ESET FILE SECURITY

ДЛЯ MICROSOFT WINDOWS SERVER

Инструкция по установке и руководство пользователя

Microsoft® Windows® Server 2003 / 2003 R2 / 2008 / 2008 R2 / 2012 / 2012 R2 / 2016

Щелкните здесь, чтобы отобразить веб-версию этого документа справки

ENJOY SAFER TECHNOLOGY™

ESET FILE SECURITY

Служба поддержки клиентов: www.eset.com/support

Испр. 24.05.2017

Содержание

Содержание

1. Введение

ESET File Security — это интегрированное решение, разработанное специально для среды Microsoft Windows Server. ESET File Security обеспечивает эффективную и надежную защиту от разных типов вредоносных программ, предлагая два вида защиты: защиту от вирусов и защиту от шпионских программ.

Основные функции ESET File Security:

- Кластер ESET: серверные продукты ESET способны взаимодействовать между собой и обмениваться такими данными, как конфигурация и оповещения, а также выполнять синхронизацию данных, необходимых для надлежащей работы группы экземпляров продуктов. Это обеспечивает одинаковую конфигурацию продукта по всему кластеру. Отказоустойчивый кластер Windows и кластер балансировки сетевой нагрузки (NLB) поддерживаются продуктом ESET File Security. Кроме того, можно добавить элементы кластера ESET вручную без необходимости использования определенного кластера Windows. Кластеры ESET работают в средах домена и рабочей группы.
- Сканирование хранилища: выполняется сканирование всех общих файлов на локальном сервере. Это упрощает выборочное сканирование только тех данных пользователя, которые хранятся на файловом сервере.
- Автоматические исключения: автоматическое обнаружение и исключение приложений и файлов на сервере, имеющих критическое значение для беспрепятственной и эффективной работы.
- eShell (оболочка ESET): управляющий интерфейс командной строки, предлагающий более продвинутым пользователям и администраторам полномасштабные возможности для управления серверными продуктами ESET. Доступна новая, улучшенная версия eShell 2.0.
- Самозащита — технология, защищающая решения по обеспечению безопасности ESET от изменения и отключения.
- Эффективное устранение проблем благодаря встроенным средствам для решения различных проблем: ESET SysInspector для диагностики системы и ESET SysRescue Live для создания загрузочного компакт-диска или USB-устройства аварийного восстановления.

ESET File Security поддерживает большинство выпусков Microsoft Windows Server 2003, 2008 и 2012 в отдельных и кластерных средах. Вы можете удаленно управлять средством ESET File Security в больших сетях с помощью ESET Remote Administrator.

1.1 Новые возможности

В ESET File Security представлены следующие новые функции:

- Поддержка кластеризации
- Исключения для процессов (повышенная совместимость с программным обеспечением сторонних производителей)
- Улучшенные возможности графического интерфейса
- Сканирование фильтрации на основе правил (возможность определения правил для файлов и выполнение специального сканирования по требованию)
- Защита от фишинга
- Оптимизация виртуализированных сред
- Сканирование Hyper-V — это новая технология, с помощью которой можно сканировать диски виртуальных машин на сервере Microsoft Hyper-V Server без необходимости установки каких-либо агентов на соответствующие виртуальные машины.

1.2 Страницы справочной системы

Это руководство поможет вам использовать ESET File Security максимально эффективно. Дополнительные сведения о любом окне программы можно получить, нажав клавишу F1, когда это окно открыто. Откроется страница справки, содержащая информацию о текущем окне.

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

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

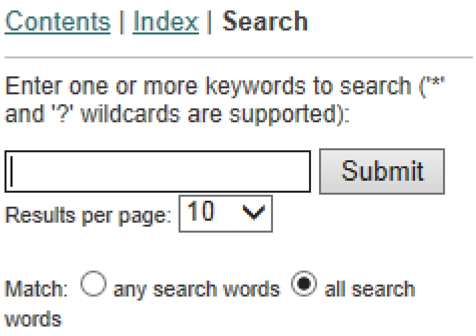
ВАЖНО!
Эта пометка означает, что информация требует вашего внимания и пропускать ее не рекомендуется. Важные примечания содержат значимую, но не критически важную информацию.

ВНИМАНИЕ!
Так обозначается критически важная информация, которая требует особого внимания. Отметка «Внимание!» используется непосредственно для того, чтобы удержать вас от совершения потенциально опасных ошибок. Прочитайте и постарайтесь понять текст предупреждения, поскольку оно содержит сведения об исключительно важных системных настройках или о возможных угрозах.

ПРИМЕР
Этот практический пример поможет понять, как можно использовать определенную функцию или компонент.

Условное обозначение	Значение
Жирный шрифт	Названия элементов интерфейса, например флажков или переключателей.
Курсив	Заполнители для предоставляемой вами информации. Например, если текст *имя файла* или *путь* указан с использованием курсива, это означает, что путь или имя файла должны ввести вы.
`Шрифт Courier New`	Команды или образцы кода.
Гиперссылка	Обеспечивает простой и быстрый доступ к разделам, на которые ведет перекрестная ссылка, или внешним веб-страницам. Гиперссылки выделяются синим цветом и иногда подчеркиванием.
%ProgramFiles%	Системный каталог ОС Windows, в котором хранятся файлы установленных программ Windows и др.

- Справочная система разделена на главы и подразделы. Нужную информацию можно найти, просматривая **содержимое** страниц справки. Или же можно использовать **Указатель** для поиска по ключевым словам либо полнотекстовый **Поиск**.



Программа ESET File Security позволяет выполнять поиск в справочной системе по ключевым словам, а также поиск в руководстве пользователя по тем или иным словам и фразам. Разница между двумя способами состоит в том, что ключевое слово, характеризующее содержимое справочной страницы, может отсутствовать в тексте этой страницы. Поиск по словам и фразам осуществляется в содержимом всех страниц. В результате отображаются все страницы, содержащие именно эти слова и фразы.

- Вы также можете опубликовать свою оценку и/или оставить отзывы в конкретных разделах справочного руководства или использовать ссылки **Была ли эта информация полезной для вас?** и **Оцените эту статью: помогла/не помогла**, расположенные в нижней части страницы справки в базе знаний ESET.

2. Требования к системе

Поддерживаемые операционные системы

- Microsoft Windows Server 2003 с пакетом обновления 2 (x86 и x64)
- Microsoft Windows Server 2003 R2 с пакетом обновления 2 (x86 и x64)
- Microsoft Windows Server 2008 (x86 и x64)
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

Серверы Storage, Small Business и MultiPoint:

- Microsoft Windows Storage Server 2008 R2 Essentials с пакетом обновления 1
- Microsoft Windows Storage Server 2012
- Microsoft Windows Storage Server 2012 R2
- Microsoft Windows Storage Server 2016
- Microsoft Windows Small Business Server 2003 (x86)
- Microsoft Windows Small Business Server 2003 R2 (x86)
- Microsoft Windows Small Business Server 2008 (x64)
- Microsoft Windows Small Business Server 2011 (x64)
- Microsoft Windows Server 2012 Essentials
- Microsoft Windows Server 2012 R2 Essentials
- Microsoft Windows Server 2016 Essentials
- Microsoft Windows MultiPoint Server 2010
- Microsoft Windows MultiPoint Server 2011
- Microsoft Windows MultiPoint Server 2012

Поддерживаемые серверные операционные системы с ролью Hyper-V:

- Windows Server 2008 R2 — виртуальные машины можно сканировать только тогда, когда они не в сети.
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

Требования к оборудованию зависят от используемой версии операционной системы. Рекомендуется ознакомиться с документацией на Microsoft Windows Server для получения дополнительных сведений о требованиях к оборудованию.

ПРИМЕЧАНИЕ.
Прежде чем устанавливать решение ESET по обеспечению безопасности, настоятельно рекомендуется установить последний пакет обновления для ОС Microsoft Server и серверного приложения. Рекомендуется также устанавливать последние обновления и исправления Windows, когда они доступны.

Минимальные требования к оборудованию:

Компонент	Требование
Процессор	Intel или AMD, одноядерный, x86 или x64
Объем памяти	256 МБ свободной памяти
Жесткий диск	700 МБ свободного места на диске
Разрешение экрана	800 x 600 пикселей или выше

