме этого, адреса, добавленные в список **Дополнительные доверенные адреса**, всегда включаются в доверенную зону подключенных к сети адаптеров (вне зависимости от типа защиты такой сети).

Для того чтобы сеть была отмечена как подключенная, необходимо выполнение указанных ниже условий.

- Сетевая идентификация: все введенные параметры должны отвечать параметрам активного подключения.
- Сетевая идентификация: если выбран сервер аутентификации, необходимо совершение успешной аутентификации с помощью сервера аутентификации ESET.
- Ограничения сети (только Windows XP): должны соблюдаться все глобальные ограничения.

Сетевая идентификация

Аутентификация выполняется на основе параметров адаптера локальной сети. Происходит сравнение всех установленных параметров с фактическими параметрами активного сетевого подключения. Разрешено использование адресов IPv4 и IPv6.



Аутентификация сети

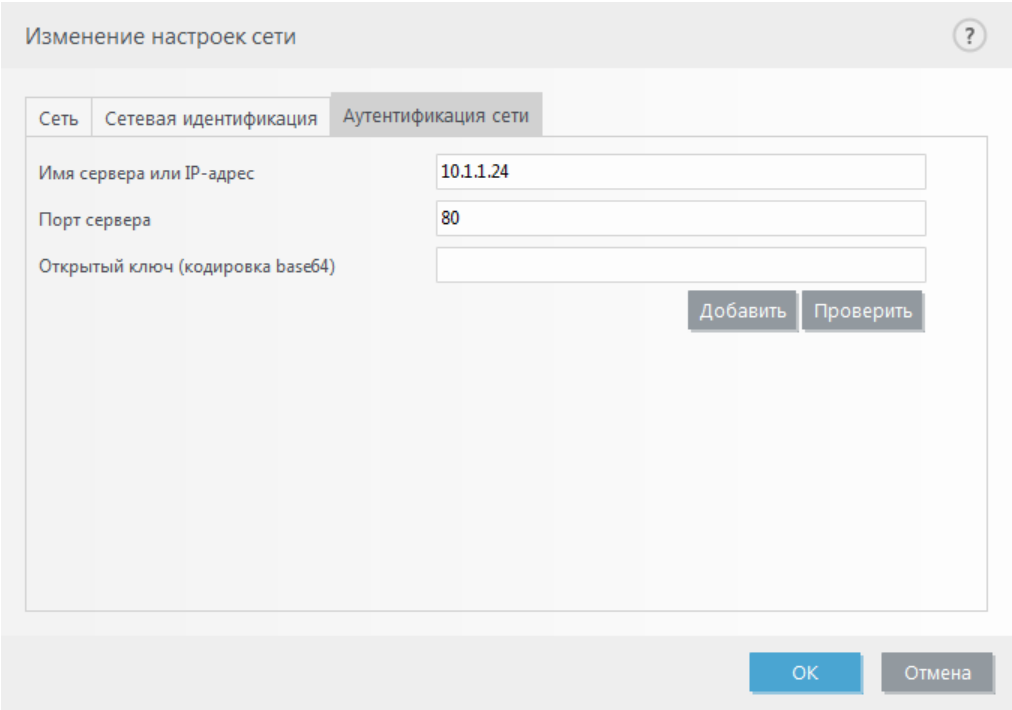
В рамках аутентификации сети выполняется поиск определенного сервера в сети, а для аутентификации сервера используется асимметричное шифрование (RSA). Имя аутентифицируемой сети должно совпадать с именем сети, указанным в настройках сервера аутентификации. Имя вводится с учетом регистра. Укажите имя сервера, его порт прослушивания и открытый ключ, соответствующий закрытому ключу сервера (см. раздел Аутентификация сети: конфигурация сервера). Имя сервера можно ввести в виде IP-адреса, имени DNS или NetBios. После имени сервера можно указать путь к файлу ключа на сервере (например, имя_сервера_/

каталог1/каталог2/аутентификация). На случай недоступности сервера можно указать дополнительные серверы через точку с запятой.

Загрузите сервер аутентификации ESET.

Открытым ключом может быть файл одного из указанных ниже типов.

- Зашифрованный открытый ключ в формате PEM (.pem). Этот ключ можно создать с помощью приложения ESET Authentication Server (см. раздел Аутентификация сети: конфигурация сервера).
- Зашифрованный открытый ключ.
- Сертификат открытого ключа (.crt).



Чтобы проверить настройки, нажмите кнопку **Проверить**. Если аутентификация прошла успешно, на экране появится сообщение *Аутентификация сервера завершена*. Если аутентификация не настроена должным образом, на экране появится одно из указанных ниже сообщений об ошибке.

Сбой аутентификации сервера. Недопустимая или несовпадающая подпись.
Подпись сервера не отвечает введенному открытому ключу.

Сбой аутентификации сервера. Имя сети не совпадает.
Настроенное имя сервера не соответствует зоне сервера аутентификации. Проверьте оба имени и убедитесь, что они одинаковы.

Сбой аутентификации сервера. Нет ответа от сервера, или получен недопустимый ответ.
Ответ отсутствует, если сервер не работает или недоступен. Недопустимый ответ может быть получен в случае, если запущен другой HTTP-сервер с указанным адресом.

Указан недействительный открытый ключ.
Проверьте, не поврежден ли файл открытого ключа.

Ограничения сети (только для Windows XP)

В современных операционных системах (Windows Vista и более новые) каждый сетевой адаптер имеет собственную доверенную зону и активный профиль файервола. К сожалению, в Windows XP такая структура не поддерживается, поэтому все сетевые адаптеры всегда имеют одну и ту же доверенную зону и профиль активного файервола. Такая конфигурация создает потенциальный риск для безопасности компьютера, одновременно подключенного к нескольким сетям. В таких случаях трафик из ненадежной сети может оцениваться с использованием доверенной зоны и профиля файервола для другой подключенной сети. Для снижения рисков для безопасности можно соблюдать следующие ограничения, позволяющие избежать

глобального применения конфигурации одной из сетей во время подключения другой (потенциально ненадежной).

В Windows XP параметры подключенной сети (доверенная зона и профиль файервола) применяются глобально, кроме случаев, когда как минимум одно из указанных ниже ограничений включено и не соблюдается.

a. Активно только одно подключение
b. Беспроводное соединение не установлено
c. Нет установленных небезопасных беспроводных подключений

4.3.5.2 Проверка подлинности сети: конфигурация сервера

Аутентификацию сети можно выполнить с помощью любого подключенного к ней компьютера или сервера. Для этого на компьютер или сервер, который всегда доступен для аутентификации, когда клиент пытается подключиться к сети, нужно установить приложение ESET Authentication Server. Файл установки приложения ESET Authentication Server можно загрузить с веб-сайта ESET.

После установки ESET Authentication Server на экран будет выведено диалоговое окно. (Приложение можно запустить, нажав кнопку **Пуск** и выбрав последовательно пункты **Программы** > **ESET** > **ESET Authentication Server**).

Для того чтобы настроить сервер аутентификации, введите имя зоны аутентификации, прослушивающий порт сервера (по умолчанию 80) и место, в котором будут храниться открытый и закрытый ключи. Далее создайте открытый и закрытый ключи, которые будут использоваться при аутентификации. Закрытый ключ должен использоваться на сервере, а открытый — импортироваться на сторону клиента, что можно сделать в разделе аутентификации зоны при настройке зоны в файерволе.

Более подробные сведения можно найти в этой статье базы знаний ESET.

4.3.6 Ведение журнала

Персональный файервол ESET Smart Security сохраняет данные обо всех важных событиях в файле журнала, который можно открыть с помощью главного меню. Щелкните **Служебные программы** > **Дополнительные средства** > **Файлы журналов**, а затем в раскрывающемся меню **Журнал** щелкните пункт **Персональный файервол**.

Файлы журнала могут использоваться для обнаружения ошибок и вторжений на компьютер. Журналы персонального файервола ESET содержат следующую информацию.

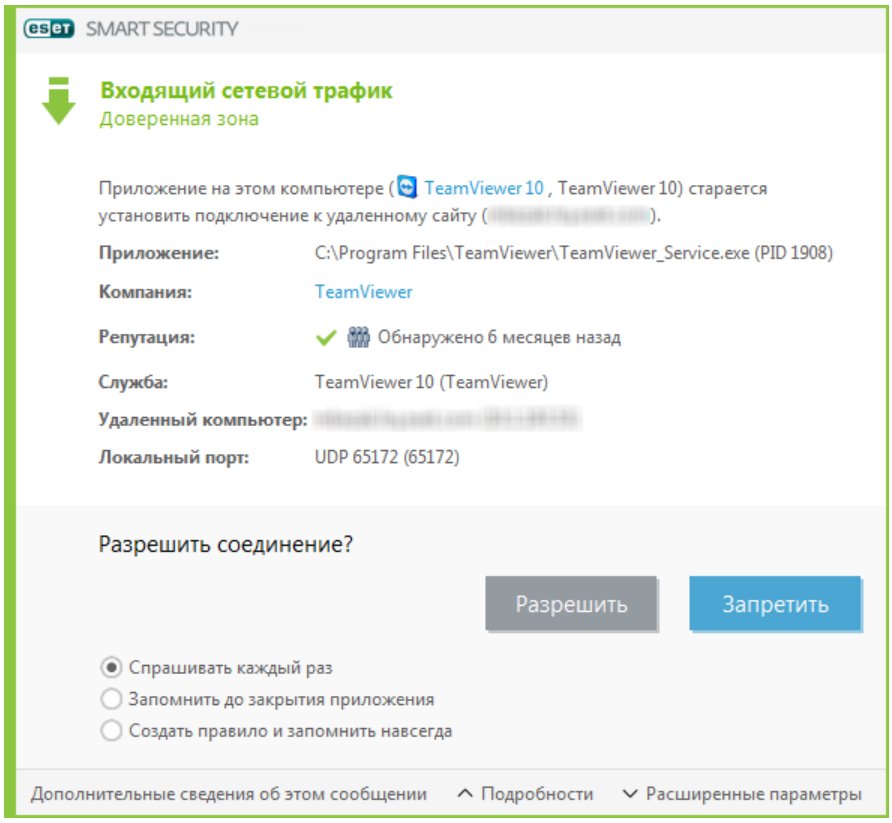
- Дата и время события
- Имя события
- Источник
- Сетевой адрес объекта
- Сетевой протокол передачи данных
- Примененное правило или имя червя (если обнаружено)
- Задействованное приложение
- Пользователь

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

4.3.7 Установка соединения: обнаружение

Персональный файервол обнаруживает каждое из вновь созданных сетевых соединений. Активный режим персонального файервола определяет, какие действия должны выполняться для нового правила. Если активирован **Автоматический режим** или **Режим на основе политики**, персональный файервол выполнит предварительно заданные действия без какого-либо вмешательства пользователя.

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



Будьте внимательны при создании новых правил и разрешайте только те соединения, в безопасности которых вы уверены. Если разрешить все соединения, персональный файервол не сможет обеспечивать защиту. Ниже перечислены наиболее важные параметры соединений.

- **Удаленный компьютер**: разрешить соединения только с доверенными и известными адресами.
- **Локальное приложение**: не рекомендуется разрешать соединения с неизвестными приложениями и процессами.
- **Номер порта**: соединения на стандартных портах (например, порт номер 80 для просмотра веб-страниц) в обычных условиях должны быть разрешены.

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

4.3.8 Решение проблем, связанных с персональным файерволом ESET

Если при установленной программе ESET Smart Security возникли проблемы подключения к сети, узнать, обусловлены они работой персонального файервола ESET или нет, можно несколькими способами. Кроме того, в персональном файерволе ESET можно создать новые правила и исключения, которые могут помочь решить проблемы с подключением.

Для решения проблем, связанных с персональным файерволом ESET, см. следующие темы справки.

- Мастер устранения неполадок
- Ведение журнала и создание правил и исключений на основе журнала
- Создание исключений на основе уведомлений персонального файервола
- Расширенное ведение журналов PCAP
- Решение проблем с фильтрацией протоколов

4.3.8.1 Мастер устранения неполадок

Мастер устранения неполадок автоматически отслеживает все заблокированные соединения и помогает устранять неполадки для исправления проблем с файерволом в работе определенных приложений и устройств. После этого мастер предложит новый набор правил, который вам нужно будет подтвердить. **Мастер устранения неполадок** можно найти в главном меню, последовательно выбрав **Настройки** > **Защита сети**.

4.3.8.2 Ведение журнала и создание правил и исключений на основе журнала

По умолчанию персональный файервол ESET вносит в журнал не все блокируемые соединения. Если вы хотите видеть, что блокирует персональный файервол, включите ведение журнала в разделе **Дополнительные настройки**. Чтобы его отобразить, последовательно выберите элементы **Служебные программы** > **Диагностика** > **Включить расширенное ведение журнала в персональном файерволе**. Если в журнале есть элемент, который персональному файерволу не следует блокировать, можно создать правило или исключение IDS, щелкнув этот элемент правой кнопкой мыши и выбрав пункт **Не блокировать подобные события в будущем**. Обратите внимание, что журнал всех заблокированных соединений может содержать тысячи элементов, поэтому найти конкретный элемент может быть трудно. После решения проблемы ведение журнала можно выключить.

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

ПРИМЕЧАНИЕ
Используйте ведение журнала, чтобы узнать, в каком порядке персональный файервол блокировал те или иные соединения. Кроме того, правила, созданные на основе журнала, будут выполнять нужные вам действия.

4.3.8.2.1 Создание правил на основе журнала

В новой версии ESET Smart Security можно создавать правила на основе журнала. В главном меню последовательно выберите **Служебные программы** > **Дополнительные средства** > **Файлы журнала**. В раскрывающемся меню выберите пункт **Персональный файервол**, щелкните нужную запись журнала правой кнопкой мыши и в контекстном меню выберите пункт **Не блокировать подобные события в будущем**. Новое правило отобразится в окне уведомлений.

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

- установите минимальную степень детализации журнала **Диагностика**, последовательно выбрав **Дополнительные настройки** (F5) > **Служебные программы** > **Файлы журнала**;
- установите флажок **Показывать уведомление при обнаружении атаки, использующей бреши в системе безопасности** в меню **Дополнительные настройки** (F5) > **Персональный файервол** > **IDS и расширенные параметры** > **Обнаружение вторжений**.

4.3.8.3 Создание исключений на основе уведомлений персонального файервола

Когда персональный файервол ESET обнаруживает вредоносную сетевую активность, отображается окно уведомлений с описанием этого события. Уведомление содержит ссылку, перейдя по которой можно получить дополнительные сведения о событии и создать исключение для этого события (если нужно).

ПРИМЕЧАНИЕ
Если сетевое приложение или устройство не соблюдает сетевые стандарты надлежащим образом, это может вызвать отображение повторяющихся уведомлений IDS файервола. Создать исключение можно непосредственно на основе уведомления. Благодаря этому персональный файервол ESET не будет обнаруживать указанное приложение или устройство.

4.3.8.4 Расширенное ведение журналов PCAP

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

1. Перейдите в раздел **Дополнительные настройки** > **Служебные программы** > **Диагностика** и выберите параметр **Включить расширенное ведение журнала в персональном файерволе**.
2. Попробуйте воспроизвести текущую проблему.
3. Выключить расширенное ведение журнала PCAP.
4. Файл журнала PCAP можно найти в папке, где создаются дампы памяти для диагностики.

- Microsoft Windows Vista или более новая версия

  C:\ProgramData\ESET\ESET Smart Security\Diagnostics

- Microsoft Windows XP

  C:\Documents and Settings\All Users\...

4.3.8.5 Решение проблем с фильтрацией протоколов

Если возникают проблемы с браузером или почтовым клиентом, сначала следует определить, нормально ли работает фильтрация протоколов. Для этого временно отключите фильтрацию протоколов приложений в дополнительных настройках (обязательно включите его после решения проблемы, иначе браузер и почтовый клиент останутся без защиты). Если после отключения неполадка исчезает, см. ниже список распространенных проблем и способов их решения.

Проблемы с обновлением или безопасностью обмена данными

У приложения проблемы с обновлением или защищенностью канала связи.

- Если включена фильтрация протоколов SSL, попробуйте временно ее отключить. Если помогло, значит, можно продолжать использовать фильтрацию SSL и выполнять обновления. Для этого нужно исключить проблемное соединение.
  Переведите фильтрацию протоколов SSL в интерактивный режим. Запустите обновление еще раз. Должно появиться диалоговое окно с уведомлением о шифрованном сетевом трафике. Приложение должно быть аналогичным тому, в связи с которым возникли проблемы, а сертификат должен исходить с того сервера, с которого выполняются обновления. Затем запомните действия для сертификата и нажмите кнопку «Пропустить». Если не отобразятся соответствующие диалоговые окна, переключитесь обратно в автоматический режим фильтрации. Проблема должна быть решена.

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

Проблема с доступом к устройству в сети

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

Проблемы с определенным веб-сайтом

Исключить определенные веб-сайты из фильтрации протоколов можно с помощью управления URL-адресами. Например, если не удается получить доступ к странице https://www.gmail.com/intl/en/mail/help/about.html, попробуйте добавить *gmail.com* в список исключенных адресов.

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

При включении фильтрации протоколов SSL программа ESET Smart Security выполняет фильтрацию протокола SSL таким образом, что установленные программы доверяют ее действиям (происходит импорт сертификата в их хранилище сертификатов). Для некоторых приложений это невозможно, если они запущены. Например, для браузеров Firefox и Opera. Закройте эти приложения (для этого рекомендуется открыть диспетчер задач и удалить записи firefox.exe и opera.exe на вкладке «Процессы»), а затем нажмите кнопку «Повторить».

Ошибка: недоверенный издатель или недопустимая подпись

Скорее всего, это значит, что при вышеописанном импорте произошла ошибка. Сначала закройте все упомянутые приложения. Затем выключите фильтрацию протоколов SSL и включите ее обратно. Будет выполнена повторная попытка импорта.

4.4 Средства безопасности

Параметр **Средства безопасности** можно использовать для настройки следующих модулей.

- Защита банковской оплаты
- Родительский контроль
- Антивор

4.4.1 Родительский контроль

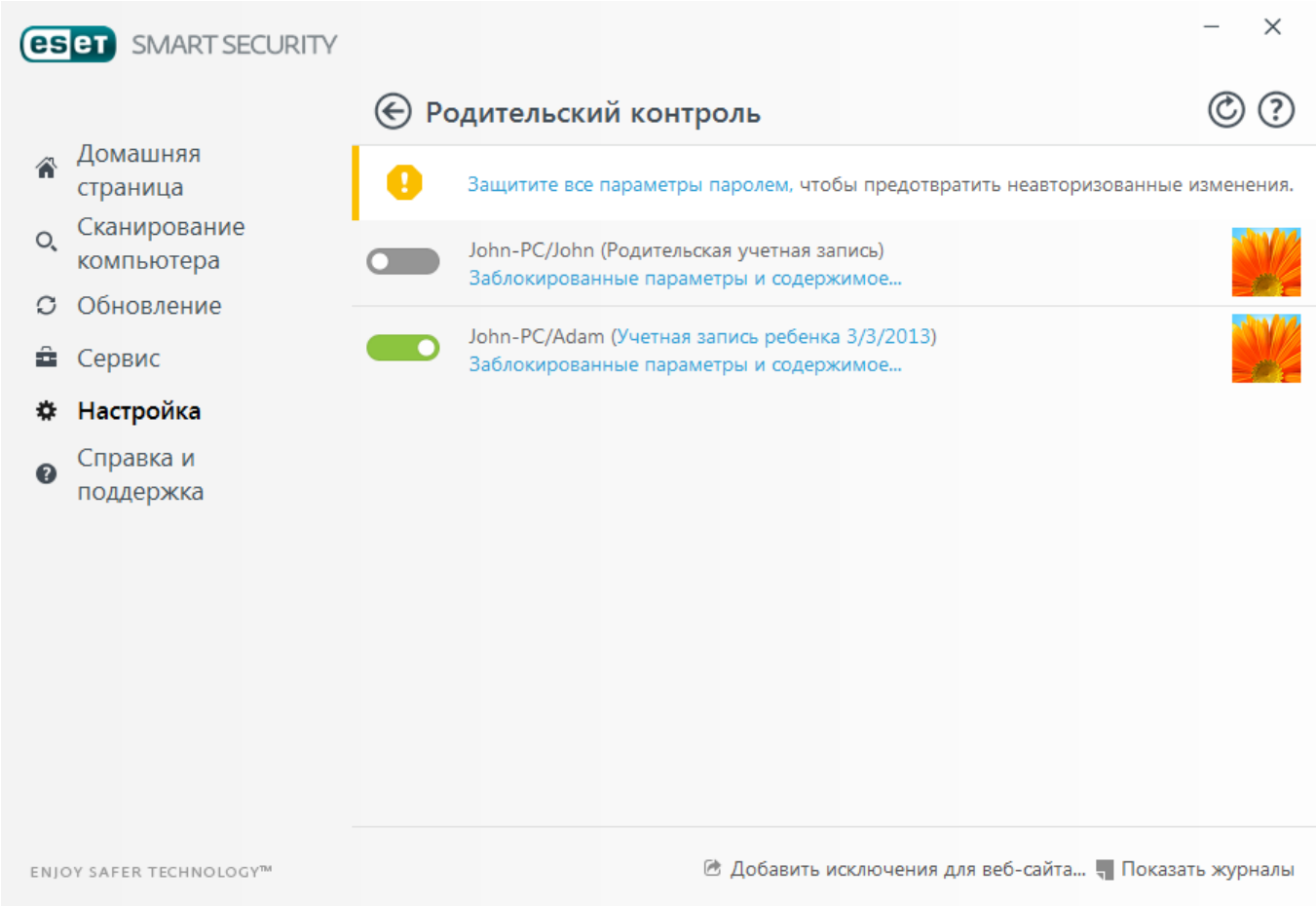
Модуль родительского контроля позволяет настраивать соответствующие параметры, которые дают родителям возможность использовать автоматизированные средства для защиты своих детей и задавать ограничения для устройств и служб. Цель заключается в предотвращении доступа детей и подростков к страницам, содержимое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

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

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

1. По умолчанию родительский контроль в программе ESET Smart Security отключен. Существует два способа активации родительского контроля.
   - В главном окне программы щелкните элемент  и последовательно выберите элементы **Настройка** > **Средства безопасности** > **Родительский контроль**, после чего включите функцию родительского контроля.
   - Нажмите клавишу F5, чтобы открыть окно **Дополнительные настройки**, выберите элемент **Интернет и электронная почта** > **Родительский контроль** и установите переключатель рядом с элементом **\Интеграция с системой**.
2. В главном окне программы выберите элементы **Настройка** > **Средства безопасности** > **Родительский контроль**. Хотя для параметра **Родительский контроль** и отображается значение **Включено**, необходимо настроить родительский контроль для нужной учетной записи, щелкнув элемент **Защитить учетную запись**

или **Родительская учетная запись**. В следующем окне укажите дату рождения, чтобы определить уровень доступа и подходящие для этого возраста веб-страницы. Теперь родительский контроль включен для указанной учетной записи. Рядом с именем учетной записи щелкните элемент **Заблокированные параметры и содержимое**, чтобы задать категории, которые требуется разрешить или заблокировать, на вкладке Категории. Чтобы разрешить или заблокировать определенные веб-страницы, которые не соответствуют категории, откройте вкладку Исключения.