3. Типы защиты

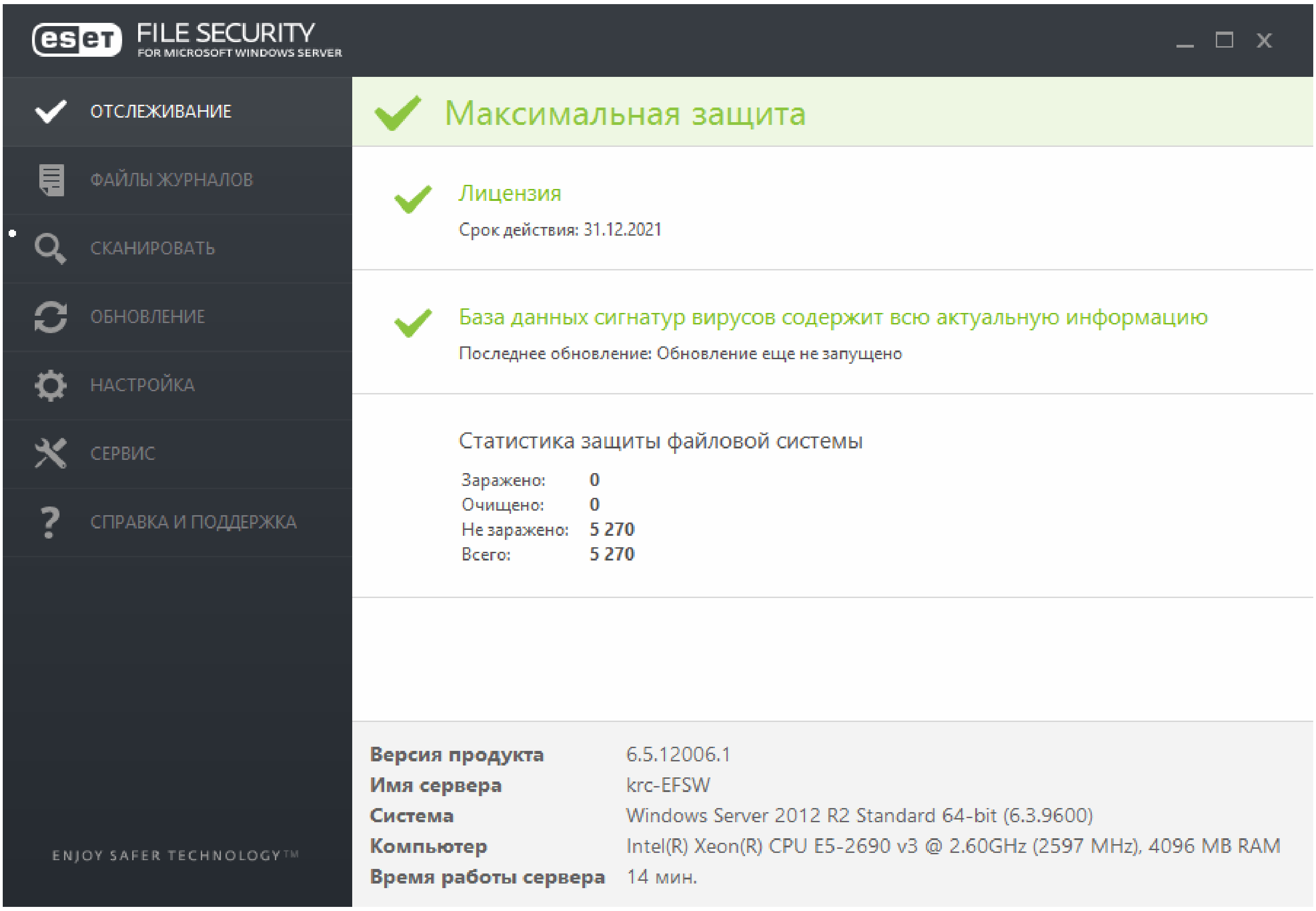
Существует два типа защиты.

- Защита от вирусов
- Защита от шпионских программ

Защита от вирусов и шпионских программ — одна из основных функций программного продукта ESET File Security. Такая защита предотвращает вредоносные атаки на компьютер путем контроля файлов, электронной почты и подключений к Интернету. Если обнаруживается угроза, модуль защиты от вирусов может обезвредить ее, сначала заблокировав, а затем очистив, удалив или переместив в папку карантина.

4. Интерфейс пользователя

Средство ESET File Security использует интуитивно понятный графический интерфейс, через который можно легко получить доступ к основным функциям программы. Главное окно ESET File Security разделено на две основные части. Основное окно справа содержит информацию, относящуюся к параметру, выбранному в главном меню слева.

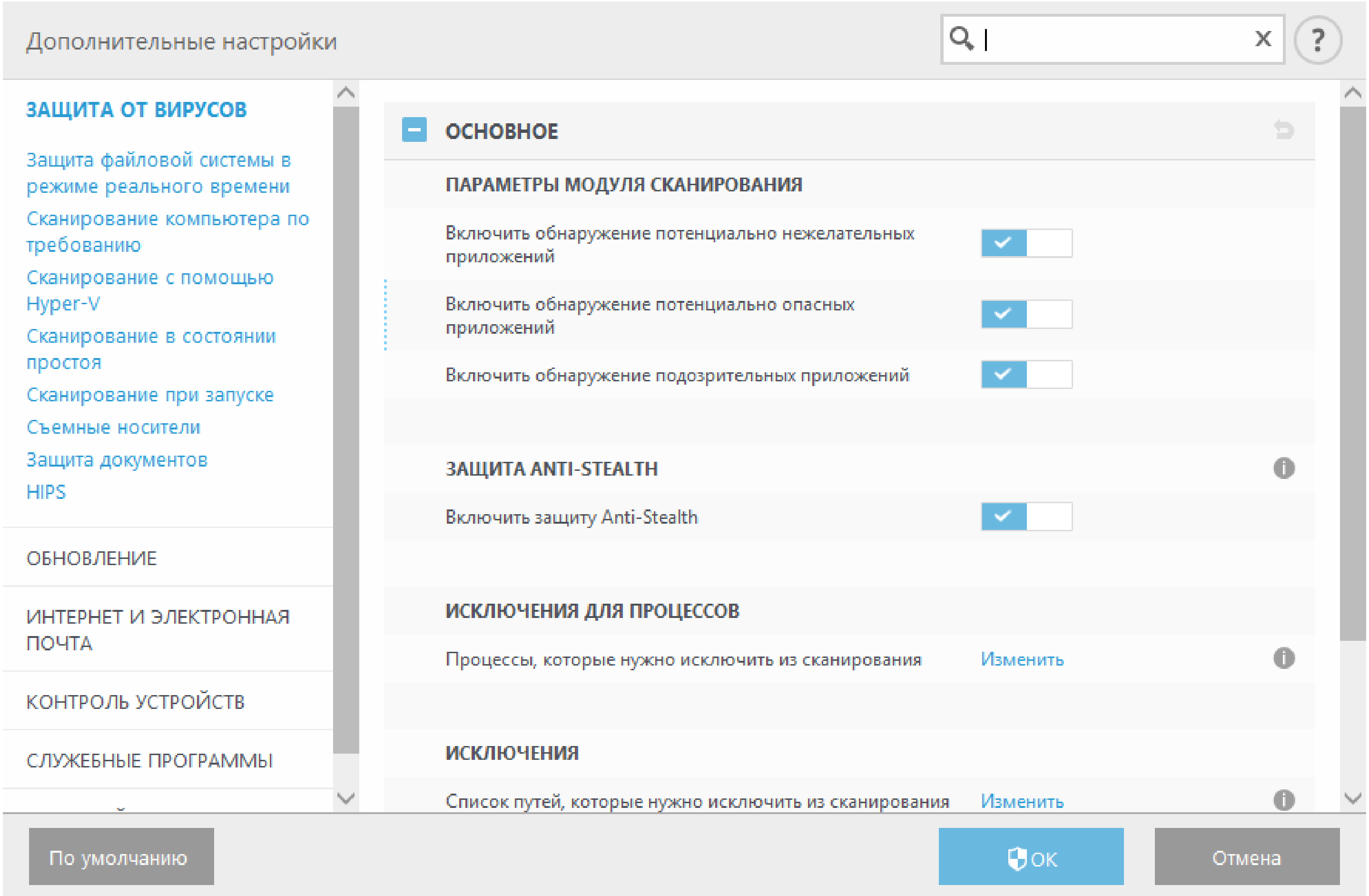


Другие разделы главного меню описаны далее.

- Мониторинг: информация о состоянии защиты ESET File Security, действительности лицензии, обновлениях базы данных сигнатур вирусов, основные статистические данные и информация о системе.
- Файлы журналов: доступ к файлам журналов, содержащим информацию обо всех важных программных событиях. В этих файлах представлены сведения об обнаруженных угрозах, а также о других событиях, имеющих отношение к безопасности.
- Сканирование: возможность сконфигурировать и запустить сканирование хранилища, сканирование Smart, выборочное сканирование и сканирование съемных носителей. Кроме того, можно повторно запустить последнюю операцию сканирования.
- Обновление: отображение информации о базе данных сигнатур вирусов и уведомление о появлении доступных обновлений. Кроме того, в данном разделе можно выполнить активацию продукта.
- Настройки: этот параметр позволяет настроить параметры безопасности сервера и компьютера.
- Служебные программы: дополнительная информация о защите системы и дополнительные средства управления безопасностью. Раздел «Сервис» содержит следующие подразделы: Запущенные процессы, Наблюдение, Статистика защиты, Кластер, Оболочка ESET, ESET SysInspector, ESET SysRescue Live (для создания компакт-диска или USB-устройства аварийного восстановления) и Планировщик. Кроме того, можно выбрать параметр Отправка образца на анализ и проверить папку Карантин.

- Справка и поддержка: доступ к страницам справки, базе знаний ESET и другим средствам поддержки. Кроме того, доступны ссылки на форму запроса в службу поддержки клиентов и информация об активации продукта.

В дополнение к основному графическому интерфейсу существует также окно **Дополнительные настройки**, которое можно открыть с любой страницы программы, нажав клавишу F5.



В окне **Дополнительные настройки** можно настраивать параметры в соответствии со своими потребностями. В меню слева можно выбрать следующие категории:

- Защита от вирусов: включение и выключение обнаружения потенциально нежелательных, небезопасных и подозрительных приложений, указание исключений, защита файловой системы в режиме реального времени, сканирование компьютера по требованию, сканирование Hyper-V и т. д.