Если в главном окне программы ESET Smart Security щелкнуть **Настройка** > **Средства безопасности** > **Родительский контроль**, вы увидите описанное далее содержимое главного окна.

Учетные записи пользователей Windows

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

ВАЖНО!
Чтобы создать новую учетную запись (например, для ребенка), воспользуйтесь приведенными далее пошаговыми инструкциями для ОС Windows 7 или Windows Vista.

1. Откройте элемент **Учетные записи пользователей**. Для этого нажмите кнопку **Пуск** (в левом нижнем углу рабочего стола), выберите пункт **Панель управления** и щелкните **Учетные записи пользователей**.
2. Щелкните **Управление учетной записью пользователя**. Если потребуется ввести пароль администратора или его подтверждение, введите пароль или подтверждение.
3. Выберите **Создать учетную запись**.
4. Введите имя для учетной записи, выберите тип учетной записи, а затем нажмите кнопку **Создать учетную запись**.
5. Повторно откройте панель родительского контроля. Для этого в главном окне программы ESET Smart Security выберите **Настройка** > **Средства безопасности** > **Родительский контроль**.

Содержимое нижней части окна

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

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

Родительский контроль

После отключения функции родительского контроля отобразится окно а **Отключить родительский контроль**. С его помощью можно настроить время, на которое отключается такая защита. После этого значение параметра изменится на **Приостановлено** или **Полностью отключено**.

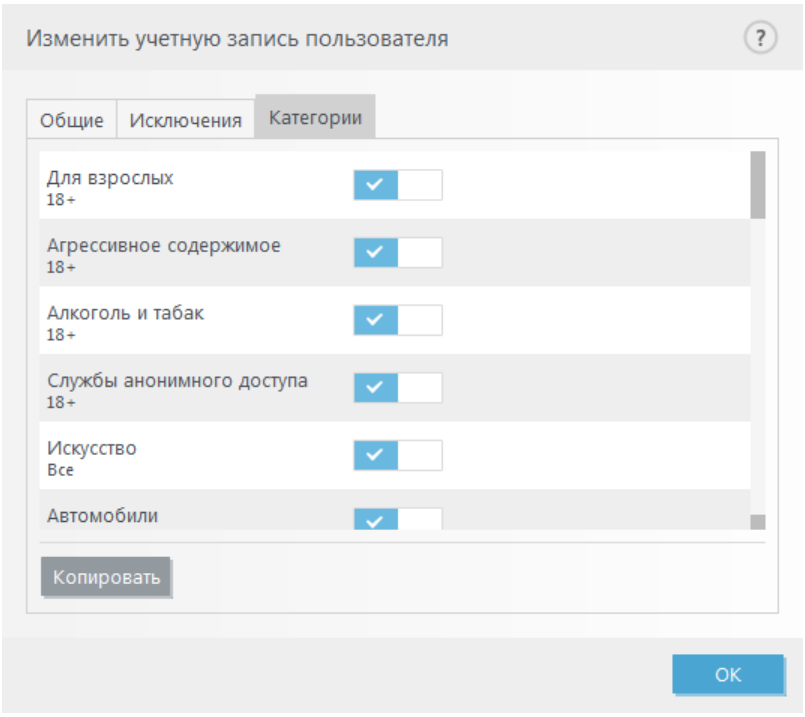
Важно защищать параметры ESET Smart Security паролем. Такой пароль задается в разделе Настройка доступа. Если пароль не задан, отобразится следующее предупреждение: **Защитить все параметры паролем**, чтобы предотвратить несанкционированные изменения. Ограничения, установленные в разделе «Родительский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

По умолчанию соединения по протоколу HTTPS (SSL) не фильтруются. Поэтому родительский контроль не может блокировать веб-страницы, адрес которых начинается с префикса *https://*. Чтобы активировать эту функцию, включите параметр **Включить фильтрацию протокола SSL/TLS** в дереве **Дополнительные настройки** в разделе**Интернет и электронная почта** > **SSL/TLS**.

ПРИМЕЧАНИЕ.
Для правильной работы родительского контроля должны быть включены функции Фильтрация содержимого, передаваемого по протоколам приложений, Проверка протокола HTTP и Персональный файервол. По умолчанию они включены.

4.4.1.1 Категории

Чтобы разрешить категорию, щелкните расположенный рядом с ней переключатель. Если оставить этот переключатель выключенным, соответствующая категория для данной учетной записи разрешена не будет.

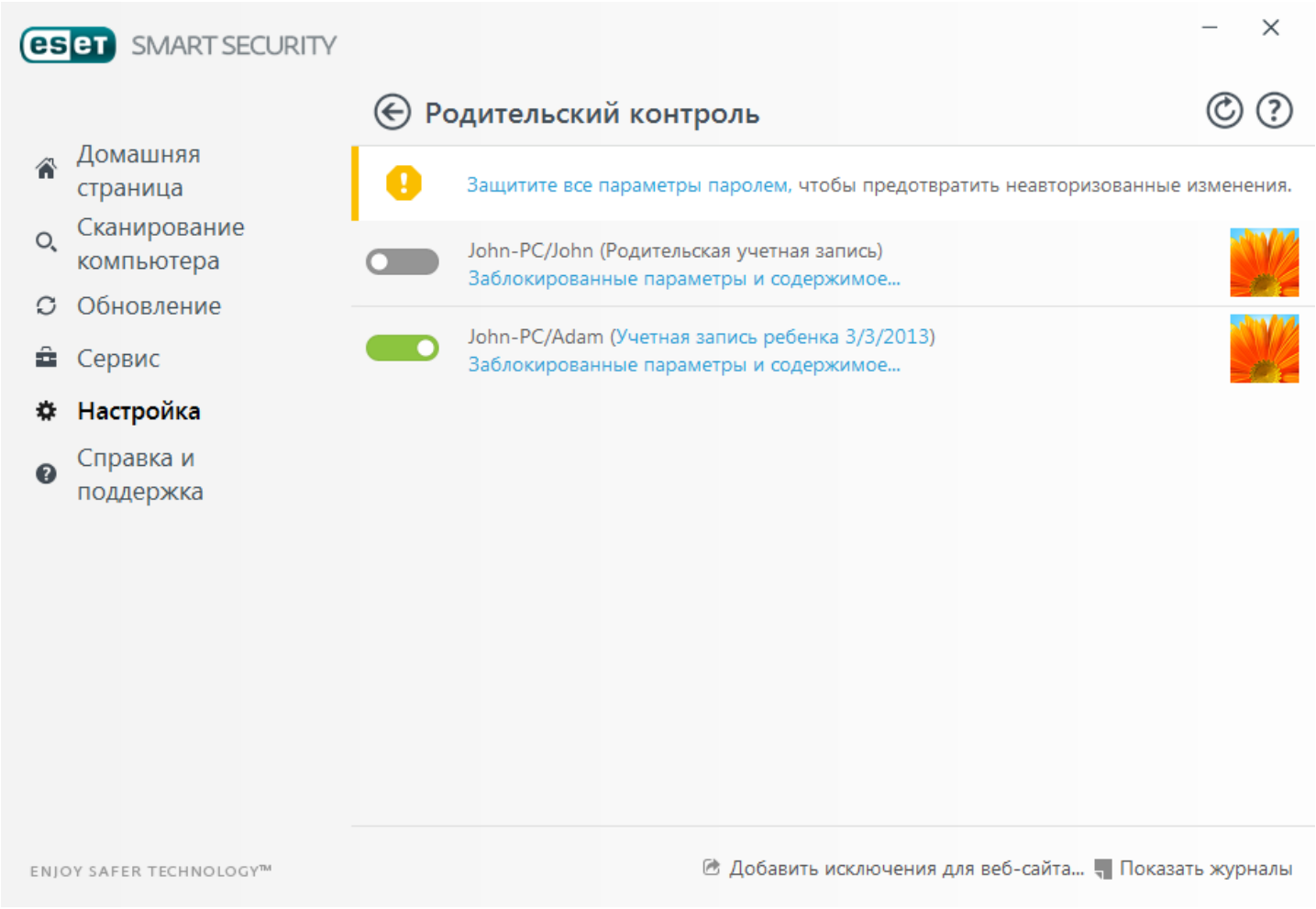


Ниже приведены некоторые примеры категорий (групп), о которых пользователям может быть неизвестно.

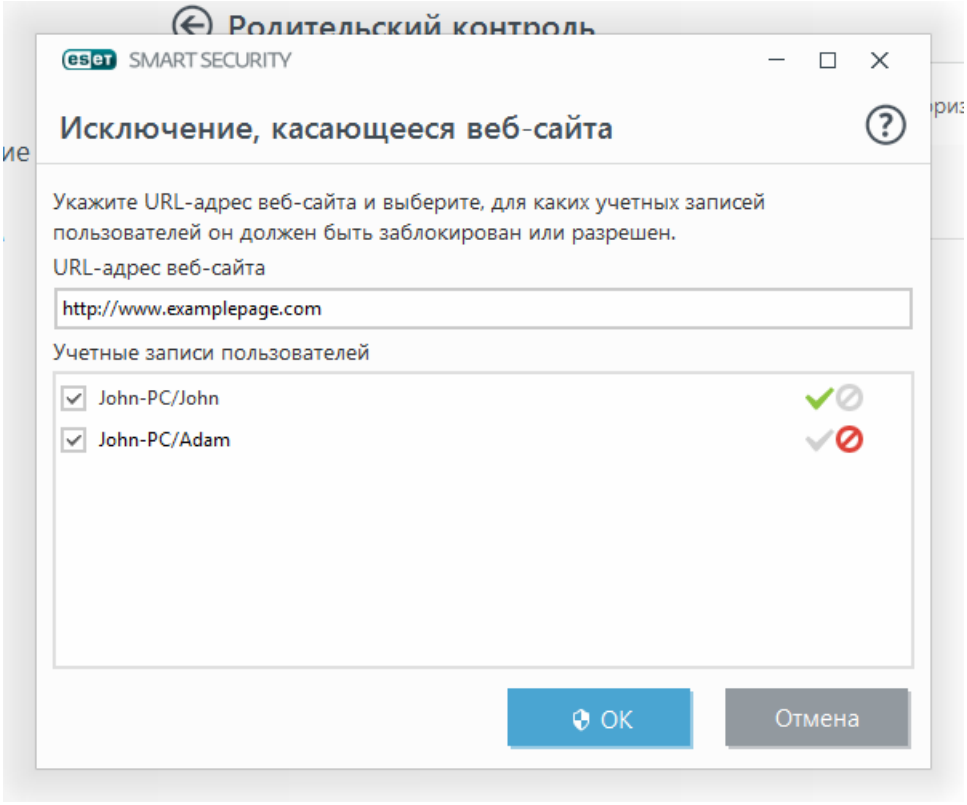
- **Разное**: обычно частные (локальные) IP-адреса, например адреса в интрасети (127.0.0.0/8, 192.168.0.0/16 и т. д). Веб-сайт, на котором отображается код ошибки 403 или 404, также попадает в эту категорию.
- **Не разрешенная**: данная категория включает веб-страницы, которые не разрешены из-за возникновения ошибки при подключении к модулю базы данных родительского контроля.
- **Без категории**: неизвестные веб-страницы, которых еще нет в базе данных родительского контроля.

4.4.1.2 Исключения, касающиеся веб-сайтов

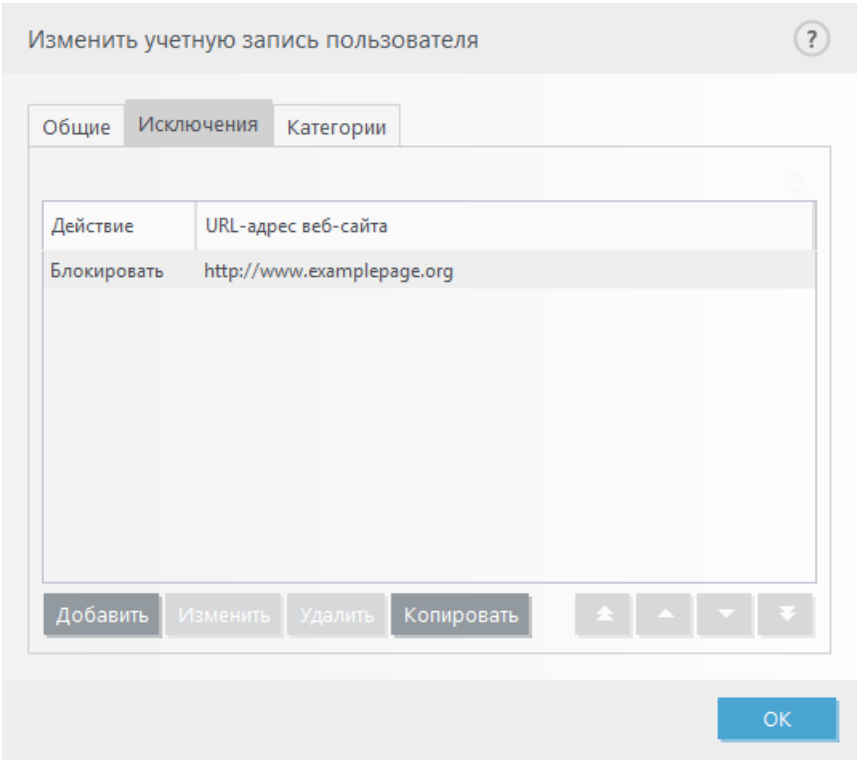
Чтобы добавить исключение для веб-сайта, последовательно выберите элементы **Настройка** > **Средства безопасности** > **Родительский контроль**, а затем щелкните элемент **Добавить исключение для веб-сайта**.



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



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



Во всех списках URL-адресов нельзя использовать специальные символы «*» (звездочка) и «?» (вопросительный знак). Например, вручную нужно вводить адреса веб-страниц с несколькими доменами верхнего уровня (*examplepage.com*, *examplepage.sk* и т. д.). При добавлении домена в список все содержимое, расположенное в нем и во всех поддоменах (например, *sub.examplepage.com*), будет разрешено или заблокировано в зависимости от выбранного вами действия на основе URL-адреса.

ПРИМЕЧАНИЕ.

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

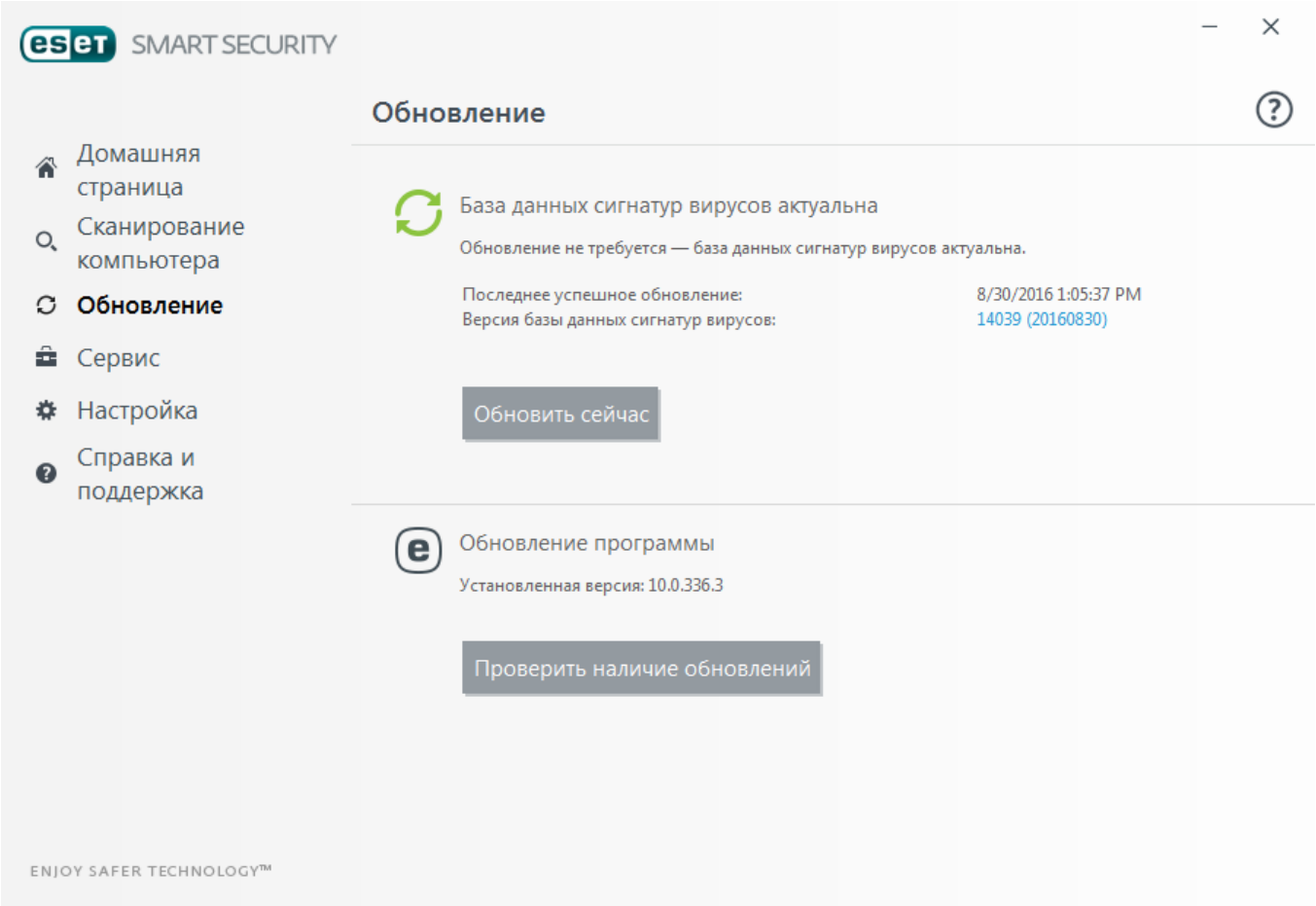
4.5 Обновление программы

Регулярное обновление ESET Smart Security — лучший способ обеспечить максимальный уровень 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 увидеть текущее состояние 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.

Также можно выполнить обновление вручную, нажав кнопку **Обновить сейчас**. 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. Для получения обновлений необходимо активировать продукт с помощью вашего лицензионного ключа. Если лицензионный ключ не был указан в процессе установки, это можно сделать для активации программы при обновлении, чтобы получить доступ к серверам обновлений ESET.

ПРИМЕЧАНИЕ
Лицензионный ключ предоставляется по электронной почте компанией ESET после приобретения ESET Smart Security.



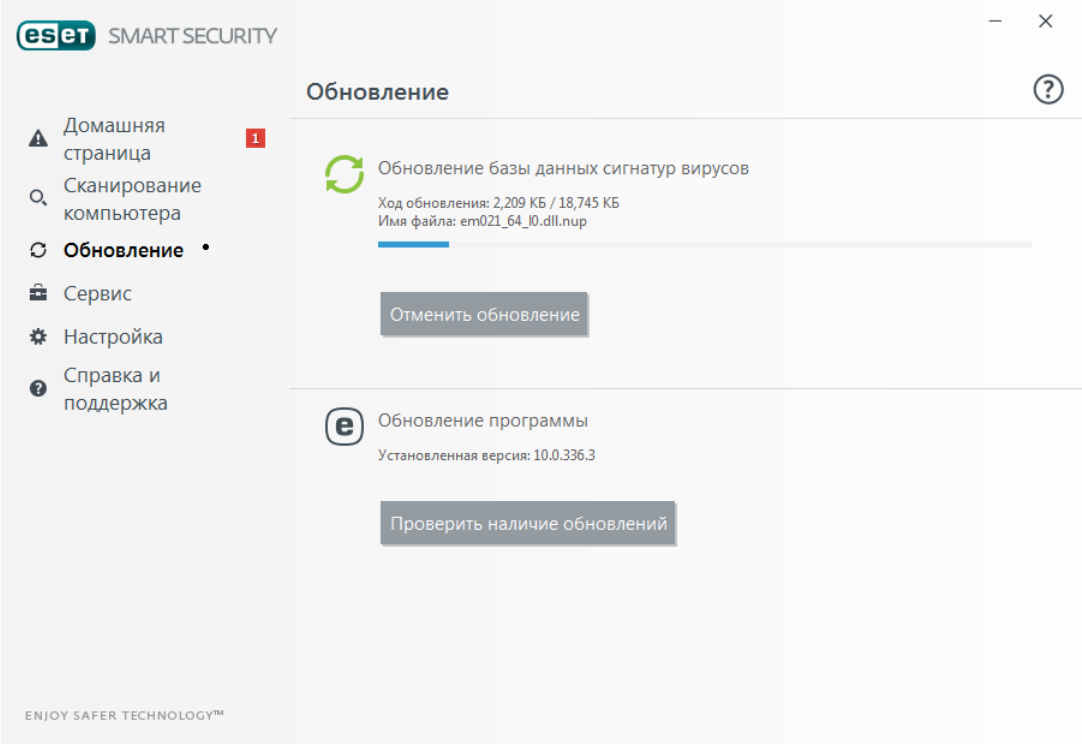
Последнее успешное обновление — дата последнего обновления. Если не отображается недавняя дата, возможно, база данных сигнатур вирусов неактуальна.