- Обновление: настройка списка профилей, создание снимков файла обновления, информация об источниках обновления, например сведения о серверах обновления и данные аутентификации для них.

- Интернет и электронная почта: настройка защиты почтового клиента, фильтрации протоколов, защиты доступа в Интернет и т. д.

- Контроль устройств: настройка правил и групп для функции контроля устройств.

- Служебные программы: настройка служебных программ, например ESET LiveGrid, файлов журнала, прокси-сервера, кластера и т. д.

- Интерфейс: настройка поведения графического интерфейса программы, состояний, сведений о лицензии и т. д.

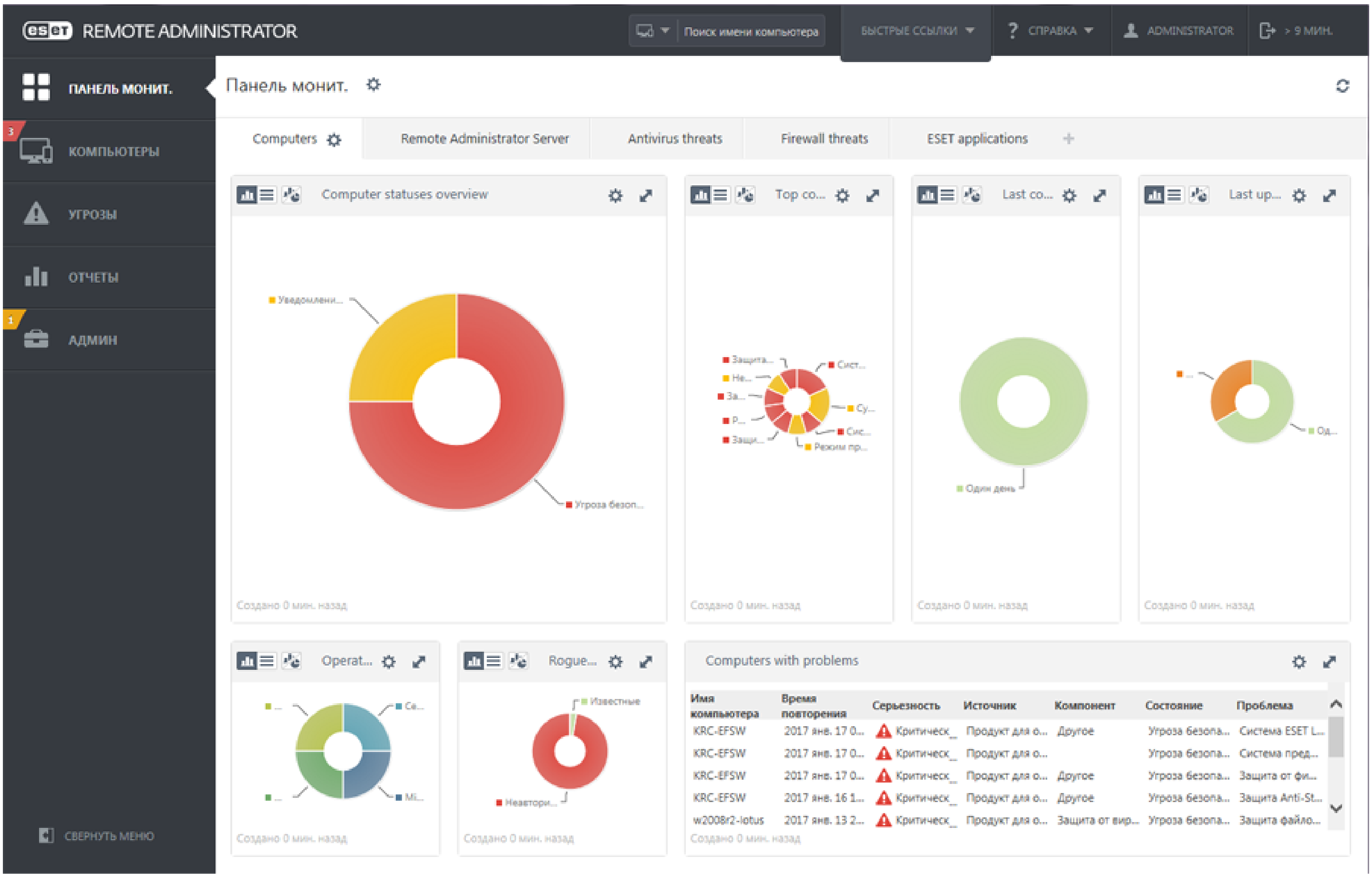
Если щелкнуть элемент (категорию или подкатегорию) в меню слева, параметры, соответствующие этому элементу, отображаются на правой вкладке.

5. Управление через ESET Remote Administrator

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

В решениях ESET для обеспечения безопасности предусмотрена поддержка сетей, использующих несколько платформ различных типов. Ваша сеть может состоять из комбинации текущих операционных систем Microsoft, Linux, Mac OS и мобильных операционных систем.

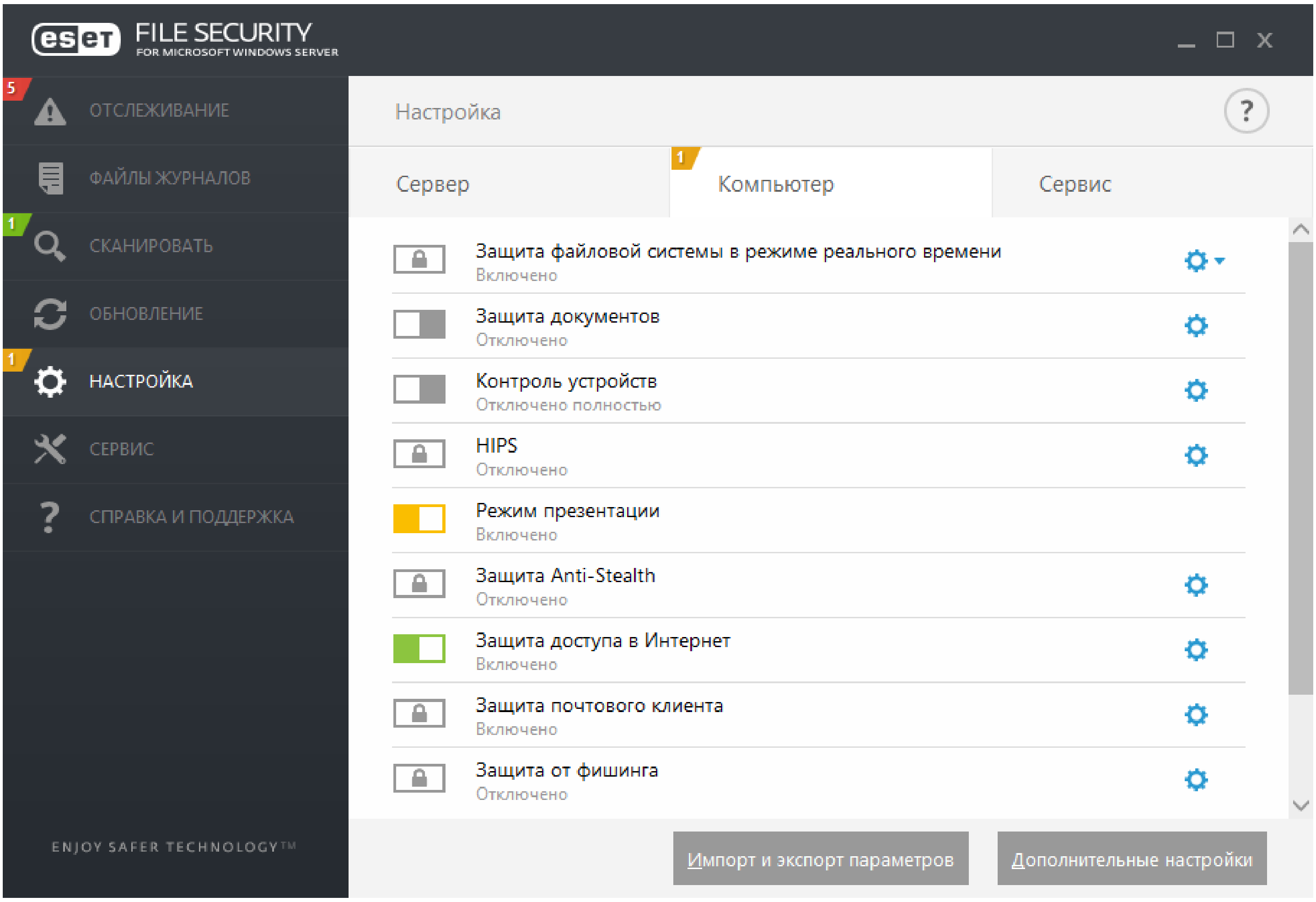
- ESET Remote Administrator Server — решение ERA Server можно установить на серверах под управлением Windows или Linux. Оно доступно также как виртуальное устройство. Это решение отвечает за взаимодействие с агентами, а также собирает и хранит сведения о приложениях.
- Веб-консоль ERA — это приложение с веб-интерфейсом, которое отображает данные, полученные с сервера ERA Server, и позволяет управлять решениями ESET по обеспечению безопасности, находящимися в вашей среде. Доступ к веб-консоли можно получить с помощью браузера. В ней отображаются общие сведения о статусах клиентов сети, и ее можно использовать для удаленного развертывания решений ESET на неуправляемых компьютерах. Если вы предоставите интернет-доступ к веб-серверу, вы сможете использовать ESET Remote Administrator практически на любом устройстве, подключенном к Интернету.
- Агент ERA — агент ESET Remote Administrator помогает установить соединение между сервером ERA Server и клиентскими компьютерами. Чтобы установить соединение между компьютером и сервером ERA Server, на этот компьютер нужно установить агент. Поскольку агент ERA находится на клиентском компьютере и может хранить несколько сценариев безопасности, его использование значительно сокращает время реагирования на новые угрозы. С помощью веб-консоли ERA агент ERA можно развернуть на неуправляемых компьютерах, распознанных с помощью Active Directory или ESET Rogue Detection Sensor.



ПРИМЕЧАНИЕ.
Дополнительные сведения о средстве ERA см. в справке ESET Remote Administrator в Интернете. Эта справка разделена на три раздела: Установка/обновление, Администрирование и Развертывание виртуального устройства. Вы можете переключаться между этими разделами с помощью навигационных вкладок в заголовке.

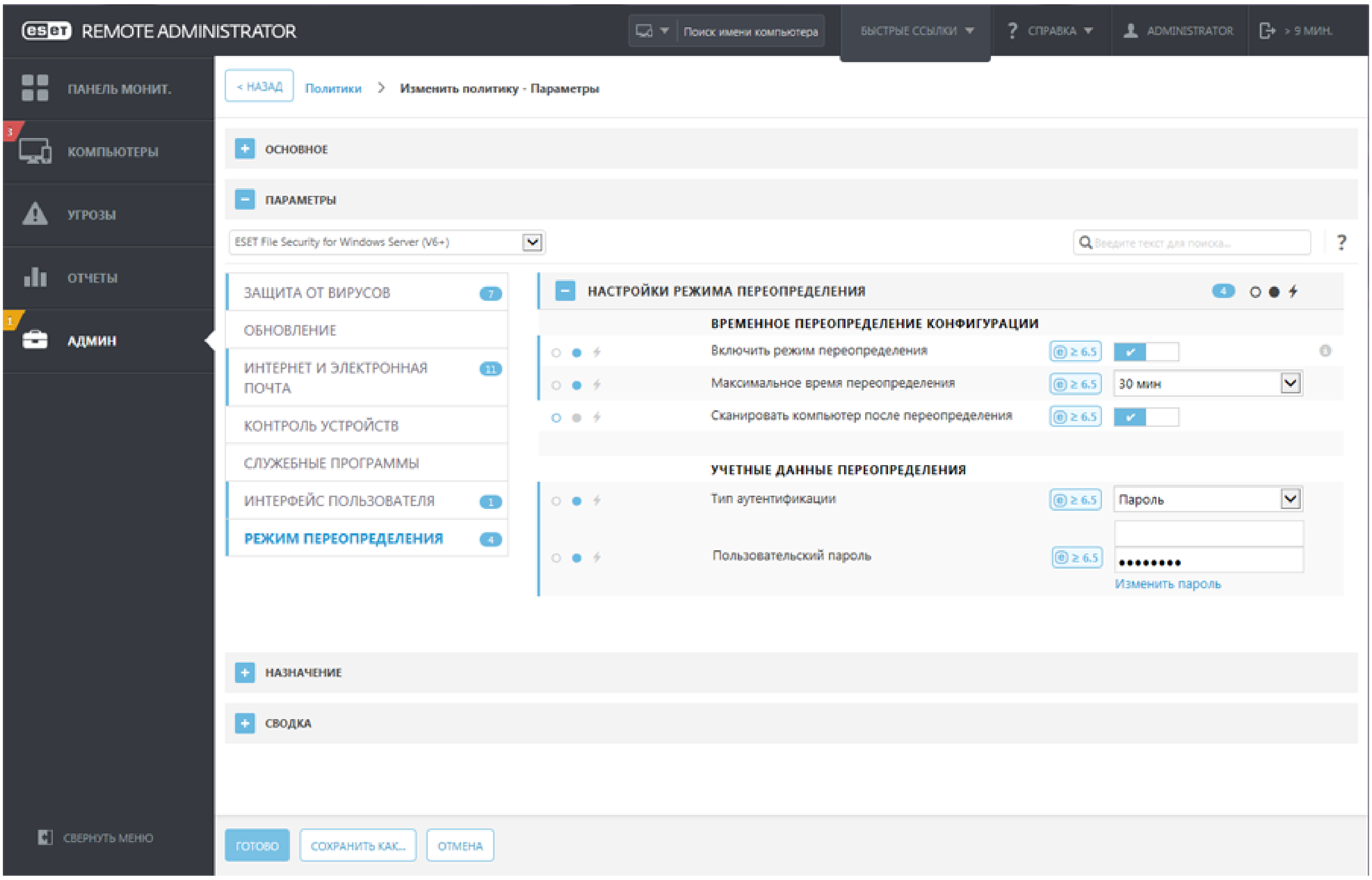
5.1 Режим переопределения

Если к ESET File Security применяется политика ESET Remote Administrator, будет отображаться значок блокировки  вместо переключателя «Включить/отключить» на странице с настройками и значок блокировки рядом с переключателем в окне **Дополнительные настройки**.

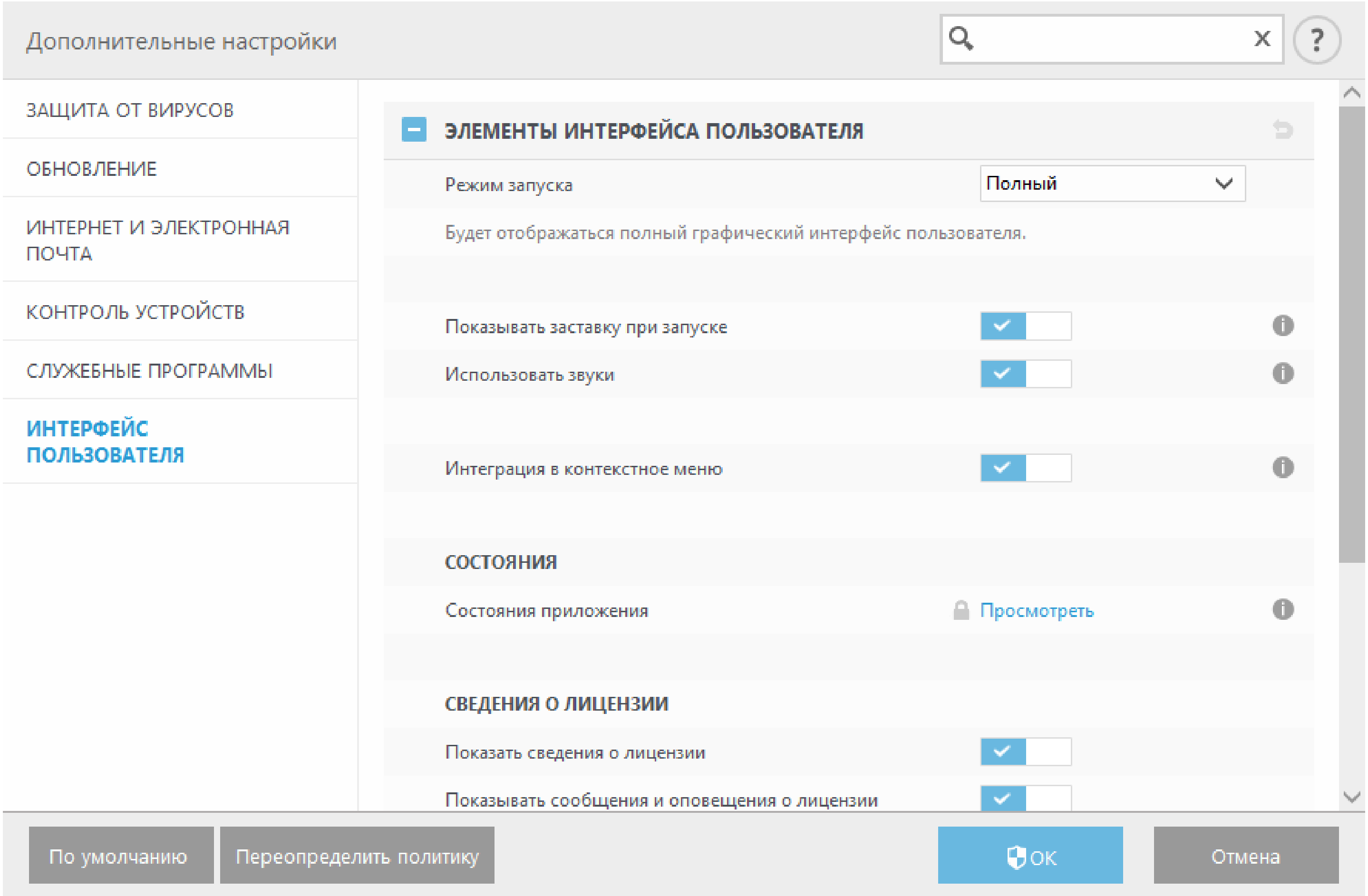


Обычно параметры, настроенные с помощью политики ESET Remote Administrator, изменить невозможно. Режим переопределения позволяет временно разблокировать эти параметры. Однако необходимо включить **режим переопределения** с использованием политики ESET Remote Administrator.