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

Нажмите **Проверить наличие обновлений**, чтобы найти последнюю доступную версию ESET Smart Security.

Процесс обновления

После нажатия кнопки **Обновить** начинается загрузка. На экран будут выведены индикатор выполнения загрузки и время до ее окончания. Чтобы прервать процесс обновления, нажмите **Отменить обновление**.

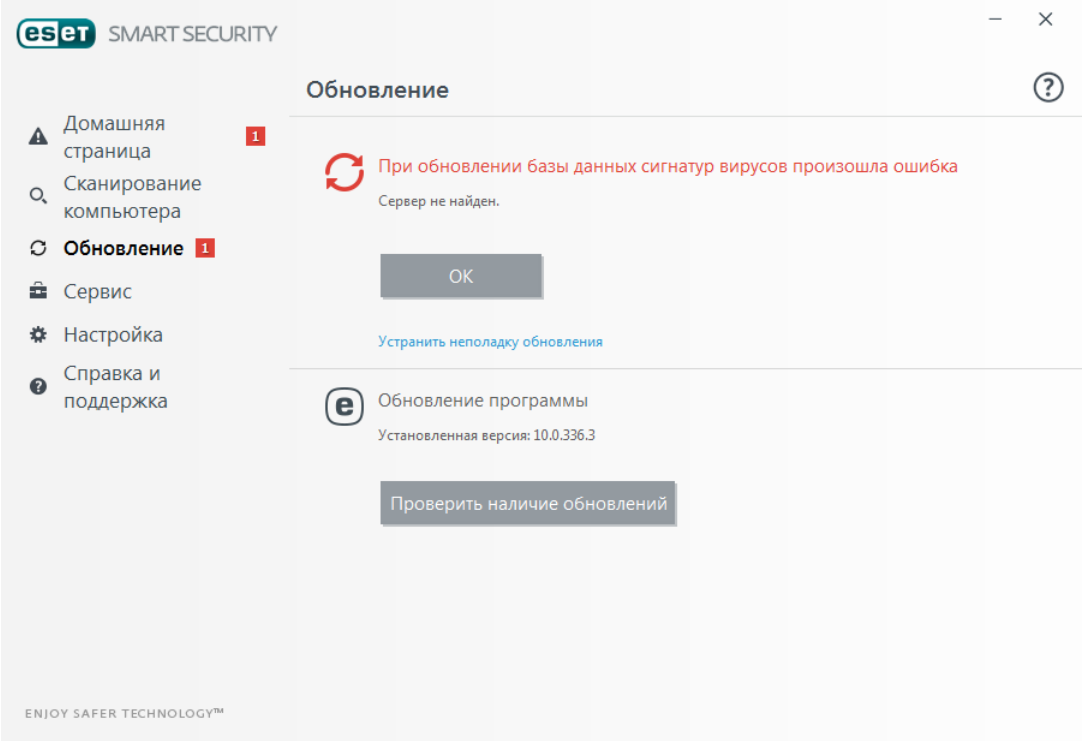


ВАЖНО!

В обычных обстоятельствах в окне **Обновление** отображается сообщение **Обновление не требуется, поскольку установленная база данных сигнатур вирусов является актуальной.**. Если этого сообщения нет, программа устарела. При этом повышается риск заражения. Необходимо обновить базу данных сигнатур вирусов как можно скорее.

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 «Дополнительные настройки» (в главном меню выберите пункт **Настройка**, после чего щелкните **Дополнительные настройки** или нажмите клавишу F5) содержатся расширенные параметры обновления. В главном меню последовательно щелкните элементы **Справка и поддержка** > **Изменить лицензию** и введите новый лицензионный ключ.
2. **Произошла ошибка при загрузке файлов обновлений**: возможная причина этой ошибки — неправильные параметры подключения к Интернету. Рекомендуется проверить наличие подключения к Интернету (например, попробуйте открыть любой веб-сайт в браузере). Если веб-сайт не открывается, возможно, не установлено подключение к Интернету или на компьютере возникли какие-либо проблемы с подключением к сети. Обратитесь к своему поставщику услуг Интернета, чтобы выяснить, есть ли у вас активное подключение к Интернету.



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

4.5.1 Параметры обновления

Параметры обновления доступны в дереве **Дополнительные настройки** (F5) в разделе **Обновление** > **Обычная**. В этом разделе приводится информация об источниках обновлений, таких как серверы обновлений, а также требуемые для них данные аутентификации.

Общие

Используемый в данный момент профиль обновления отображается в раскрывающемся списке **Выбранный профиль**. Чтобы создать новый профиль, рядом с элементом **Список профилей** нажмите кнопку **Изменить**, введите **имя профиля** и нажмите кнопку **Добавить**.

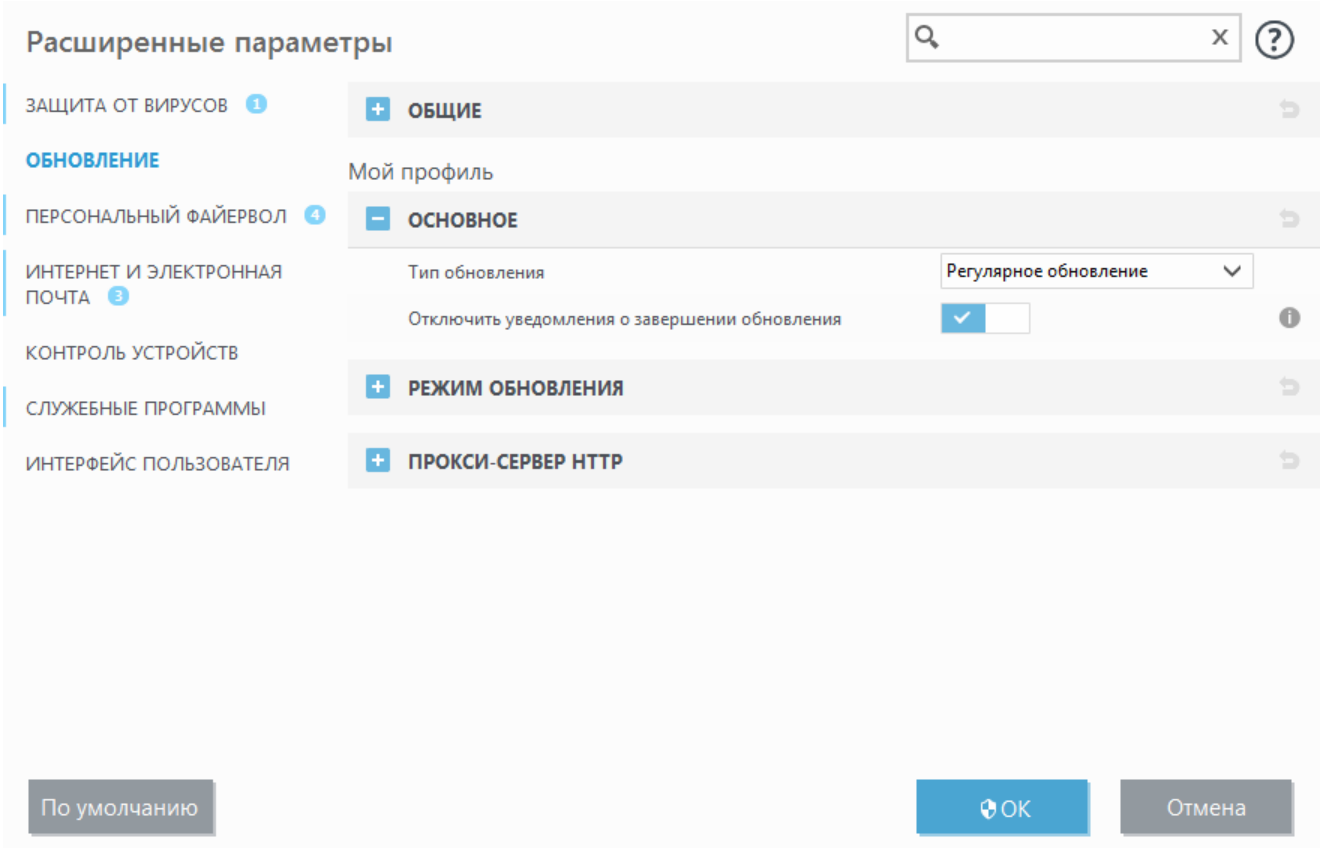
Если во время загрузки обновлений базы данных сигнатур вирусов возникли проблемы, щелкните **Очистить**, чтобы удалить временные файлы обновлений (очистить кэш).

Откат

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

ESET Smart Security создает снимки базы данных сигнатур вирусов и модулей программы для использования с функцией *отката*. Чтобы создавались снимки базы данных сигнатур вирусов, оставьте флажок **Создать снимки файлов обновлений установленным**. В поле **Количество снимков, хранящихся локально** указывается количество хранящихся снимков предыдущих состояний базы данных сигнатур вирусов.

После нажатия кнопки **Откат** (**Дополнительные настройки** (F5) > **Обновление** > **Общие**) нужно выбрать в раскрывающемся списке период 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).

Основная информация

По умолчанию для параметра **Тип обновлений** задано значение **Регулярное обновление**. Это означает, что файлы обновлений будут автоматически загружаться с сервера ESET с минимальным расходом трафика. Тестовые обновления (параметр **Тестовое обновление**) — это обновления, которые уже прошли полное внутреннее тестирование и в ближайшее время будут доступны всем пользователям. Преимущество их использования заключается в том, что у вас появляется доступ к новейшим методам обнаружения и исправлениям. Однако такие обновления иногда могут быть недостаточно стабильны и НЕ ДОЛЖНЫ использоваться на производственных серверах и рабочих станциях, где необходимы максимальные работоспособность и стабильность.

Отключить уведомления о завершении обновления: отключает уведомления на панели задач, отображаемые в правом нижнем углу экрана. Этот параметр удобно использовать, если какое-либо приложение или игра работает в полноэкранном режиме. Обратите внимание, что в игровом режиме все уведомления отключены.

4.5.1.1 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 **Выбранный профиль** отображается текущий профиль. По умолчанию это **Мой профиль**. Чтобы создать новый профиль, рядом с элементом **Список профилей** нажмите кнопку **Изменить**, введите **имя профиля** и нажмите кнопку **Добавить**.

4.5.1.2 Дополнительные настройки обновления

Расширенные параметры обновления позволяют настроить **режим обновления** и **прокси-сервер HTTP**.

4.5.1.2.1 Режим обновления

Вкладка **Режим обновления** содержит параметры, относящиеся к регулярным обновлениям программы. С помощью этих параметров можно задать поведение программы в тех случаях, когда становятся доступны новые базы данных сигнатур вирусов или обновления компонентов программы.

Обновления компонентов программы содержат новые функции или вносят изменения в функции предыдущих версий, а сами входят в регулярные обновления (баз данных сигнатур вирусов). После установки обновлений компонентов программы может потребоваться перезагрузка компьютера.

Доступны указанные ниже параметры.

Обновление приложения: когда этот параметр включен, обновление каждого из компонентов программы будет выполняться автоматически, без запросов и уведомлений.

Запрашивать подтверждение перед загрузкой обновления: если этот параметр включен, то перед установкой любого доступного обновления появляется оповещение и пользователю нужно дать согласие на установку.

Выдавать запрос, если размер обновления превышает указанный (КБ): если размер файла доступного обновления превышает указанный здесь размер, то перед установкой такого обновления появляется оповещение, и пользователю нужно дать согласие на установку.

4.5.1.2.2 Прокси-сервер HTTP

Для доступа к параметрам настройки прокси-сервера для конкретного профиля обновлений щелкните элемент **Обновление** в дереве **Дополнительные настройки** (F5), а затем **Прокси-сервер HTTP**. Выберите в раскрывающемся списке **Режим прокси-сервера** один из трех перечисленных ниже вариантов.

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

Выберите **Использовать глобальные параметры прокси-сервера**, чтобы применялись параметры конфигурации прокси-сервера, уже заданные в разделе **Служебные программы** > **Прокси-сервер** дерева расширенных параметров.

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

Подключение через прокси-сервер: этот флажок должен быть установлен в следующих случаях:

- Прокси сервер, отличный от указанного в параметре **Служебные программы** > **Прокси-сервер**, используется для обновления программы ESET Smart Security. В такой конфигурации в параметрах прокси-сервера должны быть определены сведения о новом прокси-сервере: его адрес в поле **Прокси-сервер**, коммуникационный **порт** (по умолчанию 3128), а также **имя пользователя** и **пароль** (если требуется).
- Параметры прокси-сервера не заданы глобально, однако ESET Smart Security 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) вам следует убедиться, что указанные в этом окне параметры прокси HTTP верны. Иначе 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.

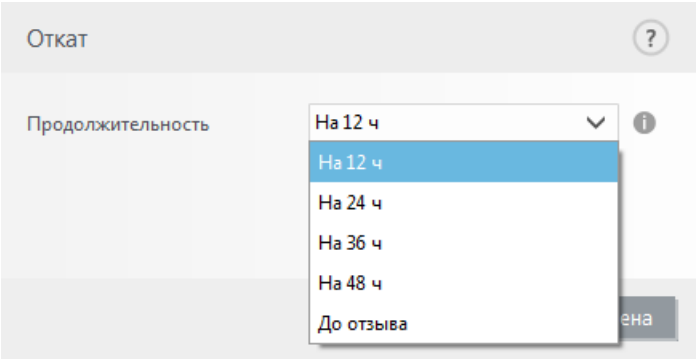
ПРИМЕЧАНИЕ.
Поля **Имя пользователя** и **Пароль** в этом разделе относятся только к прокси-серверу. Заполняйте эти поля только в том случае, если для доступа к прокси-серверу требуются имя пользователя и пароль. Указанные поля не имеют отношения к имени пользователя и паролю для программы ESET Smart Security и должны быть заполнены только в том случае, если, чтобы подключиться к Интернету через прокси-сервер, нужен пароль.

4.5.2 Откат обновления

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

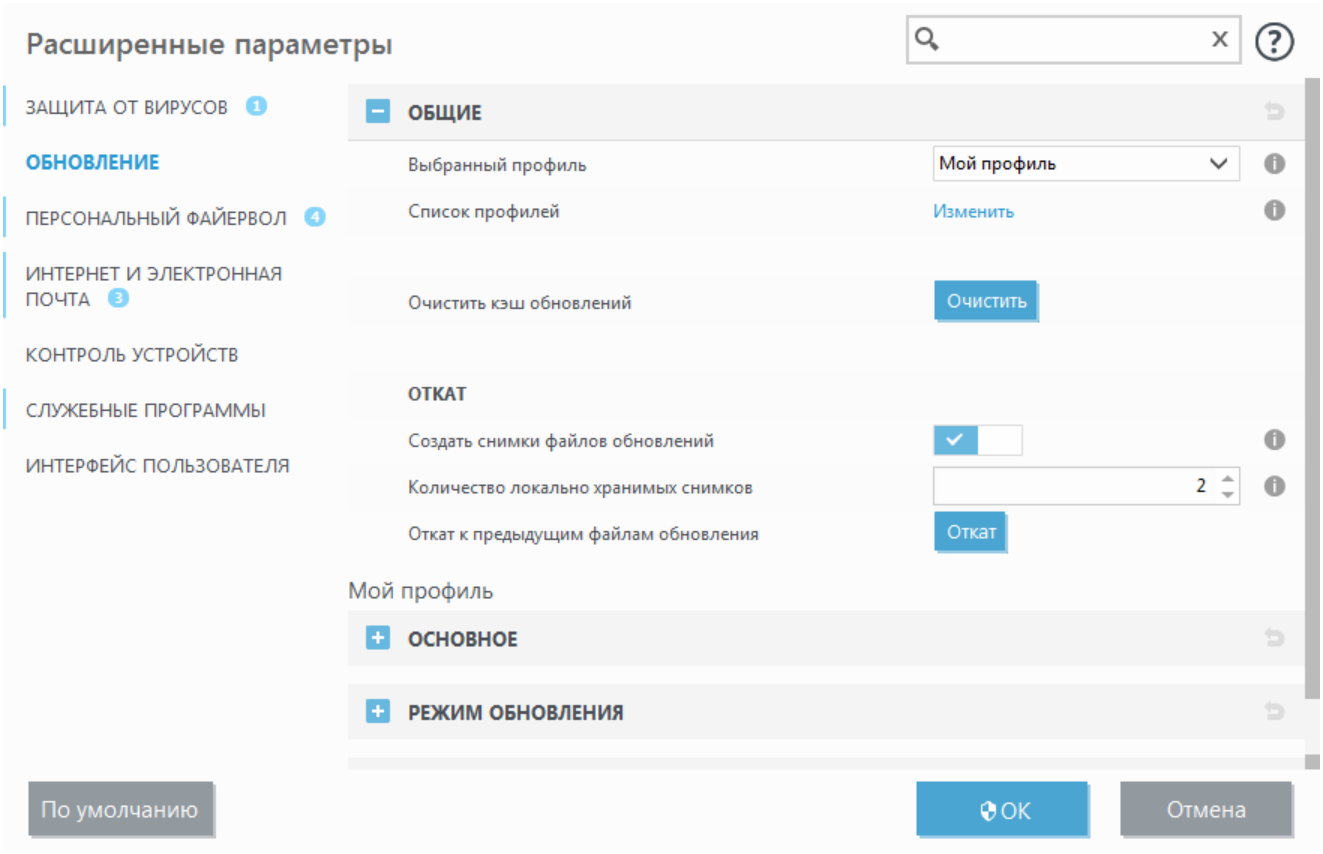
ESET Smart Security делает снимки базы данных сигнатур вирусов и модулей программы для использования с функцией *отката*. Чтобы создать снимки базы данных вирусов, установите флажок **Создать снимки файлов обновлений**. В поле **Количество снимков, хранящихся локально** указывается количество хранящихся снимков предыдущих баз данных сигнатур вирусов.

После нажатия кнопки **Откатить** (**Дополнительные настройки** (F5) > **Обновление** > **Общие**) нужно выбрать в раскрывающемся списке **Длительность** период 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.

После отката кнопка **Откат** заменяется на **Разрешить обновления**. На протяжении периода времени, выбранного в раскрывающемся меню **Приостановить обновления**, обновления не производятся. 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 6871. Версии 6870 и 6868 хранятся в качестве снимков. Обратите внимание, что версия 6869 недоступна, поскольку, например, компьютер был выключен и более новая версия обновления стала доступна до того, как была загружена версия 6869. Если в поле **Количество снимков, хранящихся локально** установить значение 2 и нажать кнопку **Откат**, программа вернется к версии 6868 базы данных сигнатур вирусов (включая модули программы). Это может занять некоторое время. Чтобы проверить, произведен ли откат к предыдущей версии, в главном окне ESET Smart Security откройте раздел Обновление.

4.5.3 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 конфигурирования запланированной задачи перейдите в раздел **Служебные программы** > **Планировщик**. По умолчанию в ESET Smart Security активированы следующие 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.

4.6 Служебные программы

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

Защита домашней сети: снижение риска возникновения проблем с безопасностью при работе в сети. Для получения дополнительных сведений щелкните здесь.

Защита банковской оплаты: ESET Smart Security защищает номера кредитных карт и другие конфиденциальные личные данные при использовании веб-сайтов интернет-банкинга или веб-сайтов оплаты в Интернете. Будет запущен защищенный браузер, чтобы обеспечить дополнительную защиту для банковских операций. Дополнительные сведения можно найти в этой статье базы знаний ESET.

Антивор: выявляет местонахождение пропавшего устройства в случае потери или кражи и помогает его найти.

Щелкните элемент Дополнительные средства, чтобы отобразить другие средства защиты вашего компьютера.

4.6.1 Защита домашней сети

Защита домашней сети: позволяет обнаруживать, что маршрутизатор взломан, а также делает доступным список устройств вашей сети. Домашние маршрутизаторы весьма уязвимы для вредоносного ПО, используемого для запуска распределенных атак типа «отказ в обслуживании» (DDoS). Данная функция позволяет выявить взломанный маршрутизатор. Кроме того, она предоставляет удобный список подключенных устройств, в котором устройства упорядочены по типам (скажем, принтер, маршрутизатор, мобильное устройство и т. п.), позволяя узнать, кто подключен к сети.

Каждое устройство, подключенное к вашей сети, отображается в представлении локатора. Задержите указатель мыши над значком, чтобы отобразить базовые сведения об устройстве, такие как имя сети и дата последнего просмотра. Щелкните значок, чтобы ознакомиться с подробными сведениями об устройстве.

Для отображения информации обо всех подключенных устройствах в виде таблицы, щелкните элемент  . В табличном представлении отображаются те же данные, что и в представлении локатора, но в удобном для чтения формате. Используя раскрывающийся список, можно фильтровать устройства, основываясь на таких критериях:

- устройства, подключенные только к текущей сети;
- устройства без категории;
- устройства, подключенные ко всем сетям.

Модуль «Защита домашней сети» отображает два диалоговых окна:

К сети подключено новое устройство: если к сети подключается не использовавшееся ранее устройство, когда пользователь подключен, то отображается уведомление.
Найдены новые сетевые устройства: если вы заново подключаетесь к своей домашней сети и в ней обнаруживается ранее не использовавшееся устройство, отображается общая информация.

ПРИМЕЧАНИЕ.
В обоих случаях вас уведомляют, что к сети пытается подключиться неавторизованное устройство.

Обнаружение взломанного маршрутизатора позволяет обнаружить взломанный маршрутизатор и повышает уровень защиты при подключении к сторонней сети. Щелкните элемент **Сканировать маршрутизатор**, чтобы вручную просканировать маршрутизатор, к которому вы подключены.

ВНИМАНИЕ!
Сканировать можно только маршрутизатор у себя дома. Делать это в сети другого человека опасно.

После сканирования маршрутизатора отображается уведомление со ссылкой на базовые сведения.

4.6.2 Защита веб-камеры

Защита веб-камеры: позволяет узнать, какие процессы и приложения осуществляют доступ к подключенной к компьютеру камере. Если нежелательное приложение попытается осуществить доступ к вашей камере, отображается окно уведомления. В нем можно **разрешить** либо **заблокировать** доступ к камере нежелательным процессам и приложениям.