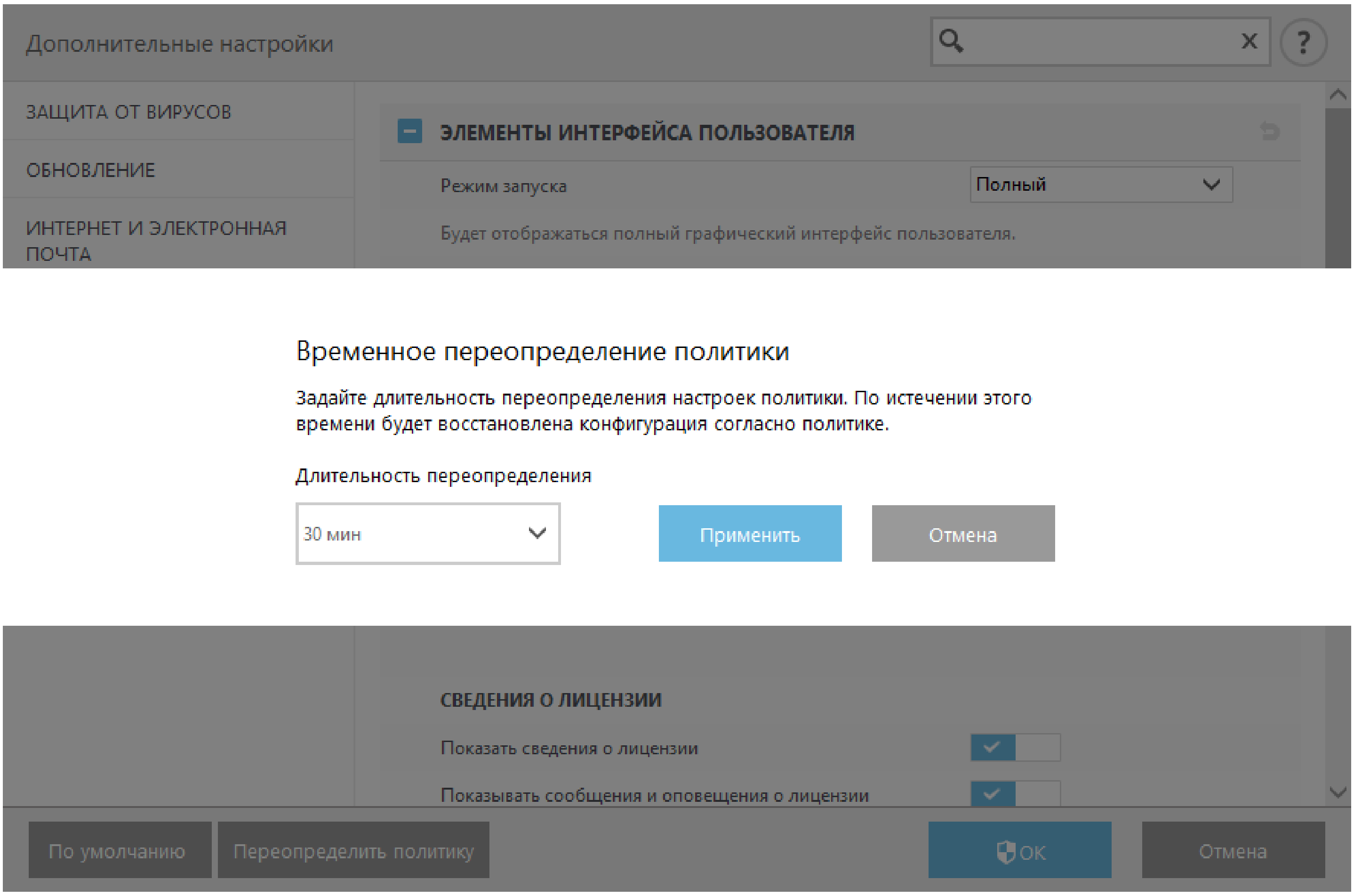
Войдите в веб-консоль ERA, перейдите в раздел **Администрирование** > **Политики**, выберите и измените существующую политику, которая применяется к ESET File Security, или создайте новую. В разделе **параметров** щелкните **Режим переопределения**, включите его и настройте остальные его параметры, в том числе «Тип аутентификации» (**Пользователь Active Directory** или **Пароль**).



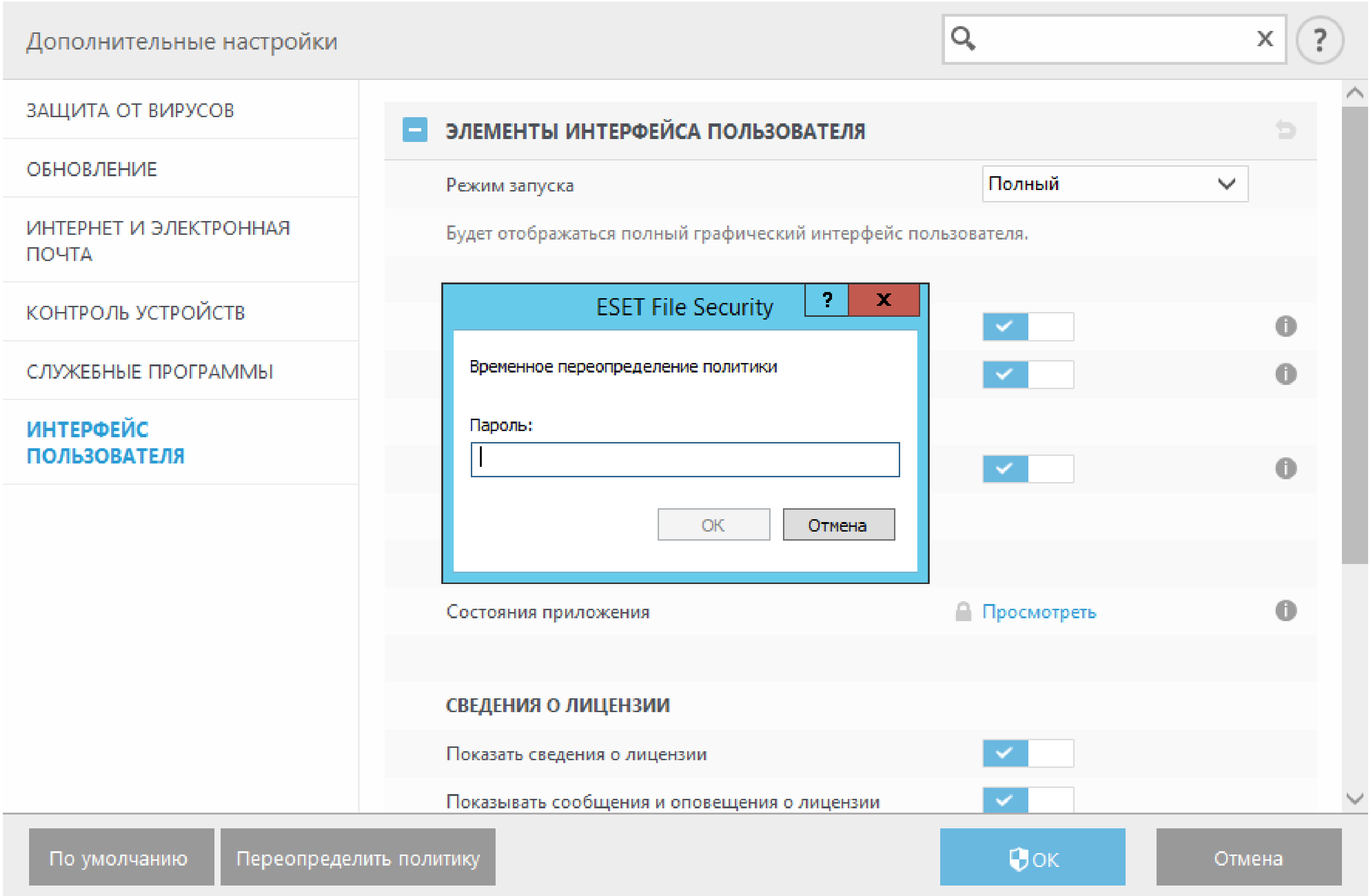
После изменения существующей или применения новой политики к ESET File Security в окне **Дополнительные настройки** появится кнопка **Переопределить политику**.



Нажмите кнопку **Переопределить политику**, задайте длительность и щелкните **Применить**.



Если в качестве типа аутентификации вы выбрали вариант **Пароль**, введите пароль для переопределения политики.



По истечении срока действия режима переопределения настройки политики ESET Remote Administrator вернутся в исходное состояние, а выполненные вами изменения будут отменены. Перед окончанием действия режима переопределения отобразится соответствующее уведомление.

Завершить переопределение можно в любое время до окончания срока его действия. Это можно сделать на странице мониторинга или в окне **Дополнительные настройки**.

6. Установка

После приобретения ESET File Security установочный файл можно загрузить с веб-сайта ESET (www.eset.com) в виде пакета с расширением `.msi`.

Обратите внимание, что установщик необходимо запускать с помощью встроенной учетной записи администратора или учетной записи администратора домена (если локальная учетная запись администратора отключена). Другие пользователи, даже если они являются участниками группы администраторов, не располагают достаточными правами доступа. Необходимо использовать встроенную учетную запись администратора, поскольку вы не сможете выполнить установку с помощью какой-либо другой учетной записи пользователя, кроме учетной записи локального администратора или администратора домена.**Запустить установочный файл можно двумя способами.**

- Войти локально с помощью учетной записи администратора и запустить установочный файл.
- Выполнить команду от имени другого пользователя. Для этого откройте командную строку администратора и запустите файл `.msi` (например, `msiexec /i efsw_nt64_ENU.msi` но необходимо заменить `efsw_nt64_ENU.msi` с точным именем загруженного установочного файла с расширением MSI).

После запуска установочного файла и подтверждения согласия с условиями лицензионного соглашения мастер установки поможет вам выполнить установку. Если вы откажетесь принять условия лицензионного соглашения, мастер завершит работу.

ВАЖНО!
Настоятельно рекомендуется устанавливать ESET File Security в только что установленной и сконфигурированной операционной системе, если это возможно. Если необходимо установить программный продукт в существующую систему, рекомендуется удалить предыдущую версию ESET File Security, перезапустить сервер и после этого установить новую версию ESET File Security.

С помощью мастера можно выбрать один из трех типов установки.

Полная
Рекомендуется выбирать этот тип установки. Будут установлены все функции программы ESET File Security. Вы можете выбрать папку для установки ESET Security, однако рекомендуется оставить значения по умолчанию.

Базовая
Этот тип установки предназначен для версий Windows Server Core. Этапы установки такие же, как и во время полной установки, но устанавливаются только основные компоненты и интерфейс командной строки. Хотя установка основных компонентов предназначена главным образом для использования с версией Windows Server Core, ее можно использовать и в обычной системе Windows Server, если необходимо. Решения ESET, устанавливаемые в таком режиме, не содержат графический интерфейс. Это означает, что при работе с ESET File Security можно использовать только интерфейс командной строки.

Чтобы выполнить установку основных компонентов из командной строки, используйте следующий пример команды:
```
msiexec /qn /i efsw_nt64_ENU.msi /l inst.log ADDLOCAL=HIPS,_Base,SERVER,_FeaturesCore,WMIProvider,Scan,Updat
```

Выборочная
Выборочная установка позволяет выбрать функции программы ESET File Security, которые будут установлены в системе. С началом установки отображается список модулей и функций продукта.

Установить ESET File Security можно не только с помощью мастера, но и с помощью командной строки (такая установка выполняется автоматически). Этот тип установки не требует взаимодействия с пользователем и называется также установкой без участия пользователя.

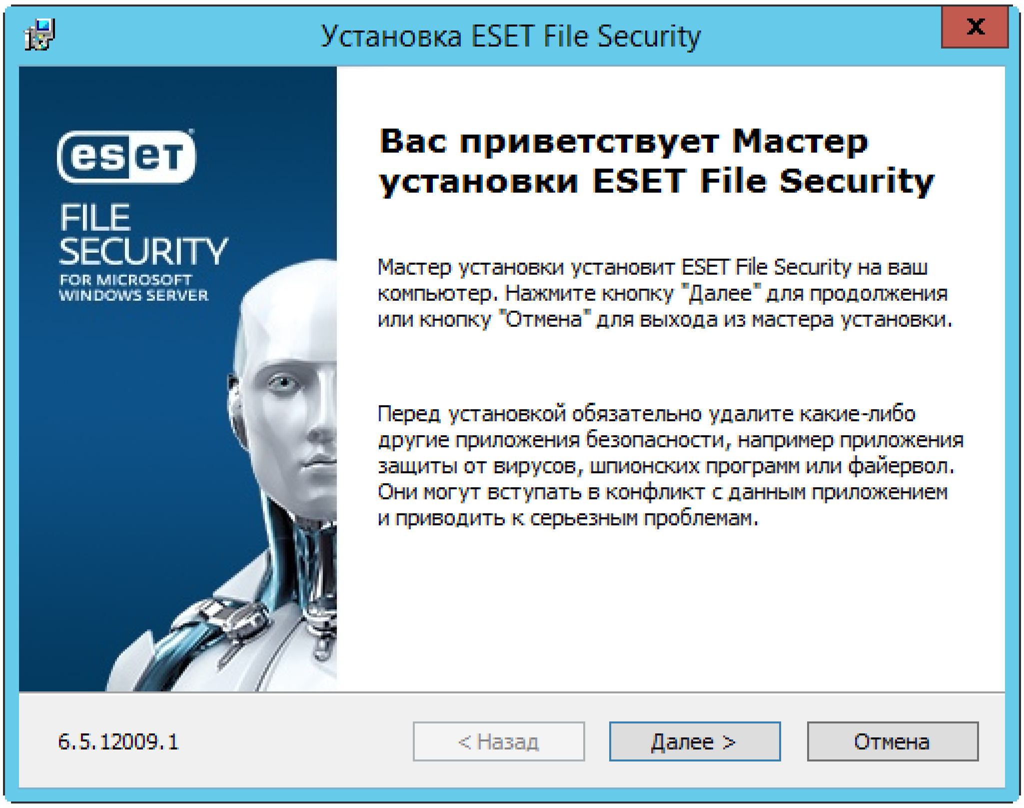
Автоматическая установка/установка без участия пользователя
Выполните следующую команду, чтобы завершить установку из командной строки: `msiexec /i <packagename> /qn /l*xv msi.log`

ПРИМЕЧАНИЕ.

Если на вашем компьютере ранее использовалось стороннее антивирусное ПО, рекомендуется полностью удалить его, прежде чем устанавливать ESET File Security. Помочь удалить стороннее программное обеспечение может средство ESET AV Remover.

6.1 Этапы установки программы ESET File Security

Выполняйте описанные далее этапы, чтобы установить ESET File Security с помощью мастера установки.



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

Выберите один из доступных типов установки. Доступные типы установки зависят от операционной системы.

Для Windows Server 2003, 2003 R2, 2012, 2012 R2, 2016, Windows Small Business Server 2003 и 2003 R2, Windows Server 2012 Essentials, 2012 R2 Essentials и 2016 Essentials доступны такие типы установки:

- **Полная**: установка всех компонентов ESET File Security.
- **Базовая** — этот тип установки предназначен для использования, если установлена версия Windows Server Core. Сам процесс такой же, как и при полной установке, но устанавливаются только ключевые компоненты. Если используется этот метод, у ESET File Security не будет графического интерфейса пользователя. Кроме того, в случае необходимости можно запустить базовую установку на обычном сервере Windows Server. Дополнительные сведения о базовой установке см. здесь.
- **Выборочная**: позволяет выбрать, какие компоненты ESET File Security будут установлены.

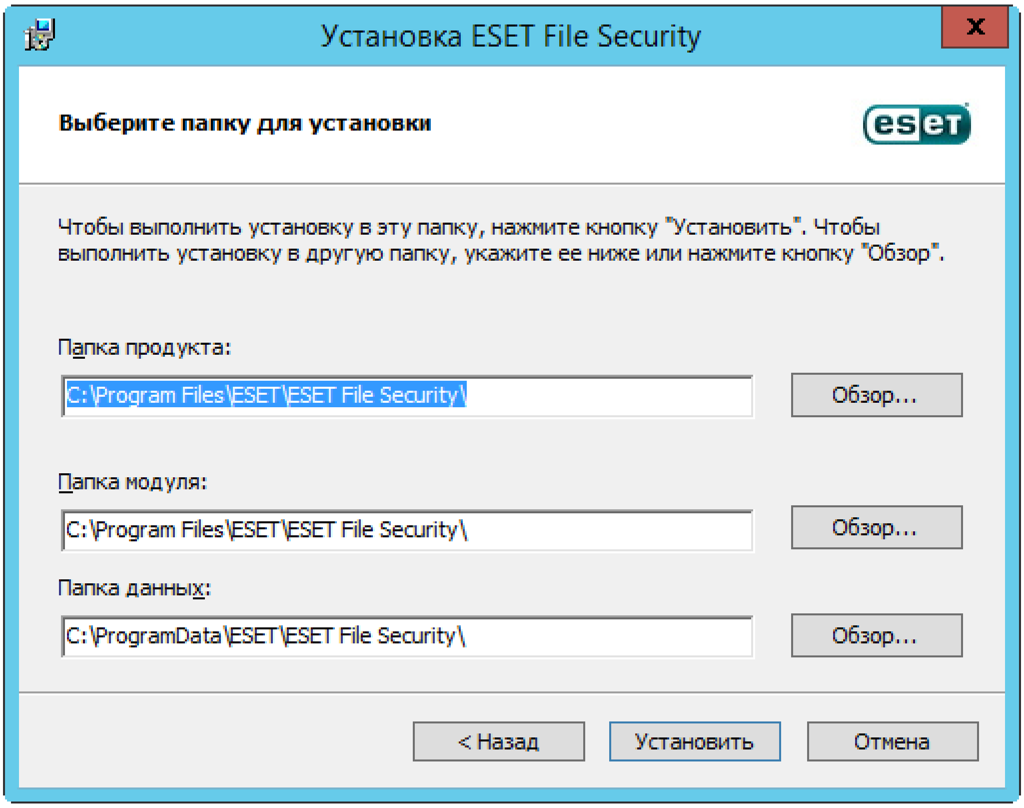
Для Windows Server 2008, 2008 R2, Windows Small Business Server 2008 и 2011 доступны такие типы установки:

- **Обычная**: установка рекомендованных компонентов ESET File Security.

- **Базовая** — этот тип установки предназначен для использования, если установлена версия Windows Server Core. Сам процесс такой же, как и при полной установке, но устанавливаются только ключевые компоненты. Если используется этот метод, в ESET File Security не будет графического интерфейса пользователя. Кроме того, в случае необходимости можно запустить базовую установку на обычном сервере Windows Server. Дополнительные сведения о базовой установке см. здесь.
- **Выборочная**: позволяет выбрать, какие компоненты ESET File Security будут установлены.