4.6.3 Служебные программы в ESET Smart Security

День **Дополнительные средства** : в этом меню представлены модули, которые помогают упростить процесс администрирования программы, а также содержатся дополнительные возможности администрирования для опытных пользователей.

В этом меню представлены следующие служебные программы.

 Файлы журналов

 Статистика защиты

 Наблюдение

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

 Сетевые подключения (если Персональный файервол включен в программе ESET Smart Security)

 ESET SysInspector

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

 Планировщик

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

 Карантин

ПРИМЕЧАНИЕ.
Компонент ESET SysRescue может быть недоступен для ОС Windows 8 в более ранних версиях продуктов ESET. В таком случае рекомендуется обновить соответствующий продукт или создать диск ESET SysRescue в другой версии Microsoft Windows.

4.6.3.1 Файлы журнала

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

Получить доступ к файлам журнала можно из главного окна программы, щелкнув элемент **Служебные программы**. > **Дополнительные средства** > **Файлы журнала**. Выберите нужный тип журнала в раскрывающемся меню **Журнал**. Доступны указанные ниже журналы.

- **Обнаруженные угрозы**: журнал угроз содержит подробную информацию о заражениях, обнаруженных программой ESET Smart Security. В журнале сохраняется информация о времени обнаружения, названии угрозы, месте обнаружения, выполненных действиях и имени 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 Smart Security. Он содержит информацию о событиях и ошибках, которые произошли во время работы программы. Он должен помогать системным администраторам и пользователям решать проблемы. Зачастую информация, которая содержится в этом журнале, оказывается весьма полезной при решении проблем, возникающих в работе программы.

- **Сканирование компьютера**: в этом окне отображаются результаты всех выполненных вручную или запланированных операций сканирования. Каждая строка соответствует одной проверке компьютера. Чтобы получить подробную информацию о той или иной операции сканирования, дважды щелкните соответствующую запись.

- **HIPS**: здесь содержатся записи о конкретных правилах системы предотвращения вторжений на узел, которые помечены для регистрации. В протоколе отображается приложение, которое запустило операцию, ее результат (разрешение или запрещение правила) и имя правила.
- **Персональный файервол**: в журнале событий файервола отображаются все попытки атак извне, которые были обнаружены персональным файерволом. В нем находится информация обо всех атаках, которые были направлены на компьютер пользователя. В столбце *Событие* отображаются обнаруженные атаки. В столбце *Источник* указываются дополнительные сведения о злоумышленнике. В столбце *Протокол* перечисляются протоколы обмена данными, которые использовались для атаки. Анализ журнала файервола может помочь вовремя обнаружить попытки заражения компьютера, чтобы предотвратить несанкционированный доступ на компьютер.
- **Отфильтрованные веб-сайты**: этот список используется для просмотра списка веб-сайтов, заблокированных при помощи защиты доступа в Интернет или родительского контроля. В каждом журнале указываются время, URL-адрес, пользователь и приложение, с помощью которого установлено подключение к конкретному веб-сайту.
- **Защита от спама**: содержит записи, связанные с сообщениями электронной почты, которые были помечены как спам.
- **Родительский контроль**: содержит список веб-страниц, разрешенных или заблокированных функцией родительского контроля. В столбцах *Тип соответствия* и *Значения соответствия* указывается, какие правила фильтрации были применены.
- **Контроль устройств**: содержит список подключенных к компьютеру съемных носителей и устройств. В журнале регистрируются только те устройства, которые соответствуют правилу контроля. В противном случае в журнале не создаются записи о них. Здесь же отображаются такие сведения, как тип устройства, серийный номер, имя поставщика и размер носителя (при его наличии).
- **Защита веб-камеры**: содержит сведения о приложениях, заблокированных модулем защиты веб-камеры.

Выберите содержимое любого журнала и нажмите клавиши **CTRL + C**, чтобы скопировать его в буфер обмена. Удерживая клавиши **CTRL** и **SHIFT**, можно выбрать несколько записей.

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

Щелкните конкретную запись правой кнопкой мыши, чтобы открыть 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 (диагностика, предупреждения и т. д.).
- **Фильтровать.../Найти...** : при выборе этого параметра на экран выводится окно Поиск в журнале, где 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.

4.6.3.1.1 Файлы журналов

Настройку ведения журнала ESET Smart Security можно открыть из главного окна программы. Нажмите **Настройка** > **Перейти к дополнительным настройкам...** > **Служебные программы** > **Файлы журнала**. Этот раздел используется для настройки управления журналами. Программа автоматически удаляет старые файлы журналов, чтобы сэкономить дисковое пространство. Для файлов журнала можно задать параметры, указанные ниже.

Минимальная степень детализации журнала: определяет минимальный уровень детализации записей о событиях.

- **Диагностика**: регистрируется информация, необходимая для тщательной настройки программы, а также все перечисленные выше записи.
- **Информация**: записываются информационные сообщения, в том числе сообщения об успешном выполнении обновления, а также все перечисленные выше записи.
- **Предупреждения**: записывается информация обо всех критических ошибках и предупреждениях.
- **Ошибки**: регистрируется информация об *ошибках загрузки файлов* и критических ошибках.
- **Критические ошибки**: регистрируются только критические ошибки (ошибки запуска защиты от вирусов, персонального файерволаи т. п.).

Записи в журнале, созданные раньше, чем указано в поле **Автоматически удалять записи старше, чем X дн.**, будут автоматически удаляться.

Оптимизировать файлы журналов автоматически: если этот флажок установлен, файлы журналов будут автоматически дефрагментироваться в тех случаях, когда процент фрагментации превышает значение, указанное в параметре **Если количество неиспользуемых записей превышает (%)**.

Нажмите кнопку **Оптимизировать**, чтобы начать дефрагментацию файлов журналов. При этом удаляются все пустые записи журналов, что улучшает производительность и скорость обработки журналов. Такое улучшение особенно заметно, если в журналах содержится большое количество записей.

Выберите Включить текстовый протокол, чтобы разрешить хранение журналов в другом формате отдельно от файлов журналов.

- **Целевой каталог**: каталог, в котором будут храниться файлы журналов (только для текстового формата и формата CSV). Каждый раздел журнала сохраняется в отдельный файл с предварительно заданным именем (например, в файл *virlog.txt* записывается раздел **Обнаруженные угрозы** файла журнала, если для хранения файлов журнала вами выбран формат обычного текста).

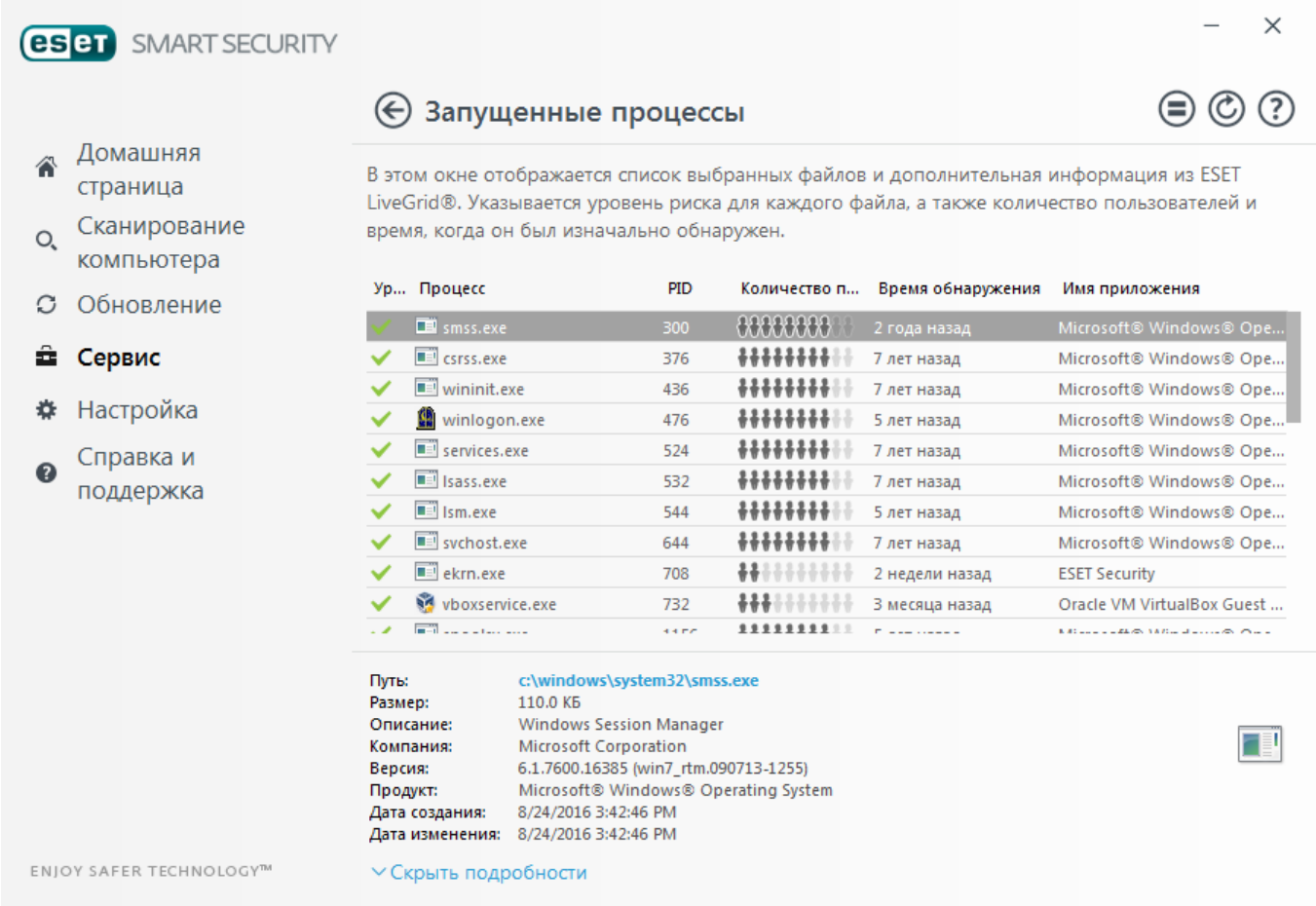
- **Тип**: если выбрать формат **Текст**, журналы будут сохраняться в текстовый файл с символами табуляции в качестве разделителей данных. То же касается формата **CSV**. Если выбрать установку **Событие**, журналы будут сохраняться не в файл, а в журнал событий Windows (его можно просмотреть на панели управления в средстве просмотра событий).

Удалить все файлы журнала: будут удалены все сохраненные журналы, выбранные в раскрывающемся списке **Тип**. После удаления журналов появится уведомление о завершении процесса удаления.

ПРИМЕЧАНИЕ
Для ускорения разрешения проблем специалисты ESET иногда могут запрашивать у пользователей журналы с их компьютеров. ESET Log Collector облегчает сбор необходимой информации. Дополнительные сведения о сборщике журналов ESET см. в этой статье базы знаний ESET.

4.6.3.2 Запущенные процессы

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



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

Уровень риска: в большинстве случаев ESET Smart Security и технология ThreatSense 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).

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

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

Количество пользователей: количество пользователей данного приложения. Эта информация собирается технологией ThreatSense.

Время обнаружения: время, прошедшее с момента обнаружения приложения технологией ThreatSense.

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

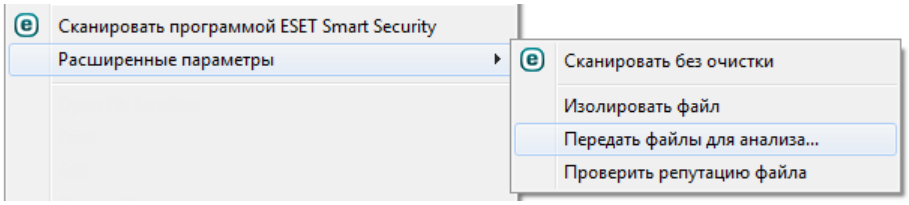
Имя приложения: конкретное имя программы или процесса.

Открыть новое окно: сведения о запущенных процессах будут отображены в новом окне.

Щелкните приложение, чтобы отобразить указанные ниже сведения о нем.

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

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



4.6.3.3 Статистика защиты

Для просмотра диаграммы статистических данных, связанных с модулями защиты ESET Smart Security, нажмите **Служебные программы** > **Статистика защиты**. Выберите интересующий вас модуль защиты в раскрывающемся списке **Статистика**, чтобы отобразить соответствующую диаграмма и ее легенду. Если навести указатель мыши на элемент в легенде, на диаграмме отобразятся данные только для этого элемента.

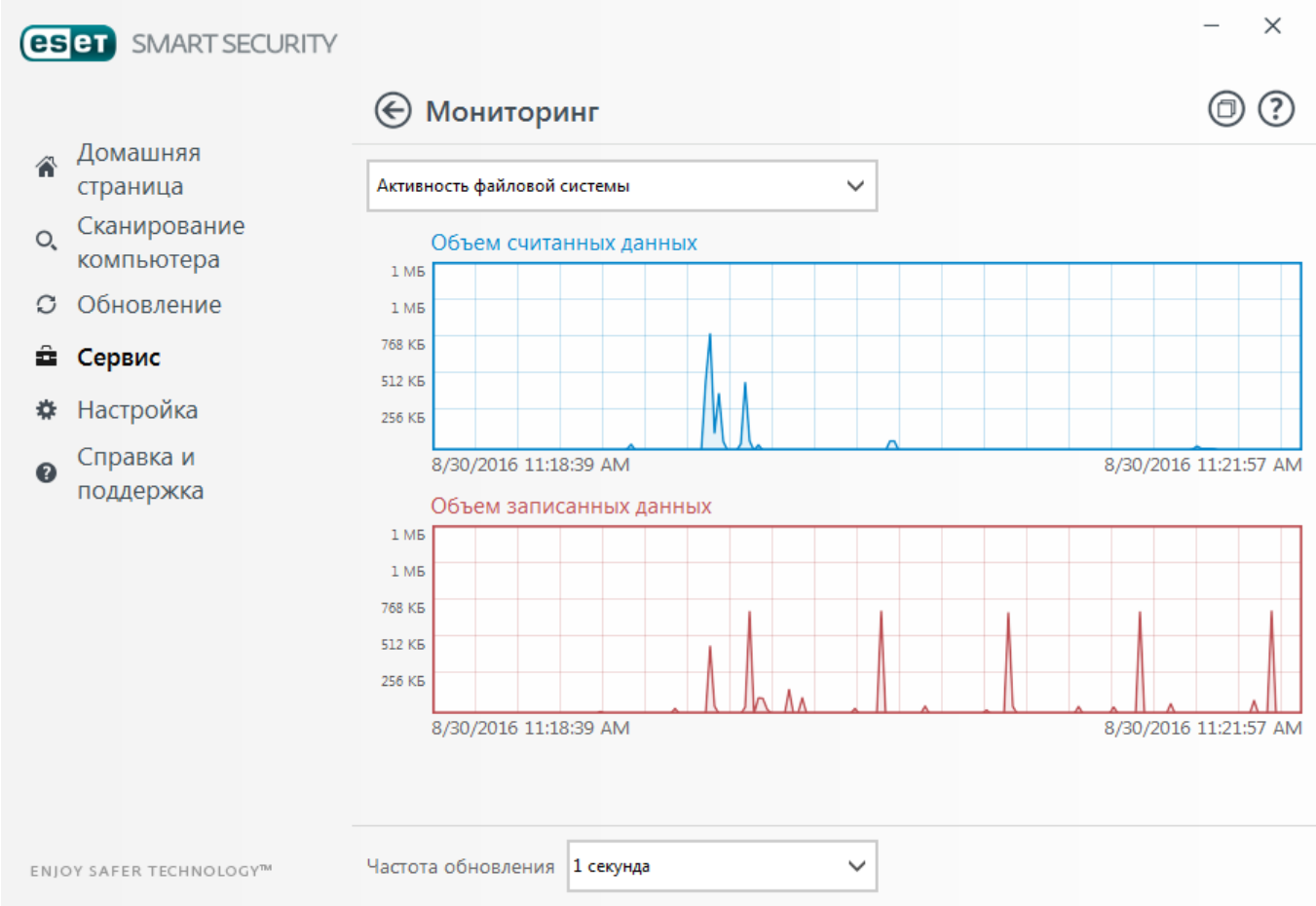
Доступны следующие статистические диаграммы.

- **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.
- **Защита почтового клиента от спама**: отображение статистики защиты от спама с момента последнего запуска.

Под статистическими диаграммами показано общее количество просканированных объектов, последний просканированный объект и метка времени статистики. Нажмите **Сброс**, чтобы удалить всю статистическую информацию.

4.6.3.4 Наблюдение

Чтобы просмотреть текущую **активность файловой системы** в виде графика, щелкните **Служебные программы** > **Дополнительные средства** > **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.

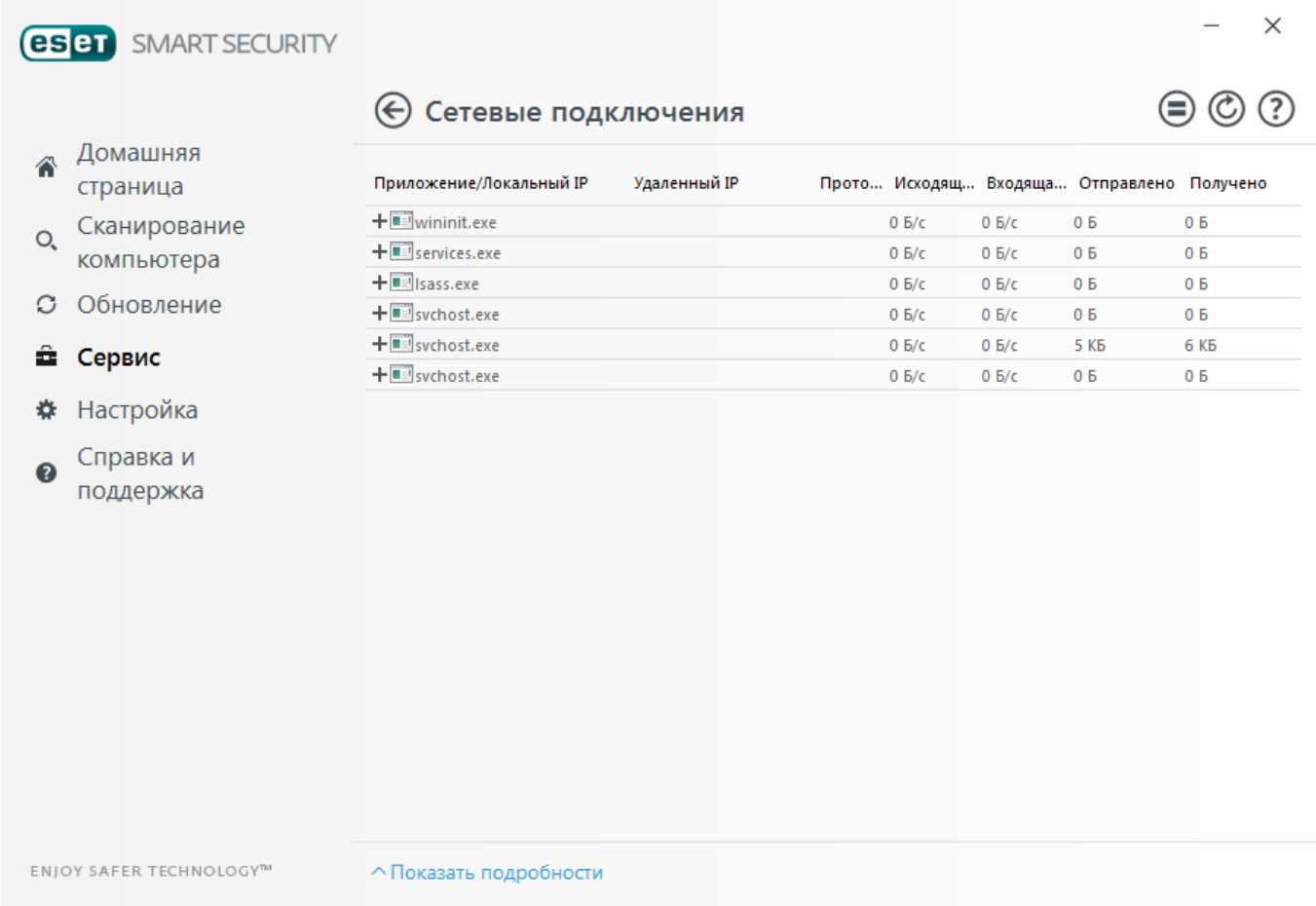
- **Шаг: 1 секунда**: диаграмма обновляется каждую секунду, временная шкала охватывает последние 10 минут.
- **Шаг: 1 минута (последние 24 часа)**: диаграмма обновляется каждую минуту, временная шкала охватывает последние 24 часа.
- **Шаг: 1 час (последний месяц)** диаграмма обновляется каждый час, временная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

На вертикальной оси **графика активности файловой системы** отмечаются прочитанные (синий цвет) и записанные (красный цвет) данные. 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.

В раскрывающемся меню **Активность** также можно выбрать **сетевую активность**. Вид диаграмм и параметры для режимов **Активность файловой системы** и **Сетевая активность** одинаковы за тем исключением, что для последней отображаются полученные (красный цвет) и отправленные (голубой цвет) данные.

4.6.3.5 Сетевые подключения

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



Первая строка содержит имя приложения и скорость передачи его данных. Для просмотра всего списка соединений отдельного приложения (а также для получения более подробной информации) нажмите **+**.

Столбцы

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

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

Протокол: используемый протокол передачи данных.

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

Отправлено/Получено: объем переданных данных в рамках соединения.

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

Щелкните подключение правой кнопкой мыши, чтобы просмотреть дополнительные параметры, в том числе следующие:

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

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

Показывать ожидание соединения: установите этот флажок, чтобы отображались только подключения, по которым в настоящий момент не происходит обмена данными, но для которых система уже открыла порт и

ожидает подключения.

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

Обновить скорость: выберите периодичность обновления активных подключений.

Обновить сейчас: перезагрузка окна «Сетевые подключения».