Полная установка

Этот способ также называют установкой всех компонентов. Он предусматривает установку всех компонентов программы ESET File Security. Вам будет предложено выбрать папку для установки. По умолчанию программа устанавливается в папку *C:\Program Files\ESET\ESET File Security*. Нажмите кнопку **Обзор**, чтобы изменить папку (не рекомендуется).



Обычная установка.

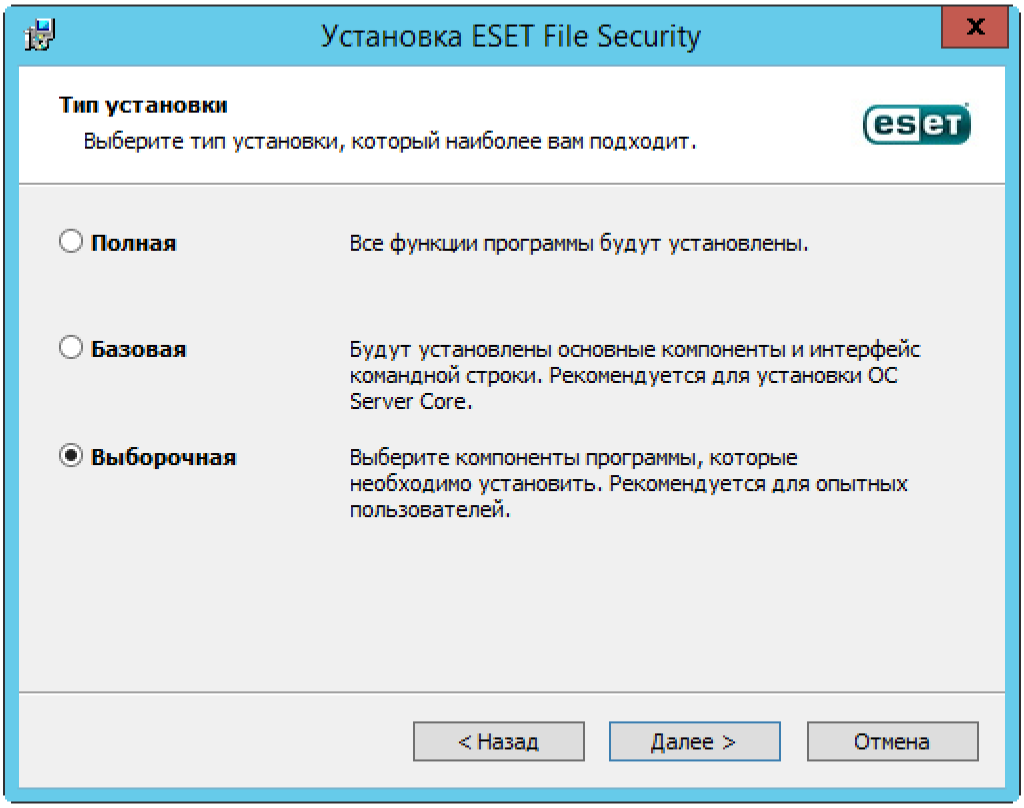
Выберите этот тип установки, чтобы установить рекомендованные компоненты ESET File Security.

ПРИМЕЧАНИЕ.
В ОС Windows Server 2008, Windows Server 2008 R2, Small Business Server 2008 и Small Business Server 2011 установка компонента **Интернет и электронная почта** отключена по умолчанию (**Обычная** установка). Если нужно установить этот компонент, выберите тип установки **Выборочная**.

Базовая установка.

Будут установлены базовые функции и интерфейс командной строки. Этот тип установки рекомендуется, если используется Windows Server Core.

Выборочная установка

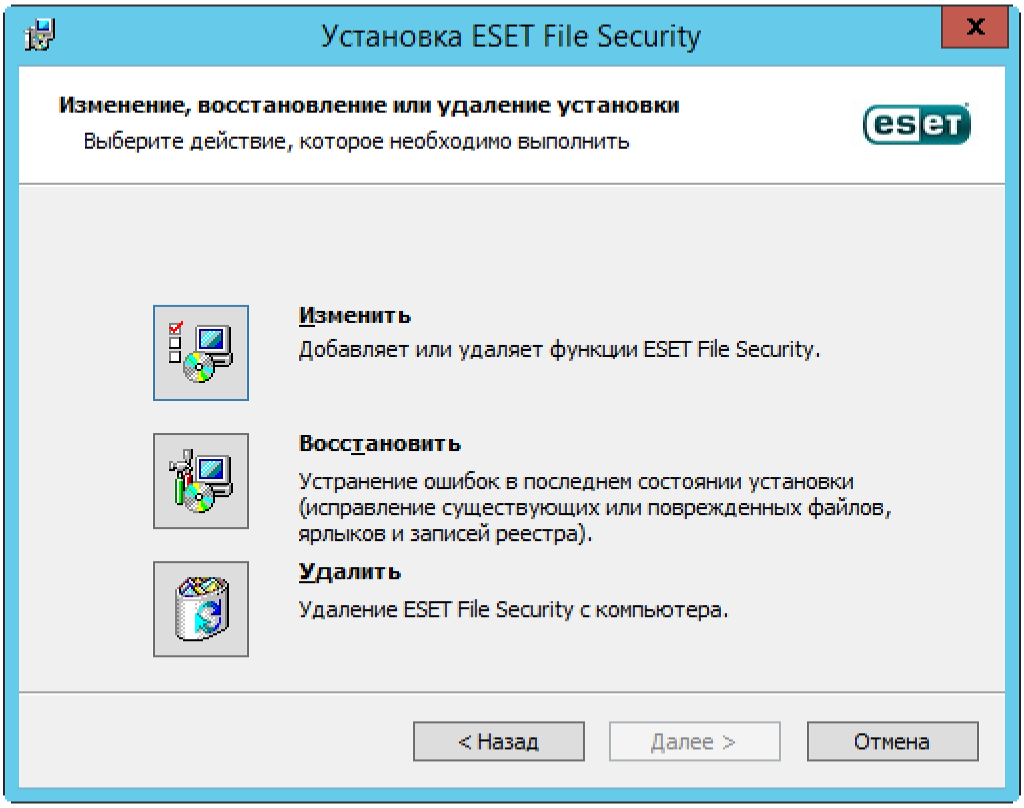


В этом типе можно выбрать, какие функции необходимо установить. Эта возможность полезна, если необходимо установить только те компоненты программы ESET File Security, которые нужны.

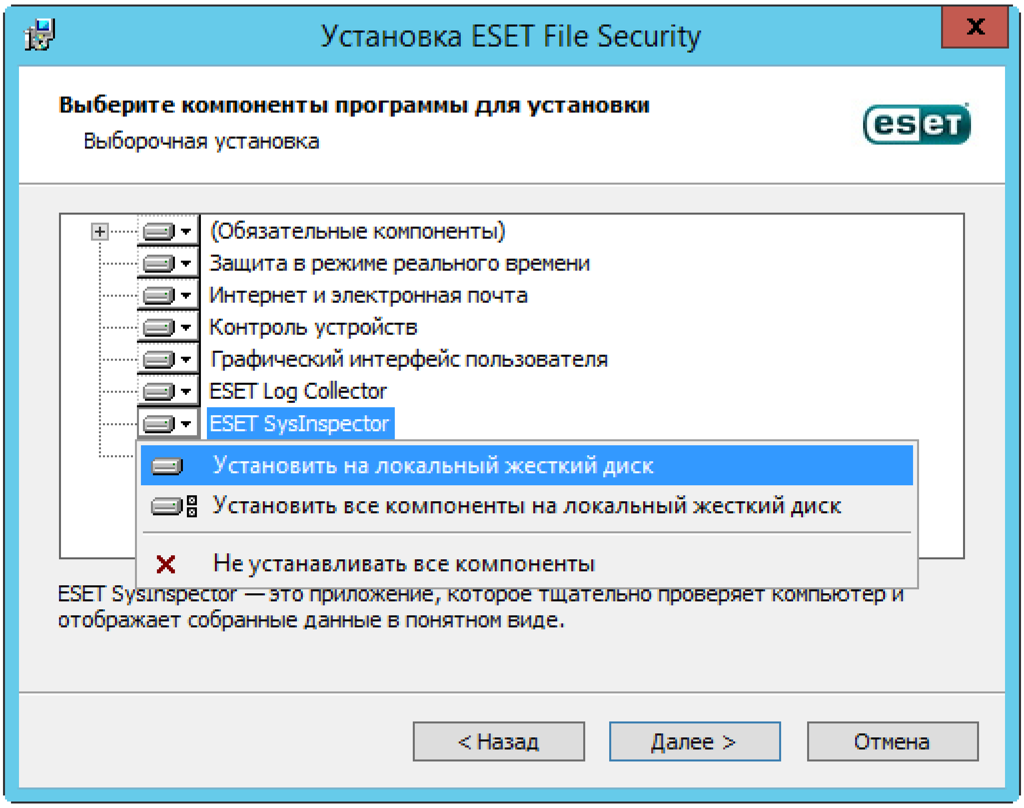
Можно добавлять и удалять компоненты существующей установки. Для этого нужно запустить установочный пакет с расширением `.msi`, который использовался при первой установке, или перейти в раздел **Программы и компоненты** (доступен в панели управления Windows). Правой кнопкой мыши щелкните ESET File Security и выберите команду **Изменить**. Чтобы добавлять или удалять компоненты, выполняйте описанные далее действия.