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

Временно запретить обмен данными для процесса: запретить текущие соединения для данного приложения. При создании нового соединения файервол использует предопределенное правило. Описание параметров см. в разделе Настройка и использование правил.

Временно разрешить обмен данными для процесса: разрешить текущие соединения для данного приложения. При создании нового соединения файервол использует предопределенное правило. Описание параметров см. в разделе Настройка и использование правил.

4.6.3.6 ESET SysInspector

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

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.

- **Показать**: открытие созданного журнала. 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 выбран один или несколько файлов 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**: удаление выделенных журналов из списка.
- **Удалить все**: удаление всех журналов.
- **Экспорт...**: экспорт журнала в файл или архив в формате *XML*.

4.6.3.7 Планировщик

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

Перейти к планировщику можно из главного окна программы ESET Smart Security, 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 (кнопки **Добавить...** и **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;**
- **регулярная проверка последней версии программы** (см. раздел Режим обновления);
- **автоматическая проверка файлов при запуске системы** (после входа пользователя в систему);
- **автоматическая проверка файлов при запуске системы** (после успешного обновления базы данных сигнатур вирусов).

Чтобы изменить параметры запланированных задач (как определенных по умолчанию, так и пользовательских), щелкните правой кнопкой мыши нужную задачу и выберите в контекстном меню команду **Изменить...** или выделите задачу, которую необходимо изменить, а затем нажмите кнопку **Изменить...**.

Добавление новой задачи

1. Щелкните **Добавить задачу** в нижней части окна.
2. Введите имя задачи.

3. Выберите нужную задачу в раскрывающемся меню.

- **Запуск внешнего приложения**: планирование исполнения 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.
- **Обновление**: планирование задачи обновления, в рамках которой обновляется база данных сигнатур вирусов и программные модули.

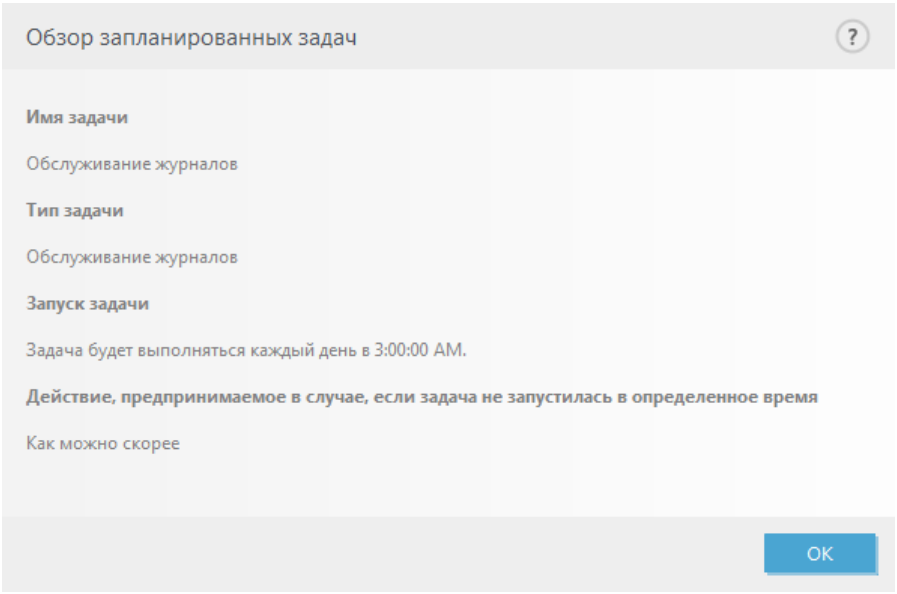
4. Чтобы активировать задачу, установите переключатель в положение **Включено** (это можно сделать позже, установив/сняв флажок в списке запланированных задач), нажмите кнопку **Далее** и выберите один из режимов времени выполнения:

- **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 указанное время в выбранный день недели.
- **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**.



4.6.3.8 ESET SysRescue

ESET SysRescue — это утилита для создания загрузочного диска, содержащего одно из решений ESET Security:ESET NOD32 Antivirus, <%ESET_INTERNET_SECURITY%>, ESET Smart Security, <% ESET_SMART_SECURITY_PREMIUM%> или какой-либо серверный продукт. Главным преимуществом ESET SysRescue является то, что решение ESET Security работает независимо от операционной системы компьютера, имея непосредственный доступ к жесткому диску и файловой системе. Это позволяет удалять такие заражения, которые в обычной ситуации (например, при запущенной операционной системе и т. п.) удалить невозможно.

4.6.3.9 ESET LiveGrid®

(основанная на передовой системе своевременного обнаружения ESET ThreatSense.Net) использует данные от пользователей ESET со всего мира и отправляет их в вирусную лабораторию ESET. Сеть ESET LiveGrid® позволяет получать подозрительные образцы и метаданные из реальных условий, поэтому мы можем незамедлительно реагировать на потребности пользователей и обеспечить готовность ESET к обезвреживанию новейших угроз. Дополнительную информацию о ESET LiveGrid® см. в глоссарии.

Пользователь может проверять репутацию запущенных процессов и файлов непосредственно в интерфейсе программы или в контекстном меню, благодаря чему становится доступна дополнительная информация из ESET LiveGrid®. Существует два варианта работы.

1. Можно принять решение не включать ESET LiveGrid®. Функциональность программного обеспечения при этом не ограничивается, но в некоторых случаях система ESET Smart Security может быстрее обрабатывать новые угрозы, чем обновление базы данных сигнатур вирусов.
2. Можно сконфигурировать ESET LiveGrid® так, чтобы отправлялась анонимная информация о новых угрозах и файлах, содержащих неизвестный пока опасный код. Файл может быть отправлен в ESET для тщательного анализа. Изучение этих угроз поможет компании ESET обновить средства обнаружения угроз.

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 Smart Security 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.

Меню настройки ESET LiveGrid®содержит несколько параметров для включения и отключения системы ESET LiveGrid®, предназначенной для отправки подозрительных файлов и анонимной статистической информации в лабораторию ESET. Эти параметры доступны через дерево расширенных параметров в разделе **Служебные программы** > **ESET LiveGrid®**.

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

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. При каждой отправке файлов или статистики в журнал событий будут вноситься записи.

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 LiveGrid® 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.

4.6.3.9.1 Подозрительные файлы

При обнаружении подозрительного файла его можно отправить в исследовательскую лабораторию ESET для анализа. Если это вредоносное приложение, информация о нем будет включена в следующее обновление сигнатур вирусов.

Фильтр исключения: этот вариант позволяет исключить из отправки определенные файлы или папки. Перечисленные в этом списке файлы никогда не будут передаваться в исследовательскую лабораторию ESET для анализа, даже если они содержат подозрительный код. Например, может быть полезно исключить файлы, в которых может присутствовать конфиденциальная информация, такие как документы и электронные таблицы. Файлы наиболее распространенных типов (.doc и т. п.) исключаются по умолчанию. При желании можно дополнять список исключенных файлов.

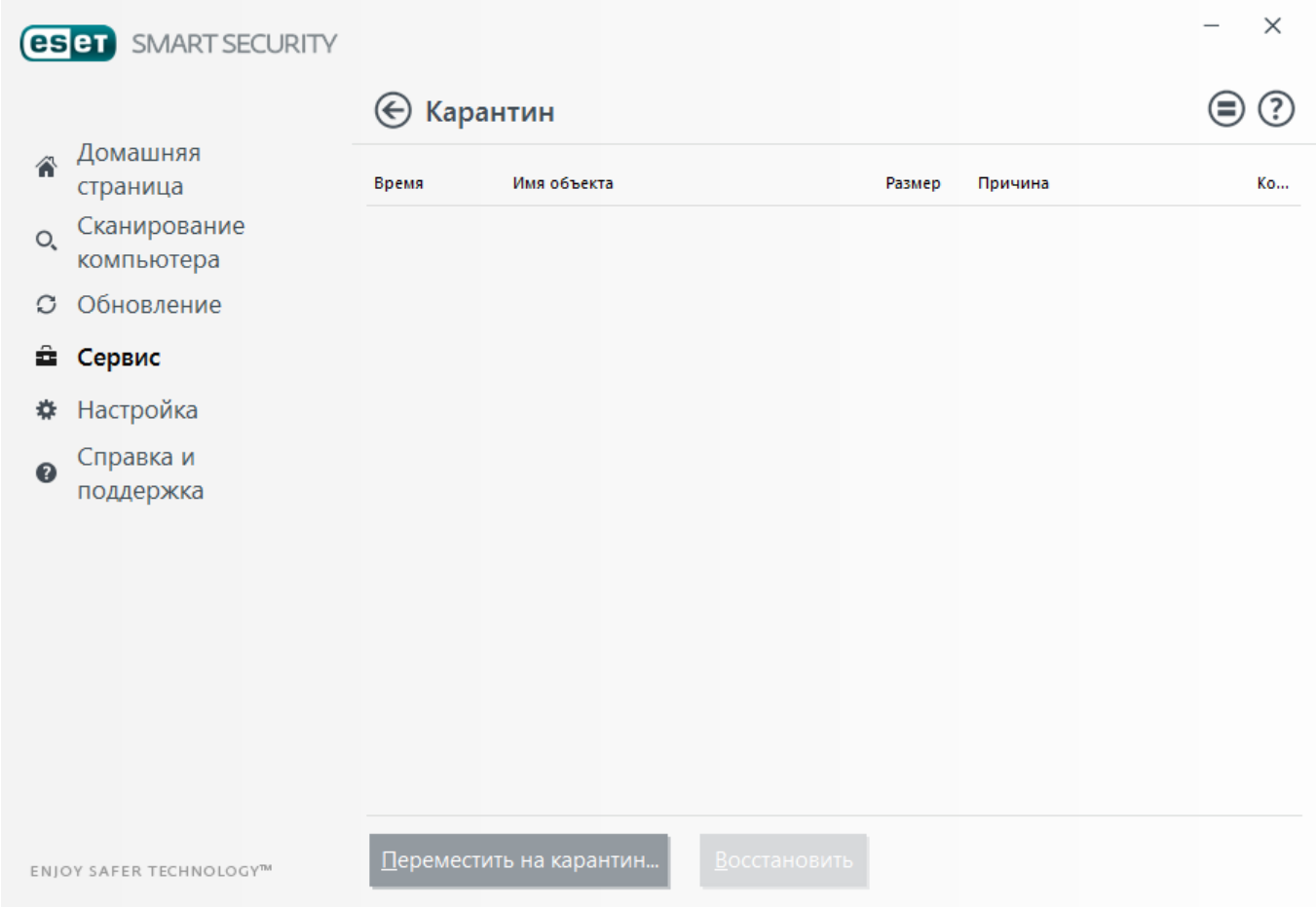
Ваш адрес электронной почты (необязательно): можно отправить адрес электронной почты вместе с подозрительными файлами, чтобы специалисты ESET могли обратиться к вам, если для анализа потребуется дополнительная информация. Имейте в виду, что компания ESET не отправляет ответы пользователям без необходимости.

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.

4.6.3.10 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 Smart Security 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 исследовательскую 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 Smart Security автоматически помещает удаленные файлы на карантин (если этот параметр не был отменен пользователем в окне предупреждения). При желании любой подозрительный файл можно поместить на карантин вручную с помощью кнопки **Карантин...**. При этом исходная копия файла не удаляется. Для этого также можно воспользоваться контекстным меню, щелкнув правой кнопкой мыши окно **Карантин** и выбрав пункт **Карантин...**.

Восстановление из карантина

Файлы, находящиеся на карантине, можно восстановить в исходном месте. Для этого предназначена функция **Восстановить**, доступная в контекстном меню определенного файла, отображающегося в окне карантина. Если файл помечен как потенциально нежелательная программа, включается параметр **Восстановить и исключить из сканирования**. Дополнительную информацию об этом типе приложения см. в глоссарии. Контекстное меню содержит также функцию **Восстановить в...**, которая позволяет восстановить файл в месте, отличном от исходного.

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

Отправка файла из карантина

Если на карантин помещен файл, который не распознан программой, или файл неверно квалифицирован как зараженный (например, в результате ошибки эвристического метода) и изолирован, передайте файл в вирусную лабораторию ESET. Чтобы отправить файл из карантина, щелкните его правой кнопкой мыши и выберите пункт **Передать на анализ**.

4.6.3.11 Прокси-сервер

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 программе ESET Smart Security 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 Smart Security 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** и укажите номер его порта в поле **Порт**.

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

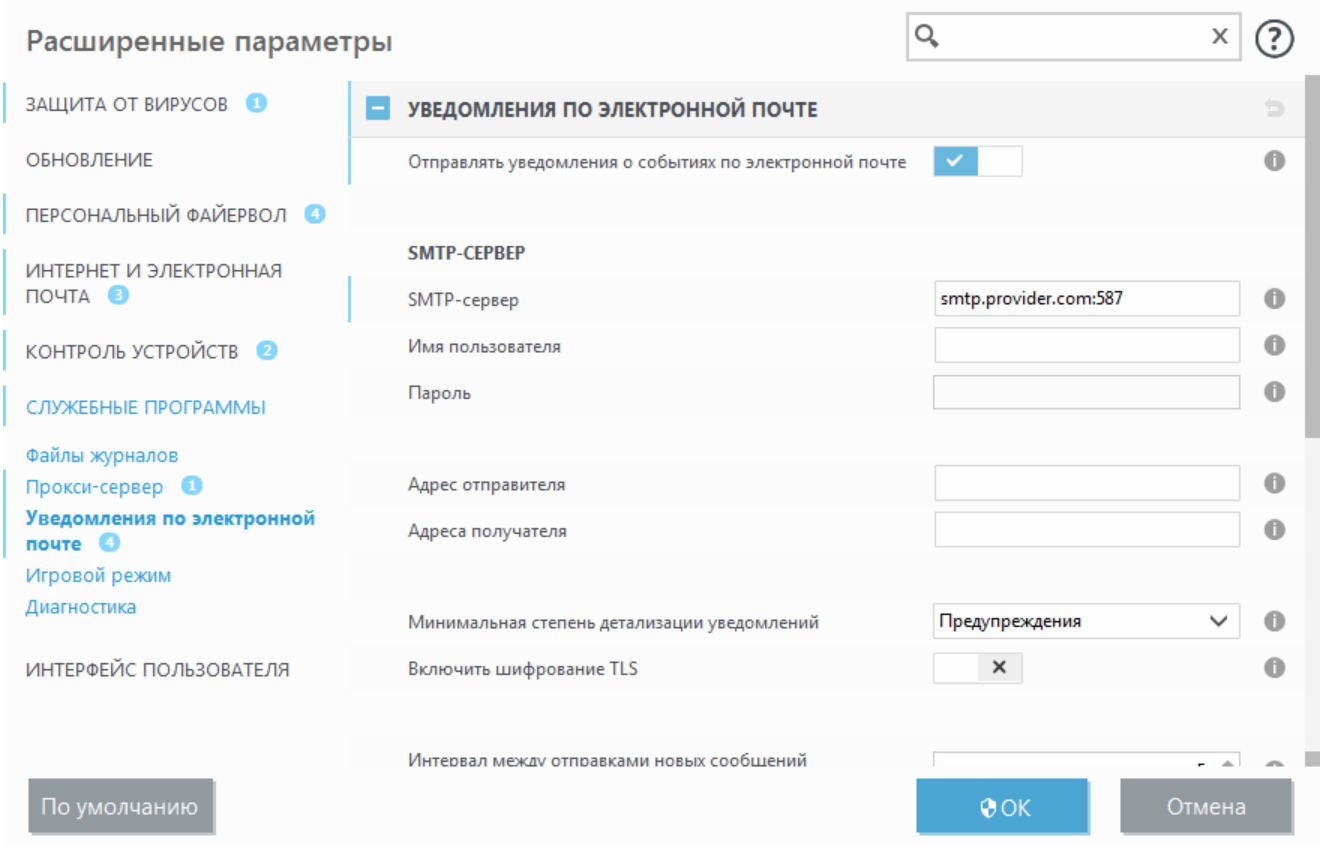
ПРИМЕЧАНИЕ.
В настройках в области **Прокси-сервер** имя пользователя и пароль нужно вводить вручную.

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 области расширенных параметров обновления (последовательно откройте **Дополнительные настройки** > **Обновление** > **Прокси-сервер HTTP** и в раскрывающемся списке **Режим прокси-сервера** выберите элемент **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.

4.6.3.12 Уведомления по электронной почте

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 Smart Security поддерживает SMTP-серверы, использующие шифрование TLS.

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

Адрес отправителя: в этом поле указывается адрес отправителя, который будет отображаться в заголовке писем с уведомлением.

Адрес получателя: в этом поле указывается адрес получателя, который будет отображаться в заголовке писем с уведомлением.

В раскрывающемся списке **Минимальная степень детализации уведомлений** можно выбрать начальный уровень отправляемых уведомлений.

- **Диагностика**: регистрируется информация, необходимая для тщательной настройки программы, а также все перечисленные выше записи.
- **Информация**: 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 оправками новых сообщений электронной почты (мин.): время в минутах, спустя которое по электронной почте будут отправляться 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).

4.6.3.12.1 Формат сообщений

В этом окне можно настроить формат сообщений о событиях, отображающихся на удаленных компьютерах.

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.

Ключевые слова (строки, разделенные символом %) в сообщении замещаются реальной информацией о событии. Доступны следующие ключевые слова.

- **%TimeStamp%**: дата и время события.
- **%Scanner%**: задействованный модуль.
- **%ComputerName%**: имя компьютера, на котором произошло событие.
- **%ProgramName%**: программа, создавшая предупреждение.
- **%InfectedObject%**: имя зараженного файла, сообщения и т. п.
- **%VirusName%**: идентифицирующие данные заражения.
- **%ErrorDescription%**: описание события, не имеющего отношения к вирусам.

Ключевые слова **%InfectedObject%** и **%VirusName%** используются только в предупреждениях об угрозах, а **%ErrorDescription%** — только в сообщениях о событиях.

Использовать символы местного алфавита: преобразование сообщений с использованием кодировки 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).

4.6.3.13 Выбор образца для анализа

Диалоговое окно отправки файлов позволяет отправить файл или сайт в ESET для анализа. Чтобы открыть это окно, выберите **Служебные программы** > **> Дополнительные средства** > > **Отправка образца на анализ**. При обнаружении на компьютере файла, проявляющего подозрительную активность, или подозрительного сайта в Интернете его можно отправить в исследовательскую 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 файл в ESET, убедитесь в том, что проблема соответствует одному из следующих критериев:

- файл совсем не обнаруживается;
- файл неправильно обнаруживается как угроза.

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

В раскрывающемся меню **Причина отправки файла** 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. Образец можно **отправить анонимно**. 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.

4.6.3.14 Центр обновления Microsoft Windows®

Функция обновления Windows является важной составляющей защиты пользователей от вредоносных программ. По этой причине обновления Microsoft Windows следует устанавливать сразу после их появления. Программное обеспечение ESET Smart Security 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.

4.7 Интерфейс

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

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

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.

Для обеспечения максимального уровня безопасности программного обеспечения можно предотвратить несанкционированное изменение, защитив параметры паролем с помощью служебной программы Параметры доступа.

4.7.1 Элементы интерфейса

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

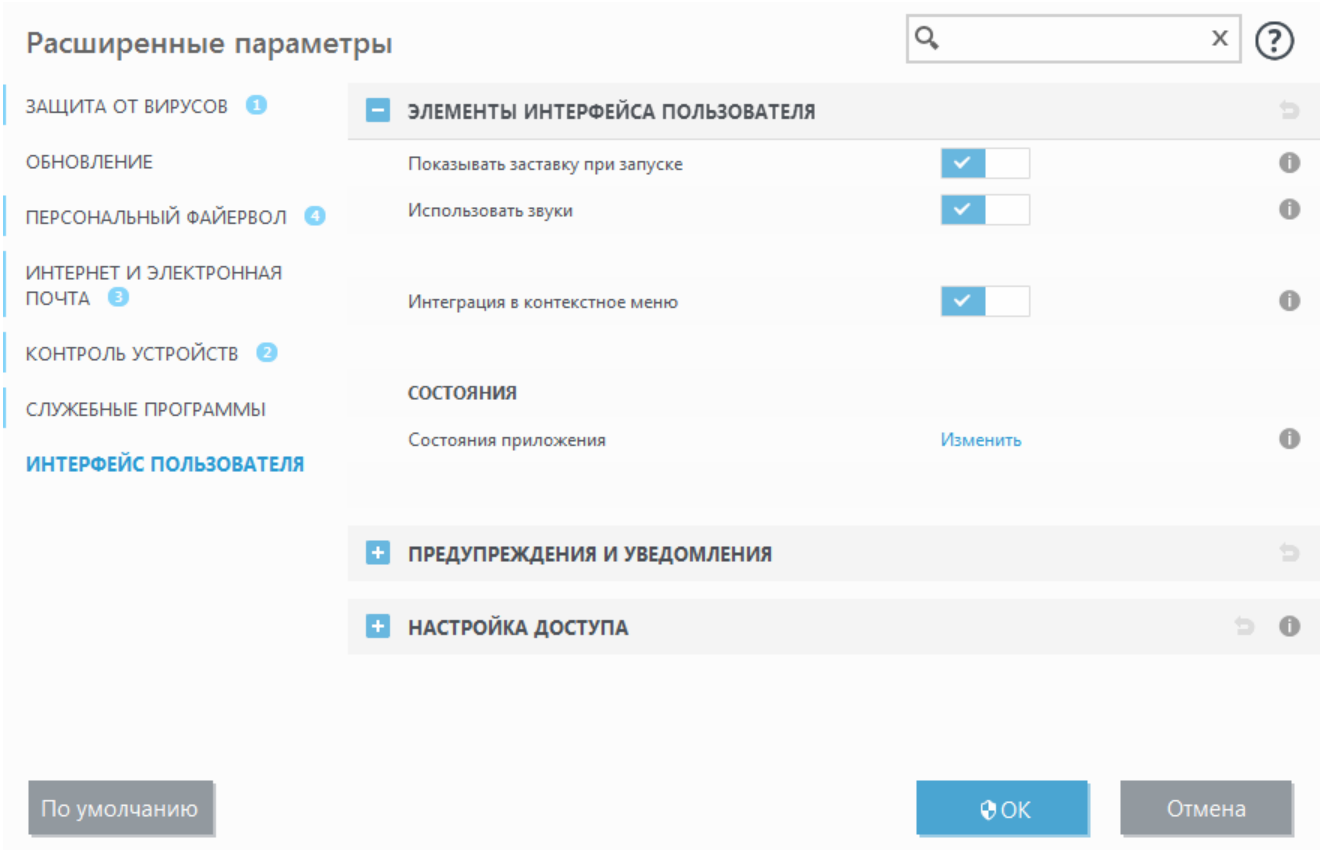
Чтобы отключить заставку ESET Smart Security, снимите флажок **Показывать заставку при запуске**.

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

Интегрировать с контекстным меню: можно интегрировать элементы управления ESET Smart Security в контекстное меню.

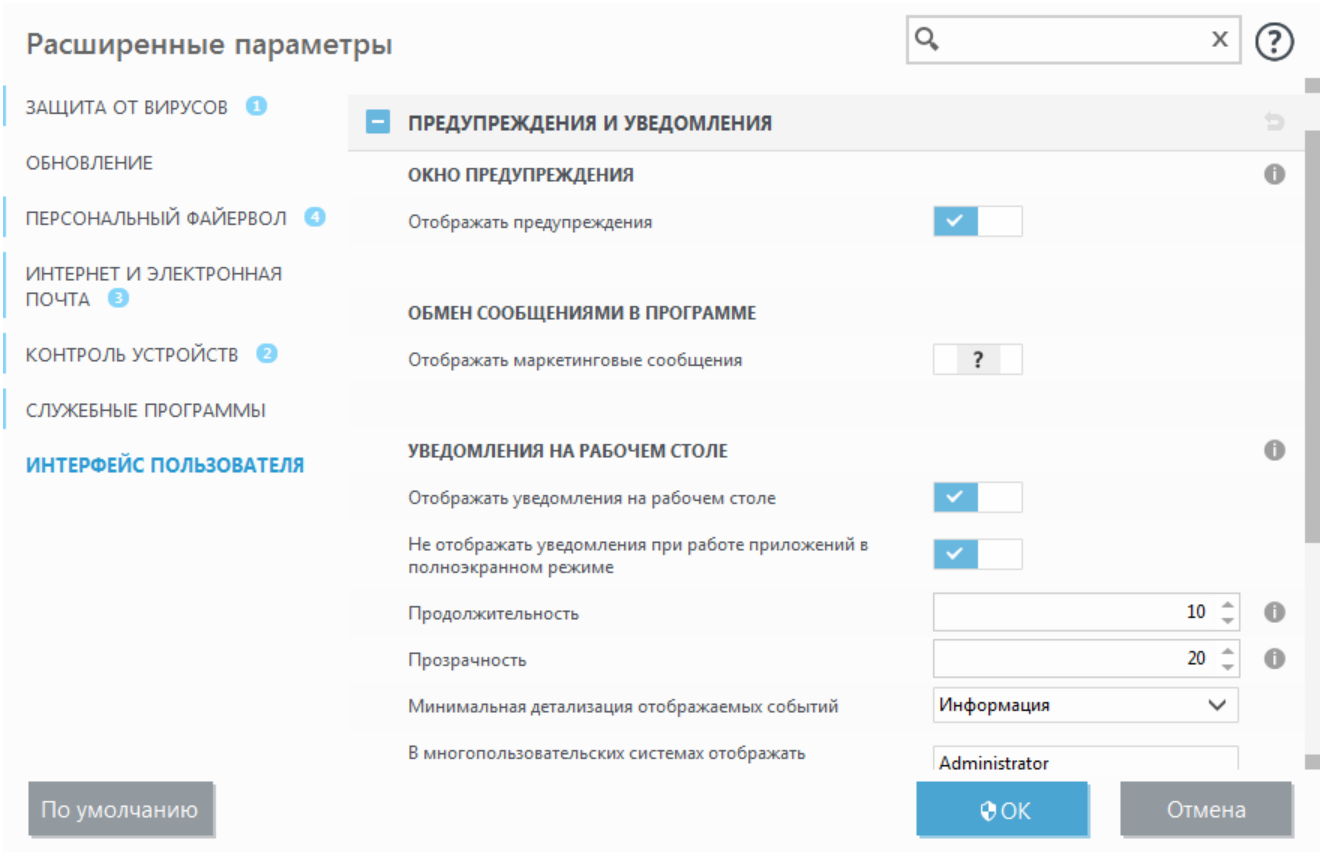
Состояния

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



4.7.2 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 Smart Security. 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; делать это следует только в некоторых особых ситуациях. В большинстве случаев рекомендуется оставить для этого параметра значение по умолчанию (включен).

Обмен сообщениями в программе

Отображать маркетинговые сообщения: функция внутрипрограммного обмена сообщениями предназначена для информирования пользователей о новостях ESET и для других сообщений. Снимите этот флажок, если не хотите получать маркетинговые сообщения.

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 детальные параметры, такие как время отображения и прозрачность окна уведомлений, можно изменить, выполнив приведенные ниже инструкции.

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

- **Диагностика**: регистрируется информация, необходимая для тщательной настройки программы, а также все перечисленные выше записи.
- **Информация**: записываются информационные сообщения, в том числе сообщения об успешном выполнении обновления, а также все перечисленные выше записи.
- **Предупреждения**: записывается информация обо всех критических ошибках и предупреждениях.
- **Ошибки**: записываются сведения об ошибках загрузки файлов и критических ошибках.
- **Критические ошибки**: регистрируются только критические ошибки (ошибки запуска защиты от вирусов, встроенного файерволаи 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, что позволяет одновременно подключаться к системе нескольким пользователям. Обычно это системный или сетевой администратор. Эта функция особенно полезна для терминальных серверов при условии, что 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.

4.7.2.1 Дополнительные настройки

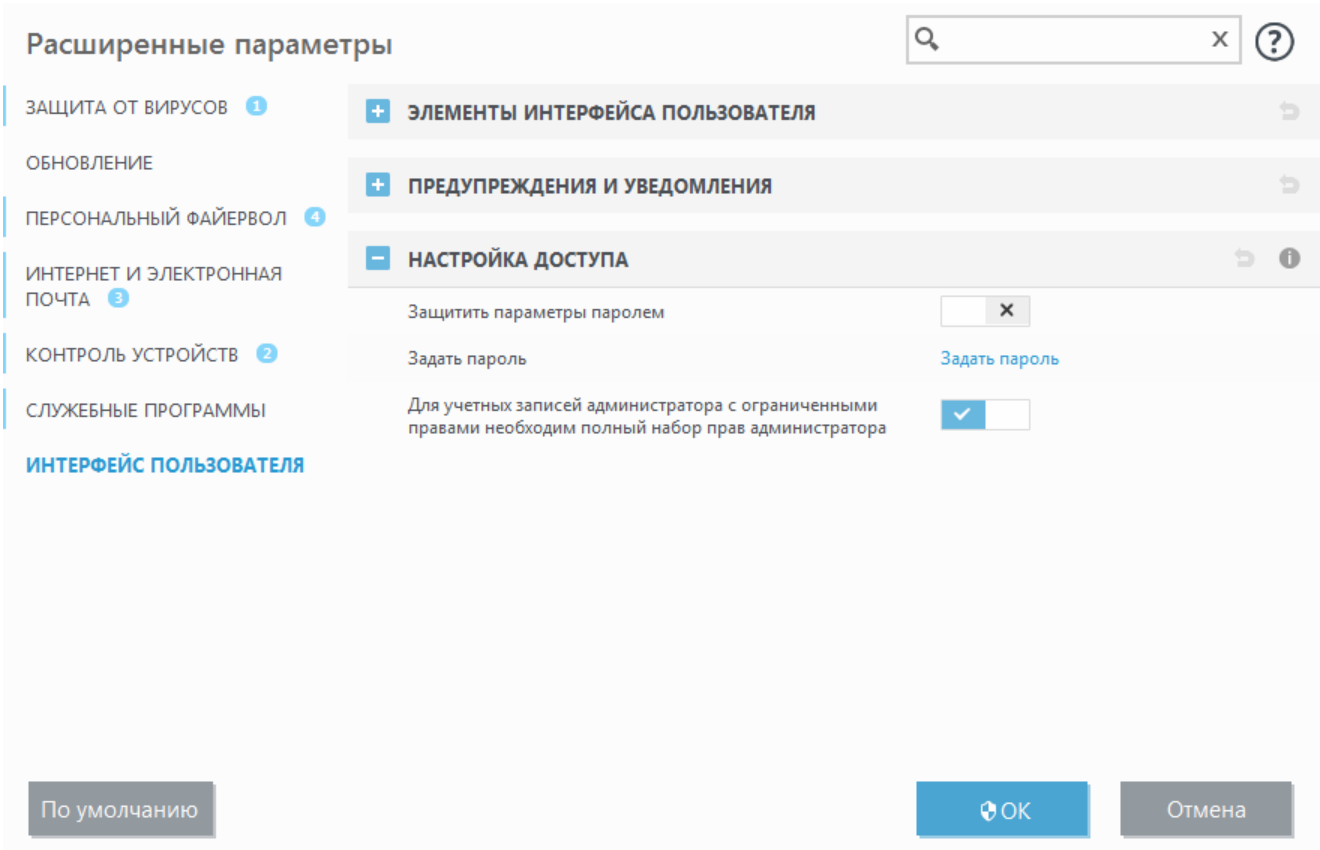
В раскрывающемся меню **Минимальная детализация отображаемых событий** можно выбрать начальный уровень серьезности предупреждений и уведомлений, которые следует отображать.

- **Диагностика**: регистрируется информация, необходимая для тщательной настройки программы, а также все перечисленные выше записи.
- **Информация**: записываются информационные сообщения, в том числе сообщения об успешном выполнении обновления, а также все перечисленные выше записи.
- **Предупреждения**: записывается информация обо всех критических ошибках и предупреждениях.
- **Ошибки**: регистрируется информация об *ошибках загрузки файлов* и критических ошибках.
- **Критические ошибки**: регистрируются только критические ошибки (ошибки запуска защиты от вирусов, персонального файерволаи т. п.).

Последний параметр этого раздела позволяет сконфигурировать, 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. Эта функция особенно полезна для терминальных серверов при условии, что все системные уведомления отправляются администратору.

4.7.3 Настройка доступа

Настройки ESET Smart Security являются важной составной частью вашей политики безопасности. Несанкционированное изменение параметров может нарушить стабильность работы системы и ослабить ее защиту. Для предотвращения несанкционированного изменения параметры ESET Smart Security можно защитить паролем.



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

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

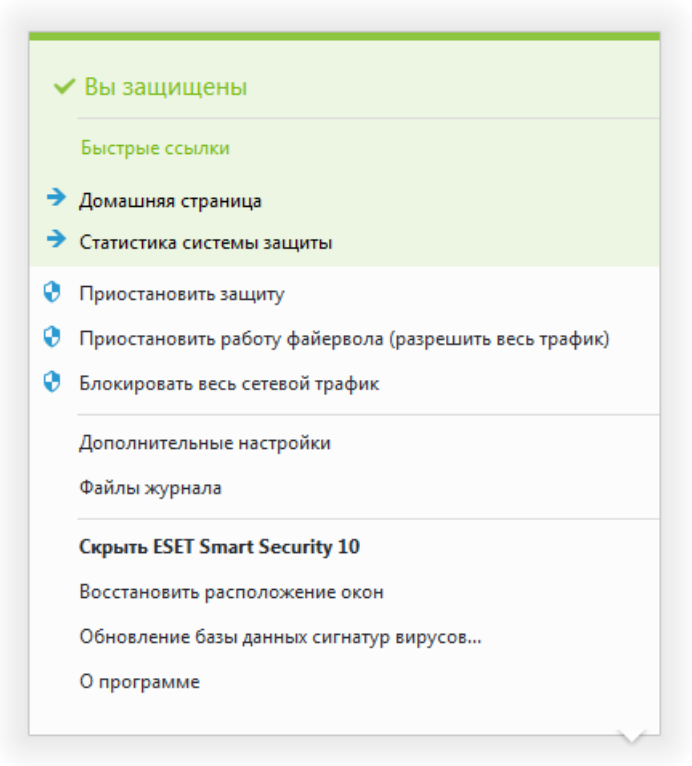
Требуется полный набор прав администратора для ограниченных учетных записей администратора: выберите этот параметр, чтобы при изменении определенных параметров системы для текущего пользователя (если у такого пользователя нет прав администратора) отображался запрос на ввод имени пользователя и пароля администратора (аналогично контролю учетных записей в Windows Vista и Windows 7). К таким изменениям относится отключение модулей защиты или файервола. В ОС Windows XP, где нет контроля учетных записей, для пользователей будет доступен параметр **Требуются права администратора (система без поддержки UAC)**.

Только для Windows XP:

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

4.7.4 Меню программы

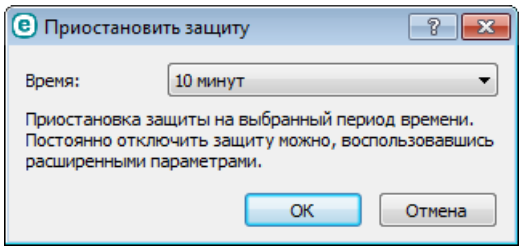
К некоторым наиболее важным функциям и настройкам можно получить доступ, щелкнув правой кнопкой мыши значок на панели задач .



Быстрые ссылки: отображение наиболее часто используемых компонентов ESET Smart Security. К ним можно быстро перейти через меню программы.

Приостановить защиту: на экран выводится диалоговое окно для подтверждения. В нем можно отключить защиту от вирусов и шпионских программ, посредством которой, путем контроля обмена файлами и данными через Интернет и электронную почту, предотвращаются атаки на компьютер со стороны злонамеренных систем.

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



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

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

Дополнительные настройки: установите этот флажок, чтобы перейти к дереву **Дополнительные настройки**. Дерево дополнительных настроек можно отобразить и другими способами, например нажать клавишу F5 или использовать меню **Настройка** > **Дополнительные настройки**.

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

СкрытьESET Smart Security: позволяет скрыть окно ESET Smart Security.

Сбросить настройки макета окна: для окна ESET Smart Security 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 Smart Security и модулях программы. Также здесь отображаются дата окончания срока действия лицензии и данные об операционной системе и системных ресурсах.

5. Для опытных пользователей

5.1 Диспетчер профилей

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

Сканирование компьютера

Предпочтительные параметры сканирования можно сохранить для использования в дальнейшем. Рекомендуется создать отдельный профиль для каждого регулярно используемого сканирования (с различными объектами, методами сканирования и прочими параметрами).

Для создания профиля откройте окно «Дополнительные настройки» (F5) и щелкните **Защита от вирусов** > **Сканирование компьютера по требованию** > **Основное** > **Список профилей**. В окне **Диспетчер профилей** есть раскрывающееся меню **Выбранный профиль**, в котором перечисляются существующие профили сканирования и есть возможность создать новый. Для создания профиля сканирования в соответствии с конкретными потребностями см. раздел Настройка параметров модуля ThreatSense, в котором описывается каждый параметр, используемый для настройки сканирования.

ПРИМЕЧАНИЕ.
Предположим, пользователю требуется создать собственный профиль сканирования, причем конфигурация **Сканировать компьютер** 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 **Выбранный профиль** и настройте остальные параметры в соответствии со своими требованиями, а затем нажмите кнопку **ОК**, чтобы сохранить новый профиль.

Обновление

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

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

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

Добавить...: создание новых профилей обновления.

В нижней части окна находится список существующих профилей.

5.2 Сочетания клавиш

Для более удобной навигации в программе ESET можно использовать следующие сочетания клавиш.

F1	вызов справки
F5	вызов окна расширенных параметров
Вверх/вниз	переход по элементам в программе
-	свертывание узлов дерева расширенных параметров
TAB	перемещение курсора по окну
Esc	закрытие активного диалогового окна

5.3 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 Smart Security. Откройте раскрывающийся список рядом с элементом **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 при анализе ограниченный объем включенной в него информации может не позволить обнаружить ошибки, которые не были вызваны непосредственно потоком, выполнявшимся в момент возникновения проблемы.
- **Полный**: когда неожиданно прекращается работа приложения, регистрируется все содержимое системной памяти. Полный дамп памяти может содержать данные процессов, которые выполнялись в момент создания дампа.

Включить расширенное ведение журнала в персональном файерволе: запись всех сетевых данных, проходящих через персональный файервол в формате PCAP. Это помогает разработчикам диагностировать и устранять проблемы, связанные с персональным файерволом.

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 Windows Vista и более поздних версиях 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*.

Создать дамп диагностики: нажмите кнопку **Создать**, чтобы создать в **целевом каталоге** файлы дампа диагностики.

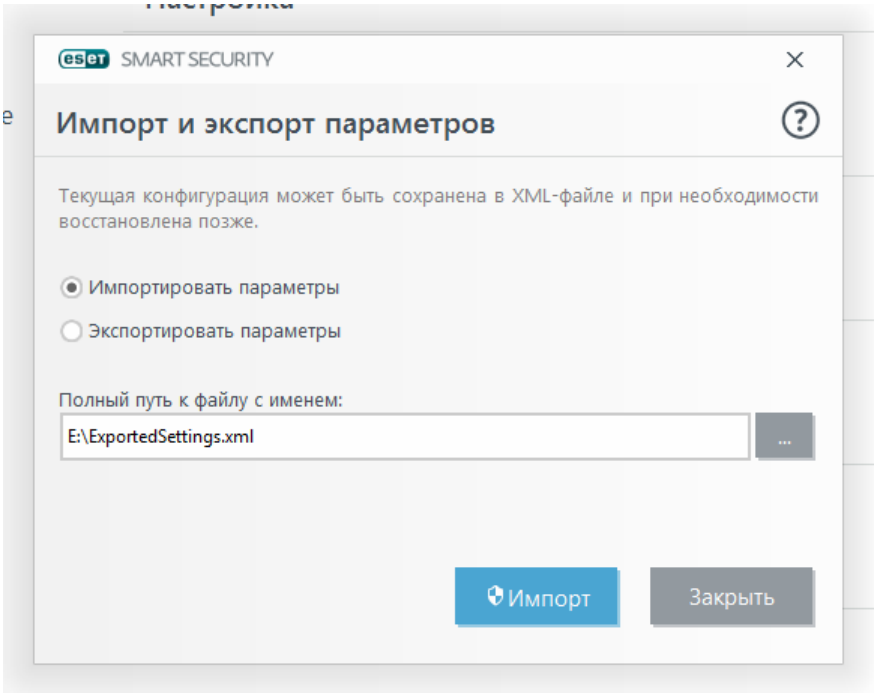
5.4 Импорт и экспорт параметров

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

Импорт и экспорт файлов конфигурации удобны, если нужно создать резервную копию текущей конфигурации программы ESET Smart Security 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 меню выберите пункт **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.

5.5 ESET SysInspector

5.5.1 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 Smart Security.

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.

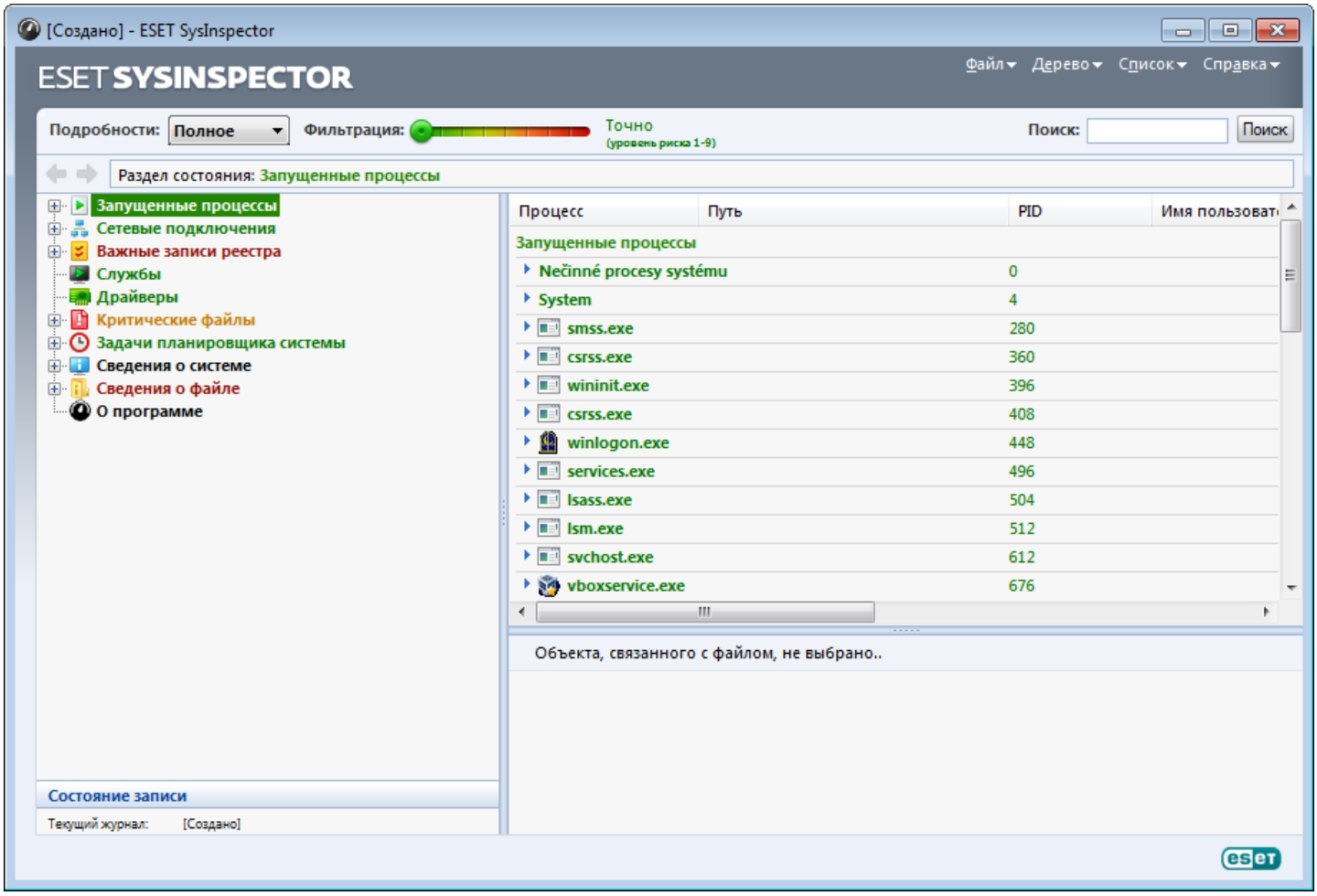
5.5.1.1 Запуск ESET SysInspector

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 Smart Security**).

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

5.5.2 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.).



5.5.2.1 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.

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.

Внимание! 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.

5.5.2.2 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.

5.5.2.2.1 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

5.5.2.3 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.

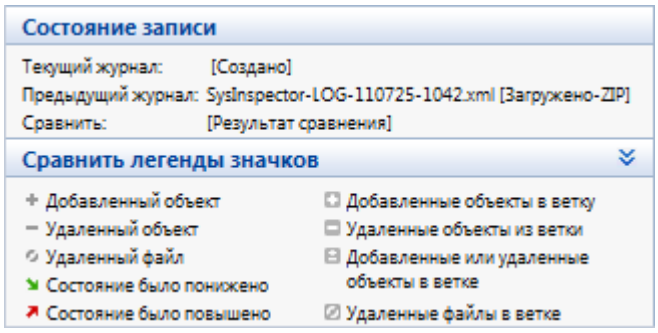
ПРИМЕЧАНИЕ. При сравнении двух файлов журнала в меню **Файл** выберите пункт **Сохранить журнал** и сохраните журнал как файл в формате ZIP. В результате будут сохранены оба файла. Если такой файл впоследствии открыть, содержащиеся в нем журналы сравниваются автоматически.

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

5.5.3 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.

5.5.4 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.

5.5.4.1 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.

5.5.4.2 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.

10) Запланированные задачи

Этот раздел содержит информацию о запланированных задачах.

Пример.

```
10) Scheduled tasks
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe /c
- c:\users\admin\appdata\local\google\update\googleupdate.exe /ua /installsource
- %windir%\system32\appidpolicyconverter.exe
- %windir%\system32\appidcertstorecheck.exe
- aitagent
[...]
```

5.5.4.3 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 службы «%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.

5.5.5 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.

Пример

В системе Windows 2000 есть приложение HyperTerminal, которое находится в папке *C:\Program Files\Windows NT*. Главный исполняемый файл приложения не имеет цифровой подписи, однако программа ESET SysInspector помечает его как подписанный корпорацией Майкрософт. Причиной этому служит ссылка в файле *C:\WINNT \system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat*, которая указывает на файл *C:\Program Files\Windows NT\hypertrm.exe* (главный исполняемый файл приложения HyperTerminal), а файл *sp4.cat* имеет цифровую подпись Майкрософт.

5.5.6 ESET SysInspector как часть приложения ESET Smart Security

Чтобы открыть раздел ESET SysInspector в ESET Smart Security, 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.

5.6 Командная строка

Модуль защиты от вирусов ESET Smart Security 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.

Настройки

/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): ecls.exe попытается автоматически очистить или удалить зараженные файлы. • **тщательная**: ecls.exe попытается автоматически очистить или удалить зараженные файлы без вмешательства пользователя (вам не будет предложено подтвердить удаление файлов). • **наиболее тщательная**: ecls.exe удалит все файлы без проведения очистки независимо от их типа. • **удаление**: ecls.exe удалит все файлы без проведения очистки, кроме важных, таких как системные файлы Windows.
/quarantine	копировать зараженные файлы, если они очищены, в карантин (дополнительно к действию, выполняемому при очистке)
/no-quarantine	не копировать зараженные файлы в карантин

Общие параметры

/help	показать справку и выйти
/version	показать сведения о версии и выйти
/preserve-time	сохранить последнюю отметку о времени доступа

Коды завершения

0	угроз не обнаружено
1	угроза обнаружена и очищена
10	некоторые файлы не удалось просканировать (могут быть угрозами)
50	обнаружена угроза
100	ошибка

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

6. Глоссарий

6.1 Типы заражений

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

6.1.1 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 исследовательскую лабораторию ESET для изучения. В ряде случаев зараженные файлы изменяются настолько, что их невозможно очистить. В таком случае их нужно заменять чистыми копиями.

6.1.2 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 считаные 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.

6.1.3 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.

6.1.4 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 Smart Security доступны преимущества технологии Anti-Stealth, которая также позволяет обнаруживать и устранять активные руткиты.

6.1.5 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.

6.1.6 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.

6.1.7 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.

6.1.8 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 Smart Security 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.

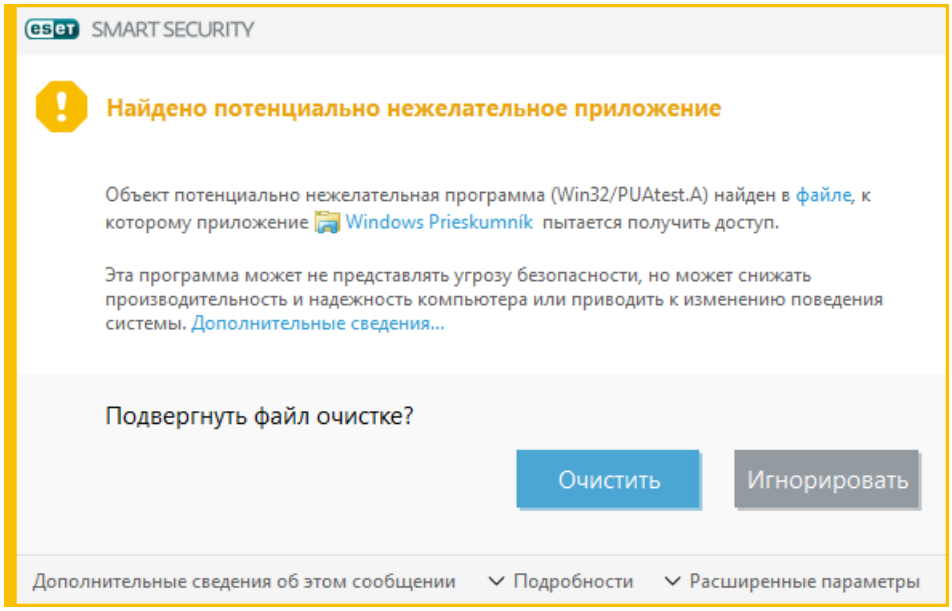
6.1.9 Потенциально нежелательные приложения

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

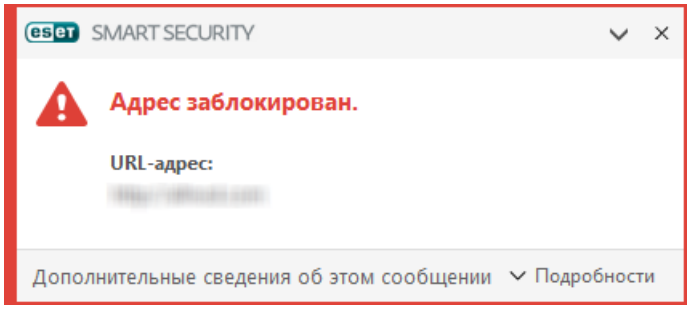
Предупреждение — обнаружена потенциальная угроза

Когда обнаруживается потенциально нежелательное приложение, можно решить, какое действие следует выполнить.

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

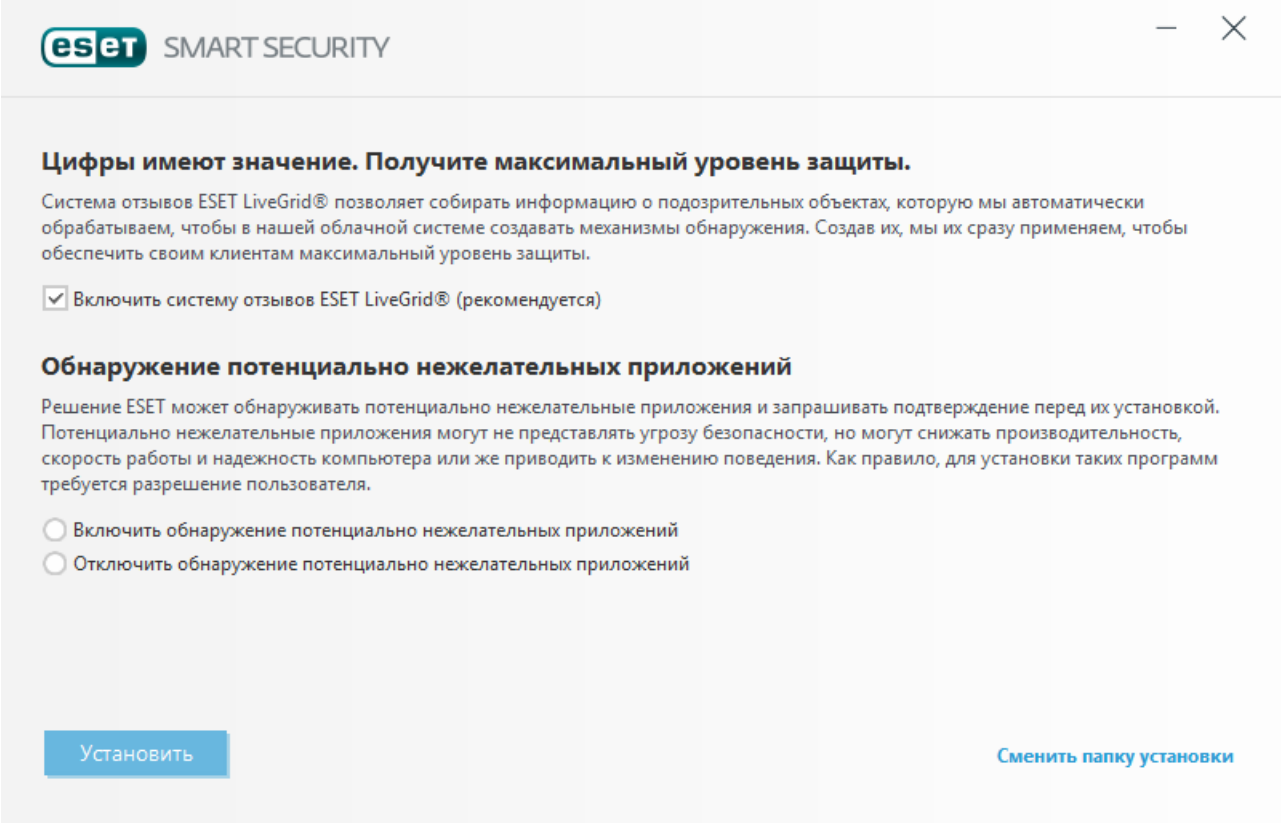


Если обнаруживается потенциально нежелательное приложение и его не удается очистить, отображается уведомление **Адрес заблокирован**. Для получения дополнительных сведений об этом событии перейдите из главного меню в раздел **Служебные программы** > **Дополнительные средства** > **Файлы журналов** > **Отфильтрованные веб-сайты**.



Потенциально нежелательные приложения — параметры

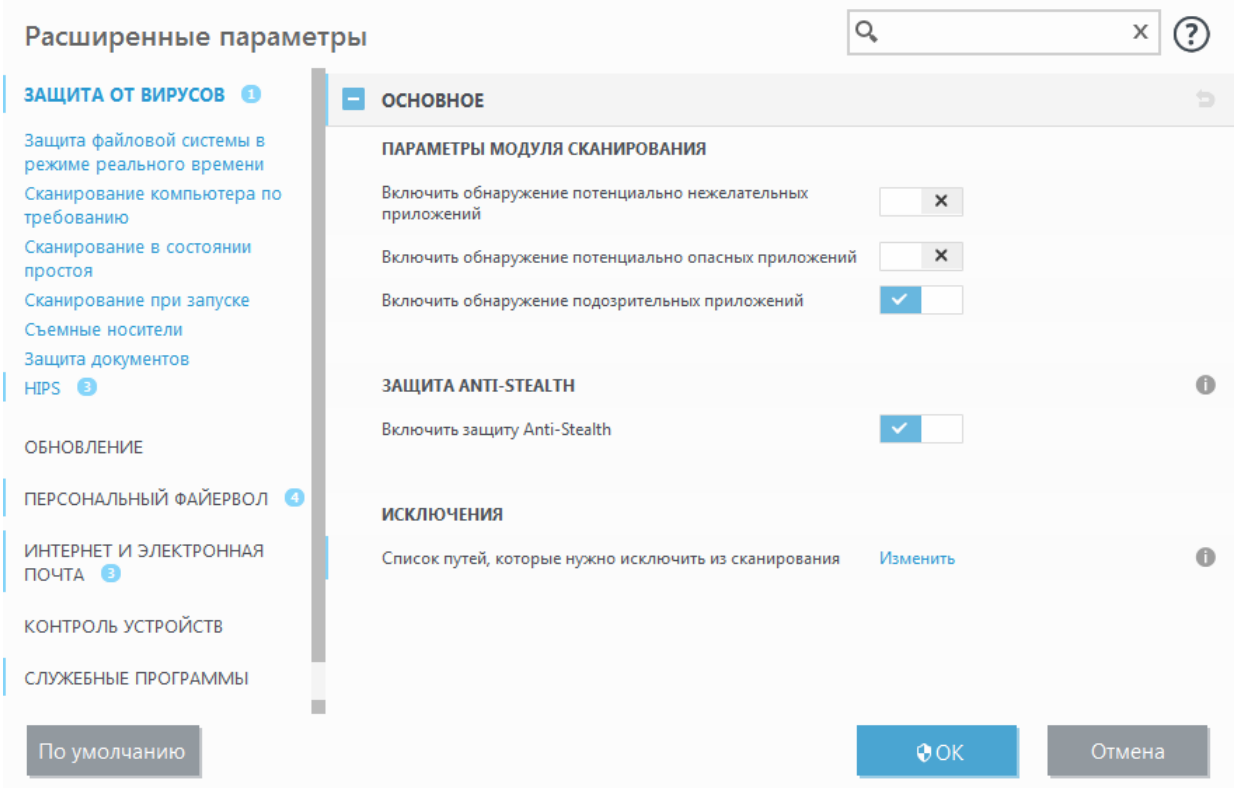
При установке программы ESET можно включить обнаружение потенциально нежелательных приложений (см. изображение ниже).



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 приведенным ниже инструкциям.

1. Откройте программу ESET. Как открыть программу ESET на моем компьютере?
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 рекламной программой, которые могут изменить домашнюю страницу браузера или параметры поиска. При этом файлообменные ресурсы часто не уведомляют поставщиков программного обеспечения или получателей загруженных файлов о внесенных изменениях и скрывают настройки, позволяющие от них отказаться. Именно поэтому компания ESET считает оболочки потенциально нежелательными приложениями и дает пользователям возможность отказаться от их загрузки.

Обновленную версию данной страницы справки см. в этой статье базы знаний ESET.

6.1.10 Ботнет

Бот или веб-робот — это автоматизированная вредоносная программа, которая сканирует блоки сетевых адресов и заражает уязвимые компьютеры. Это позволяет хакерам захватить контроль над множеством компьютеров одновременно и превратить их в ботов (называемых также зомби). Зачастую хакеры используют ботов для заражения больших количеств компьютеров, которые образуют сеть — так называемый ботнет. Как только ботнет проник в ваш компьютер, его могут использовать при распределенных атаках типа «отказ в обслуживании» (DDoS), в качестве прокси, а также для выполнения автоматизированных задач в Интернете без вашего ведома (например, для отправки спаса, вирусов или кражи личной и конфиденциальной информации, такой как банковские учетные данные или номера кредитных карт).

6.2 Типы удаленных атак

Существует множество специальных технологий, с помощью которых злоумышленники могут атаковать удаленные компьютеры. Они подразделяются на несколько категорий.

6.2.1 DoS-атаки

DoS-атаки (атаки типа *отказ в обслуживании*) представляют собой попытку сделать компьютер или сеть недоступными тем пользователями, для которых они предназначены. Обмен данными между пользователями пораженного компьютера затруднен или невозможен в приемлемом режиме. Компьютеры, подвергшиеся действию DoS-атаки, обычно должны быть перезагружены для восстановления нормальной работы.

В большинстве случаев объектами этой атаки становятся веб-серверы, а целью является вывод их из строя и, как следствие, их недоступность на некоторое время.

6.2.2 Атака путем подделки записей кэша DNS

Атака путем подделки записей кэша DNS (сервер доменных имен) позволяет хакерам убедить DNS-сервер любого компьютера в том, что предоставляемые подложные данные являются истинными. Ложная информация кэшируется на определенное время, давая злоумышленникам возможность перезаписать ответы DNS-сервера с IP-адресами. В результате при попытке посещения веб-сайтов пользователь загружает компьютерные вирусы и черви вместо исходного содержимого.

6.2.3 Атаки червей

Компьютерные черви — это содержащие злонамеренный код программы, которые атакуют главные компьютеры и распространяются через сеть. Сетевые черви используют уязвимости системы безопасности различных приложений. Благодаря Интернету они распространяются по всему земному шару за считаные часы после запуска в сеть.

Многих из атак червей (Sasser, SqlSlammer) можно избежать, используя настройки персонального файервола по умолчанию или с помощью блокировки незащищенных и неиспользуемых портов. Очень важно регулярно устанавливать новейшие пакеты обновления операционной системы.

6.2.4 Сканирование портов

Сканирование портов используется, чтобы определить, какие порты компьютера открыты на узле сети. Сканер портов представляет собой программное обеспечение, которое предназначено для поиска таких портов.

Компьютерный порт является виртуальной точкой, которая управляет сетевым трафиком в обоих направлениях. Это является критичным с точки зрения сетевой безопасности. В больших сетях данные, которые собираются с помощью сканера портов, могут помочь выявить потенциальные уязвимости компьютерных систем. Такое использование является допустимым.

Однако сканеры часто используются злоумышленниками для взлома систем безопасности. Первым шагом отправляется серия пакетов на каждый из портов. В зависимости от полученных ответов определяется, какой из портов можно использовать. Сканирование не причиняет вреда само по себе, но следует иметь в виду, что такая активность зачастую является признаком попытки выявления уязвимости и последующей атаки злоумышленников на систему.

Сетевые администраторы обычно советуют блокировать все неиспользуемые порты и защищать используемые от неавторизованного доступа.

6.2.5 TCP-десинхронизация

TCP-десинхронизация — это метод, используемых в атаках подмены одного из участников TCP-соединения. Этот метод основан на процессах, которые происходят, когда порядковый номер приходящего пакета отличается от ожидаемого. Пакеты с неожиданными номерами пропускаются (или сохраняются в специальном буфере, если они попадают в текущее окно соединения).

При десинхронизации обе стороны обмена данными пропускают полученные пакеты. В этот момент злоумышленники могут заразить и передать пакеты с правильным порядковым номером. Злоумышленники могут даже манипулировать обменом данных и вносить в него изменения.

В атаках путем подмены одного из участников целью является внедрение в двухсторонний обмен данными между сервером и клиентом. Многие атаки в этом случае могут быть предотвращены путем использования аутентификации для каждого из сегментов TCP. Кроме того, следует использовать рекомендуемые параметры для сетевых устройств.

6.2.6 SMB Relay

SMB Relay и SMB Relay 2 являются особыми программами, которые способны атаковать удаленные компьютеры. Эти программы используют уязвимость протокола SMB, который встроен в NetBIOS. Если пользователь предоставляет общий доступ к каким-либо папкам через локальную сеть, скорее всего это осуществляется с помощью протокола SMB.

В рамках обмена данными по локальной сети происходит обмен данными хеш-таблиц паролей.

SMB Relay принимает соединения по UDP на портах 139 и 445, транслирует пакеты, которыми обмениваются клиент и сервер, и подменяет их. После подключения и аутентификации соединение с клиентом прерывается. SMB Relay создает новый виртуальный IP-адрес. Новый адрес доступен с помощью следующей команды: net use \\192.168.1.1. После этого доступ к адресу открыт для любой сетевой функции Windows. SMB Relay транслирует весь обмен данными по протоколу SMB через себя, кроме процессов установления соединения и аутентификации. Удаленная атакующая сторона может использовать IP-адрес, пока подключен клиентский компьютер.

SMB Relay 2 работает на основе того же принципа, что и SMB Relay, но использует имена NetBIOS вместо IP-адресов. Обе программы используют атаки «злоумышленник в середине». Эти атаки позволяют удаленной атакующей стороне считывать, вставлять и изменять сообщения между двумя сторонами, не обнаруживая себя. Атакованные таким методом компьютеры зачастую прекращают отвечать на запросы пользователя или внезапно перезагружаются.

Для того чтобы избежать проблем подобного рода, рекомендуется использовать пароли для аутентификации или ключи.

6.2.7 Атаки по протоколу ICMP

Протокол ICMP является популярным и широко используемым протоколом Интернета. Применяется он преимущественно подключенными к сети компьютерами для отправки сообщений об ошибках.

Удаленные злоумышленники пытаются использовать уязвимости протокола ICMP. Протокол ICMP предназначен для передачи данных в одном направлении без аутентификации. Это позволяет злоумышленникам организовывать DoS-атаки (отказ в обслуживании) или атаки, предоставляющие не имеющим на это права лицам доступ ко входящим и исходящим пакетам.

Типичными примерами атак по протоколу ICMP являются ping-флуд, флуд эхо-запросов по протоколу ICMP и smurf-атаки. Компьютеры, подвергающиеся атаке по протоколу ICMP, значительно замедляют свою работу (это касается всех приложений, использующих Интернет), и у них возникают проблемы при подключении к Интернету.

6.3 Технологии ESET

6.3.1 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.

Когда блокировщик эксплойтов обнаруживает подозрительный процесс, он может сразу же остановить его работу и записать данные об угрозе, которые затем отправляются в облачную систему ThreatSense. Эти данные затем обрабатываются в исследовательской лаборатории ESET 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).

6.3.2 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, расширенный модуль сканирования памяти — 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.

6.3.3 Защита от сетевых атак

Модуль защиты от сетевых атак — это расширение персонального файервола, улучшающее обнаружение известных уязвимостей на уровне сети. Благодаря обнаружению распространенных уязвимостей в широко используемых протоколах, таких как SMB, RPC и RDP, защита от уязвимостей представляет собой еще один важный уровень защиты от распространяющихся вредоносных программ, сетевых атак и использования уязвимостей, для которых еще не был выпущен или установлен пакет исправления.

6.3.4 ESET LiveGrid®

Сеть ESET LiveGrid®, основанная на передовой системе раннего обнаружения ThreatSense.Net®, использует данные, предоставленные пользователями ESET со всего мира, и отправляет их в исследовательскую лабораторию ESET. Сеть ESET LiveGrid® позволяет получать подозрительные образцы и метаданные из реальных условий, 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 LiveGrid® 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 вирусов на компьютере пользователя (что происходит несколько раз в день).

6.3.5 Защита от ботнетов

Защита от ботнетов обнаруживает вредоносные программы, анализируя их протоколы обмена данными по сети. Вредоносные программы ботнетов меняются весьма часто в отличие от сетевых протоколы, которые не менялись годами. Эта новая технология помогает ESET обезвреживать вредоносные программы, которые пытаются избежать выявления и подключить ваш компьютер к ботнет-сети.

6.3.6 Блокировщик эксплойтов Java

Блокировщик эксплойтов Java — это расширение существующей защиты блокировщика эксплойтов. Он осуществляет мониторинг Java на предмет поведения, подобного поведению 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.).

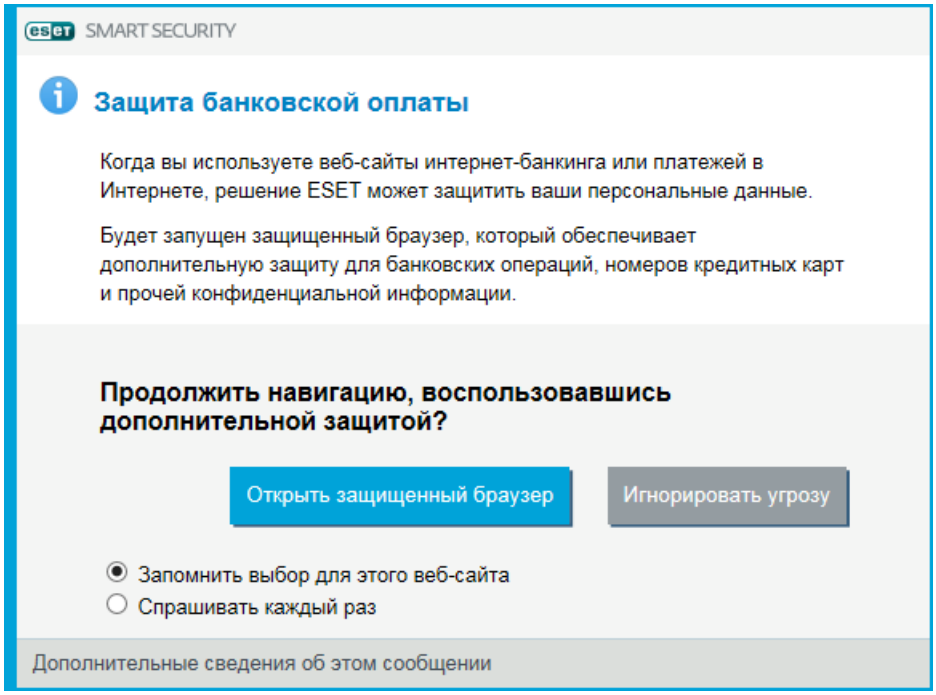
6.3.7 Защита банковских платежей

Модуль защиты банковской оплаты — это дополнительный уровень безопасности, разработанный для защиты ваших финансовых данных при осуществлении финансовых операций в Интернете.

ESET Smart Security содержит встроенный список предварительно заданных веб-сайтов, при попытке открытия которых открывается защищенный браузер. Вы можете добавлять другие веб-сайты или редактировать этот список с помощью настроек программы.

Дополнительные сведения об этой функции см. в статье базы знаний ESET:
Как использовать функцию «Защита банковской оплаты ESET»

В большинстве случаев защита банковской оплаты запускается в используемом по умолчанию браузере, когда вы посещаете известный веб-сайт интернет-банкинга.



В ответ на предложение об использовании защиты банковской оплаты рекомендуется нажать кнопку **Открыть защищенный браузер**.

Если вы решите более не использовать защищенный браузер для сохраненного сайта, последовательно выберите элементы **Дополнительные настройки** (F5) > **Сервис** > **Защита банковской оплаты**, что позволит вам удалить сайт из списка URL-адресов, при переходе по которым открывается защищенный браузер.

Для защиты браузера необходимо использовать шифрованный обмен данными по протоколу HTTPS. Для использования защищенного режима просмотра ваш браузер должен соответствовать перечисленным ниже минимальным требованиям.

- Mozilla Firefox 24
- Internet Explorer 8
- Google Chrome 30

Рекомендуется закрывать защищенный браузер по завершении банковских операций и платежей в Интернете.

6.3.8 Защита от атак на основе сценариев

Защита от атак на основе сценариев — это защита от злонамеренного кода на языке Javascript в браузерах и защита на базе Antimalware Scan Interface (AMSI) от сценариев в Powershell.

ВНИМАНИЕ!
Для работы этой функции необходимо, чтобы система HIPS была включена.

Функция защиты от атак на основе сценариев поддерживается для таких браузеров:

- Mozilla Firefox,
- Google Chrome,
- Internet Explorer,
- Microsoft Edge.

ПРИМЕЧАНИЕ.
Минимальные поддерживаемые версии браузеров могут различаться, поскольку файловые сигнатуры браузеров часто меняются. Последняя версия браузера поддерживается всегда.

6.3.9 Защита от программ-шантажистов

Программа-шантажист — это особый тип вредоносного ПО, блокирующий доступ пользователя к системе путем блокирования ее экрана или шифрования файлов. Модуль защиты от программ-шантажистов осуществляет мониторинг поведения приложений и процессов, которые пытаются изменить ваши личные данные. Если поведение приложения определяется как злонамеренное или репутационное сканирование показывает, что приложение является подозрительным, это приложение блокируется или решение о его блокировании предлагается принять пользователю.

ВАЖНО!
Для правильного функционирования модуля защиты от программ-шантажистов система ESET Live Grid должна быть включена.

6.4 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.

6.4.1 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.

6.4.2 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.

6.4.3 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 (такой как 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.

6.4.4 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.

6.4.4.1 Правила

В контексте решений для защиты от спама и почтовых клиентов под правилами понимаются инструменты обработки электронной почты. Правило состоит из двух логических частей:

1. условие (например, получение сообщения с определенного адреса);
2. действие (например, удаление сообщения, перемещение его в указанную папку).

Количество и сочетания правил зависят от конкретного решения по защите от спама. Правила предназначены для борьбы со спамом (нежелательными сообщениями). Стандартные примеры приведены далее.

- 1. Условие: во входящем сообщении содержатся некоторые слова, часто присутствующие в нежелательных сообщениях.
  2. Действие: удалить сообщение.
- 1. Условие: у входящего сообщения есть вложение с расширением .exe.
  2. Действие: удалить вложение и доставить сообщение в почтовый ящик.
- 1. Условие: входящее сообщение отправлено сотрудником компании, в которой работает пользователь.
  2. Действие: переместить сообщение в папку «Работа».

Рекомендуется использовать сочетание правил в программах защиты от спама, чтобы упростить администрирование и более эффективно отфильтровывать спам.

6.4.4.2 «Белый» список

Вообще под «белым» списком понимается перечень объектов или лиц, которые являются приемлемыми или имеют доступ. Термин «"белый" список электронной почты» означает список адресов пользователей, от которых разрешено получать сообщения. Такого рода списки создаются на основе поиска по ключевым словам в адресах электронной почты, именах домена или IP-адресах.

Если «белый» список работает в «исключительном» режиме, сообщения с других адресов, доменов или IP-адресов получаться не будут. Если же «белый» список не является исключительным, такие сообщения не будут удаляться, а будут обрабатываться каким-либо другим способом.

«Белый» список обладает противоположным «черному» списку назначением. «Белые» списки сравнительно просто поддерживать, значительно проще, чем «черные». Для большей эффективности фильтрации спама рекомендуется использовать и «белый», и «черный» списки.

6.4.4.3 «Черный» список

В общем случае «черный» список является списком неприемлемых или запрещенных объектов или лиц. В виртуальном мире это метод, позволяющий принимать сообщения, которые приходят от всех пользователей, отсутствующих в таком списке.

Существует два типа «черных» списков. К первому типу относятся списки, созданные самими пользователями, в их приложениях для защиты от спама, а ко второму — профессиональные регулярно обновляемые «черные» списки, которые создаются специализированными учреждениями и распространяются через Интернет.

Принципиально важно использовать «черный» список для блокировки спама, но при этом вести такой список сложно, так как новые объекты блокирования появляются ежедневно. Рекомендуется использовать и «белый», и «черный» список, чтобы максимально эффективно отфильтровывать спам.

6.4.4.4 Список исключений

В список исключений обычно входят адреса электронной почты, которые могут быть подделаны и использоваться для отправки спама. Сообщения электронной почты, полученные с адресов, присутствующих в списке исключений, всегда будут сканироваться на предмет наличия спама. По умолчанию в списке исключений присутствуют все адреса электронной почты из существующих учетных записей почтовых клиентов.

6.4.4.5 Контроль на стороне сервера

Контроль на стороне сервера — это метод выявления массовых рассылок спама на основе количества полученных сообщений и реакции пользователей на них. Каждое сообщение оставляет уникальный цифровой «отпечаток», который основан на его содержимом. Уникальный идентификационный номер ничего не говорит о содержимом сообщения. Однако два одинаковых сообщения имеют одинаковые отпечатки, тогда как два различающихся — разные.

Если сообщение помечено как спам, его отпечаток отправляется на сервер. Если сервер получает и другие идентичные отпечатки (соответствующие одному и тому же нежелательному сообщению), этот отпечаток сохраняется в базе данных отпечатков спама. При сканировании входящих сообщений программа отправляет отпечатки сообщений на сервер. Сервер возвращает данные о тех отпечатках, которые соответствуют сообщениям, уже помеченным пользователями как спам.

7. Часто задаваемые вопросы

Эта глава содержит ответы на некоторые из наиболее часто задаваемых вопросов и решения проблем пользователей. Нажмите ссылку, описывающую вашу проблему.

Выполнение обновления ESET Smart Security
Удаление вируса с компьютера
Разрешение обмена данными определенному приложению
Включение родительского контроля для учетной записи
Создание задачи в планировщике
Планирование задачи сканирования (каждые 24 часа)

Если ваша проблема не включена в список на страницах справки выше, попробуйте найти ее на страницах справки ESET Smart Security.

Если решение проблемы не удалось найти с помощью поиска в содержимом справочной системы, перейдите в регулярно обновляемую базе знаний ESET в Интернете. Ссылки на самые популярные статьи базы знаний, которые помогут вам решить распространенные проблемы, перечислены ниже.

Во время установки программы ESET появилось сообщение об ошибке. Что это означает?
Как ввести имя пользователя и пароль в программу ESET Smart Security или ESET NOD32 Antivirus?
Во время установки программы ESET появилось сообщение, что установка преждевременно завершена.
Что делать после обновления лицензии? (пользователи домашней версии)
Что делать, если мой адрес электронной почты изменится?
Запуск Windows в безопасном режиме или в безопасном режиме с поддержкой сети

При необходимости направьте свои вопросы в нашу онлайн-службу технической поддержки. Контактная форма находится на вкладке **Справка и поддержка** программы ESET Smart Security.

7.1 Выполнение обновления ESET Smart Security

Обновлять ESET Smart Security 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).

7.2 Удаление вируса с компьютера

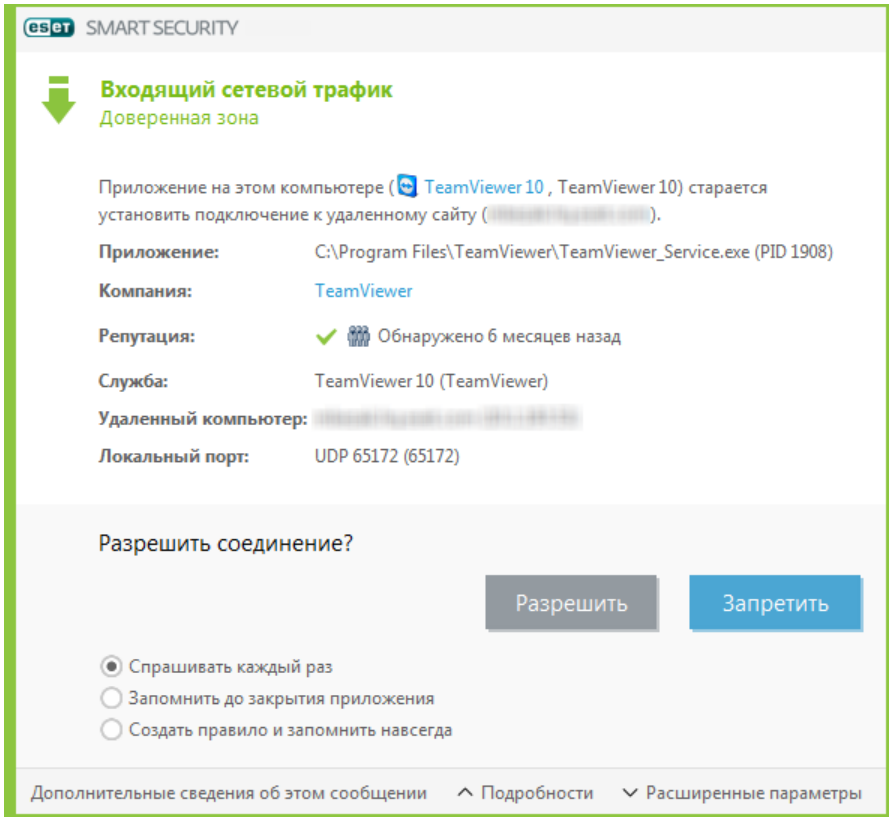
Если компьютер начал работать медленнее, часто зависать и проявлять другие признаки заражения вредоносной программой, рекомендуется выполнить следующие действия.

1. В главном окне программы щелкните **Сканирование ПК**.
2. Щелкните элемент **Сканировать компьютер**, чтобы запустить сканирование компьютера.
3. После завершения сканирования просмотрите журнал на предмет количества проверенных, зараженных и очищенных файлов.
4. Если необходимо проверить только определенную часть диска, щелкните **Выборочное сканирование** и укажите объекты, которые следует сканировать на наличие вирусов.

Дополнительные сведения можно найти в статье нашей регулярно обновляемой базы знаний ESET.

7.3 Разрешение обмена данными определенному приложению

Если в интерактивном режиме обнаруживается новое подключение, но соответствующего правила не найдено, пользователь получает запрос, предлагающий разрешить или запретить его. Если нужно, чтобы программа ESET Smart Security выполняла одно и то же действие при каждой попытке приложения установить подключение, установите флажок **Запомнить действие (создать правило)**.



Можно создать правила персонального файервола для приложений еще до их обнаружения программой ESET Smart Security. Это можно сделать в окне настроек персонального файервола, последовательно выбрав **Сеть** > **Персональный файервол** > **Правила и зоны** > **Настройка**. Чтобы отобразить в окне **Настройка зон и правил** вкладку **Правила**, необходимо установить интерактивный режим фильтрации для персонального файервола.

На вкладке **Общие** укажите имя, направление и протокол передачи данных для правила. В этом окне можно определить действие, которое нужно выполнить при применении правила.

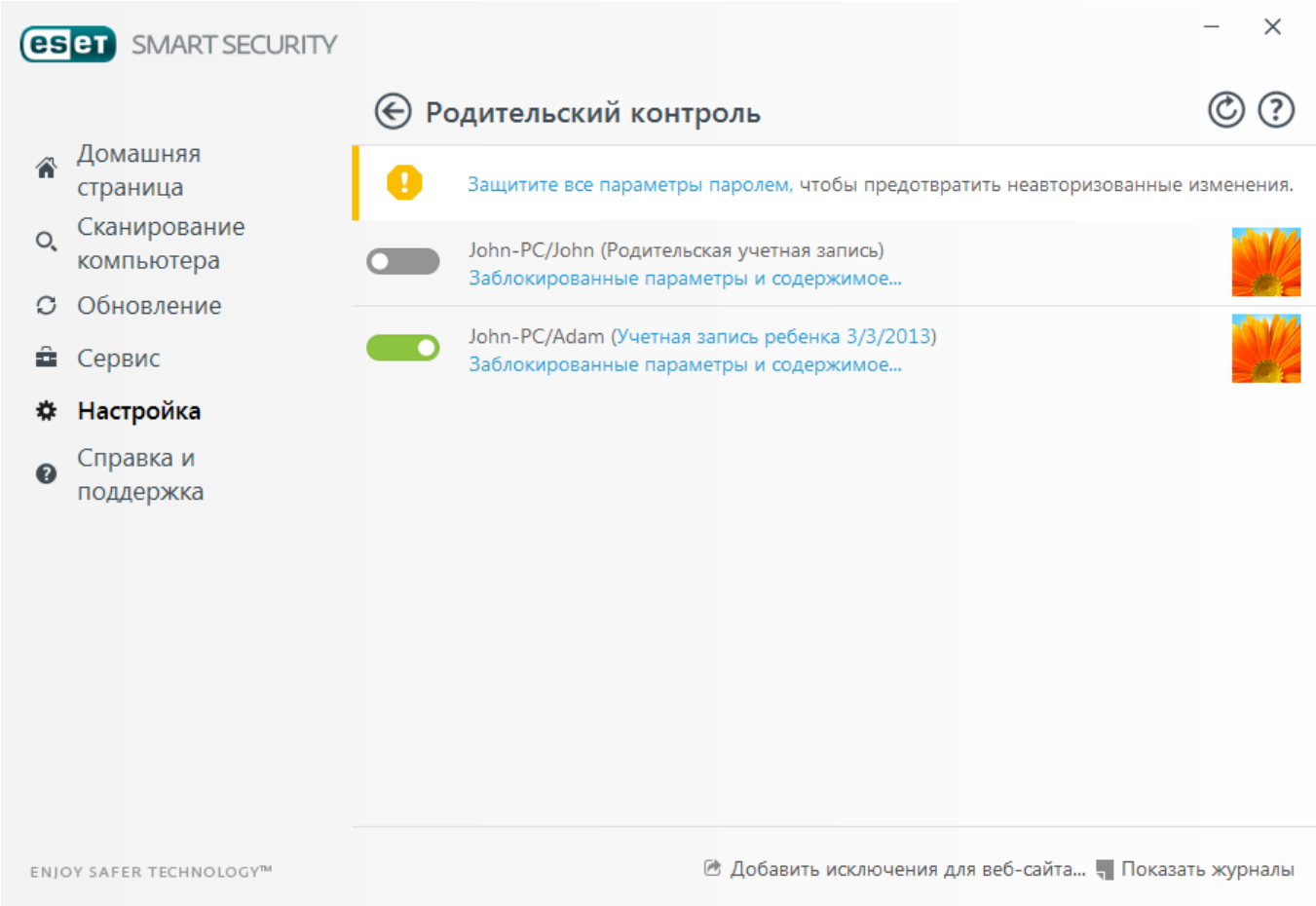
Введите путь к исполняемому файлу приложения и порт передачи данных на локальном компьютере на вкладке **Локальный компьютер**. Перейдите на вкладку **Удаленный компьютер** и введите удаленный адрес и порт (при необходимости). Новое правило начнет действовать немедленно и сработает сразу, как только данное приложение попытается установить подключение.

7.4 Включение родительского контроля для учетной записи

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

1. По умолчанию родительский контроль в программе ESET Smart Security отключен. Существует два способа активации родительского контроля.
   - В главном окне программы щелкните элемент  и последовательно выберите элементы **Настройка** > **Средства безопасности** > **Родительский контроль**, после чего включите функцию родительского контроля.
   - Нажмите клавишу F5, чтобы открыть окно **Дополнительные настройки**, выберите элемент **Интернет и электронная почта** > **Родительский контроль** и установите переключатель рядом с элементом **\Интеграция с системой**.

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



7.5 Создание задачи в планировщике

Для создания задачи выберите **Служебные программы** > **Планировщик**, а затем нажмите кнопку **Добавить** или щелкните правой кнопкой мыши и выберите команду **Добавить...** в контекстном меню. 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, исполняемых при запуске 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 ПК по требованию** - выполнение сканирования файлов и папок на компьютере.
- **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 (ч)**).

На следующем этапе отображается окно сводной информации о текущей планируемой задаче. После внесения всех необходимых изменений нажмите **Готово**.

На экран будет выведено диалоговое окно, в котором можно выбрать профили, используемые для запланированной задачи. Здесь можно задать основной и вспомогательный профили. Вспомогательный профиль используется, если задачу невозможно выполнить с применением основного профиля. Подтвердите внесенные изменения, нажав кнопку **Готово**, после чего новая задача появится в списке текущих запланированных задач.

7.6 Планирование еженедельного сканирования компьютера

Чтобы запланировать регулярную задачу, откройте главное окно программы и выберите **Служебные программы** > **Планировщик**. Ниже приведено краткое описание процедуры планирования задачи, предусматривающей сканирование локальных дисков каждые 24 часа. Подробные инструкции см. в статье нашей базы знаний.

Для того чтобы запланировать задачу сканирования, выполните следующие действия.

1. В главном окне планировщика нажмите **Добавить**.
2. В раскрывающемся меню выберите **Сканирование ПК по требованию**.
3. Введите имя задачи и выберите частоту выполнения задачи **Еженедельно**.
4. Задайте день и время выполнения задачи.
5. Выберите установку **Выполнить задачу как можно скорее**, чтобы выполнить задачу позже в случае, если запланированное выполнение задачи не запустится по какой-либо причине (например, если компьютер будет выключен).
6. Просмотрите сводную информацию о запланированной задаче и нажмите **Готово**.
7. В раскрывающемся меню **Объекты** выберите пункт **Жесткие диски**.
8. Нажмите **Готово** для применения задачи.