Изменение компонентов (добавление или удаление), восстановление и удаление

Доступны три возможности: можно **изменить** установленные компоненты, **восстановить** установленную программу ESET File Security или **удалить** ее полностью.



При выборе команды **Изменить** отобразится список всех доступных компонентов программы. Выберите компоненты, которые необходимо добавить или удалить. Одновременно можно добавить или удалить несколько компонентов. Щелкните компонент и выберите нужный пункт раскрывающегося меню.



Выбрав один из пунктов, нажмите кнопку **Изменить**, чтобы внести необходимые изменения.

ПРИМЕЧАНИЕ.
Добавлять новые компоненты можно в любое время. Для этого нужно запустить установщик. Для изменений не требуется перезапуск сервера.

6.1.1 Установка из командной строки

Все приведенные ниже параметры должны использоваться только с **сокращенным**, **основным** и **отсутствующим** уровнями интерфейса. Сведения о версии **msiexec**, используемой для соответствующих параметров командной строки, см. в этой документации.

Поддерживаемые параметры:

APPDIR=<путь>
- Путь — действительный путь к каталогу.
- Каталог установки приложения.
- Например, `efsw_nt64_ENU.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

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

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

ADDEXCLUDE=<список>
- Список ADDEXCLUDE — это список разделенных запятыми имен всех функций, которые не должны быть установлены. Он заменяет устаревший список REMOVE.
- Если указано, что функцию не нужно устанавливать, в список следует явно включить весь путь (т. е. все подчиненные функции) и связанные невидимые функции.
- Например, `efsw_nt64_ENU.msi /qn ADDEXCLUDE=<list>`

ПРИМЕЧАНИЕ.
Свойство **ADDEXCLUDE** нельзя использовать вместе со списком **ADDLOCAL**.

ADDLOCAL=<список>
- Установка компонентов — список необязательных функций, которые нужно установить локально.
- Использование с пакетами формата MSI компании ESET: `efsw_nt64_ENU.msi /qn ADDLOCAL=<list>`
- Дополнительные сведения о свойстве **ADDLOCAL** см. на странице http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx.

Правила

- **Список ADDLOCAL** — это разделенный запятыми список всех функций, которые будут установлены.
- При выборе устанавливаемой функции в список нужно явно добавить весь путь (указать все родительские функции).
- Чтобы все делать верно, см. дополнительные правила.

Наличие функции

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

Ниже приведен пример дерева функций ESET File Security.

Дерево функций	Имя функции	Наличие функции

Компьютер	Компьютер	Обязательная
Компьютер/Защита от вирусов и шпионских программ	Защита от вирусов	Обязательно
Компьютер/Защита от вирусов и шпионских программ > Защита файловой системы в режиме реального времени	Защита в режиме реального времени	Обязательно
Компьютер/Защита от вирусов и шпионских программ > Сканирование компьютера	Сканирование	Обязательно
Компьютер/Защита от вирусов и шпионских программ > Защита документов	Защита документов	Необязательная
Компьютер/Контроль устройств	Контроль устройств	Необязательно
Фильтрация протоколов Интернета и электронной почты	Фильтрация протоколов	Невидимая
Интернет и электронная почта/Защита доступа в Интернет	Защита доступа в Интернет	Необязательно
Интернет и электронная почта/Защита почтового клиента	Защита почтового клиента	Необязательно
Интернет и электронная почта/Защита почтового клиента/Почтовые модули	Почтовые модули	Невидимый режим
Интернет и электронная почта/Контроль доступа в Интернет	Контроль доступа в Интернет	Необязательно
Зеркало обновлений	Зеркало обновлений	Необязательная

Дополнительные правила

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

Пример команды: `efsw_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,WebAccessProtection,ProtocolFiltering`

Примеры базовой установки из командной строки:

```
msiexec /qn /i efsw_nt64_ENU.msi /l inst.log ADDLOCAL=HIPS,_Base,SERVER,_FeaturesCore,WMIProvider,Scan,Updat
```

```
msiexec /qn /i efsw_nt64_ENU.msi /l*xv msi.log ADDLOCAL=SERVER,eShell,RealtimeProtection CFG_POTENTIALLYUNWA
```

Список свойств CFG_:

CFG_POTENTIALLYUNWANTED_ENABLED=1/0

- 0 — отключено, 1 — включено.

CFG_LIVEGRID_ENABLED=1/0

- 0 — отключено, 1 — включено;
- LiveGrid.

FIRSTSCAN_ENABLE=1/0

- 0 — отключить, 1 — включить;
- Запланировать новое первое сканирование после установки.

CFG_PROXY_ENABLED=0/1

- 0 — отключено, 1 — включено.

CFG_PROXY_ADDRESS=<IP-адрес>

- IP-адрес прокси-сервера.

CFG_PROXY_PORT=<порт>

- Номер порта прокси-сервера.

CFG_PROXY_USERNAME=<пользователь>

- Имя пользователя для проверки подлинности.

CFG_PROXY_PASSWORD=<пароль>

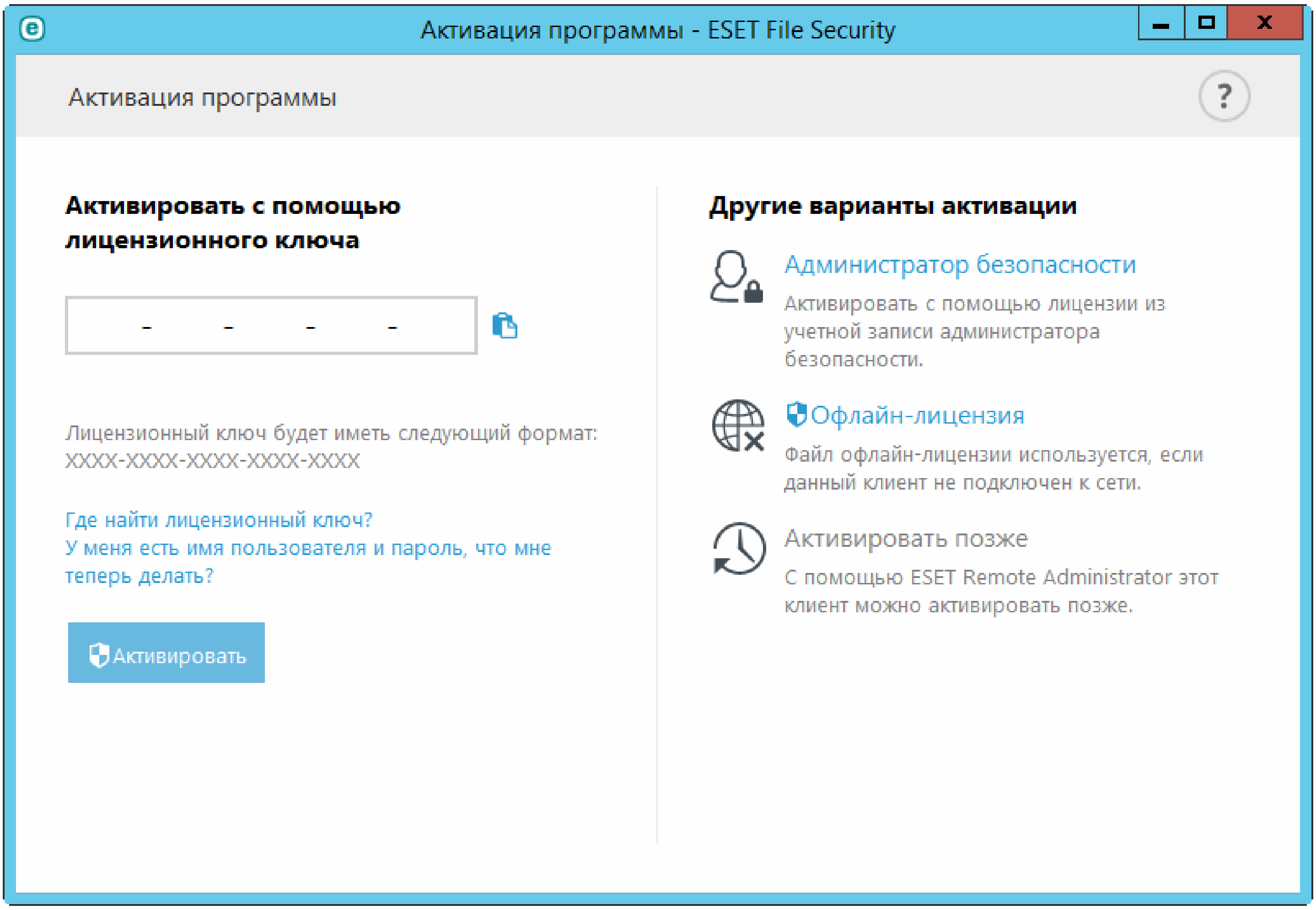
- Пароль для проверки подлинности.

6.1.2 Установка в кластерной среде

ESET File Security можно развернуть в кластерной среде (например, в отказоустойчивом кластере). Рекомендуется установить ESET File Security на активном узле, а затем распределить установку по пассивным узлам с помощью компонента Кластер ESET программного обеспечения ESET File Security. Помимо установки, кластер ESET служит для репликации конфигурации ESET File Security, обеспечивая согласованность между узлами кластера, необходимыми для корректной работы.

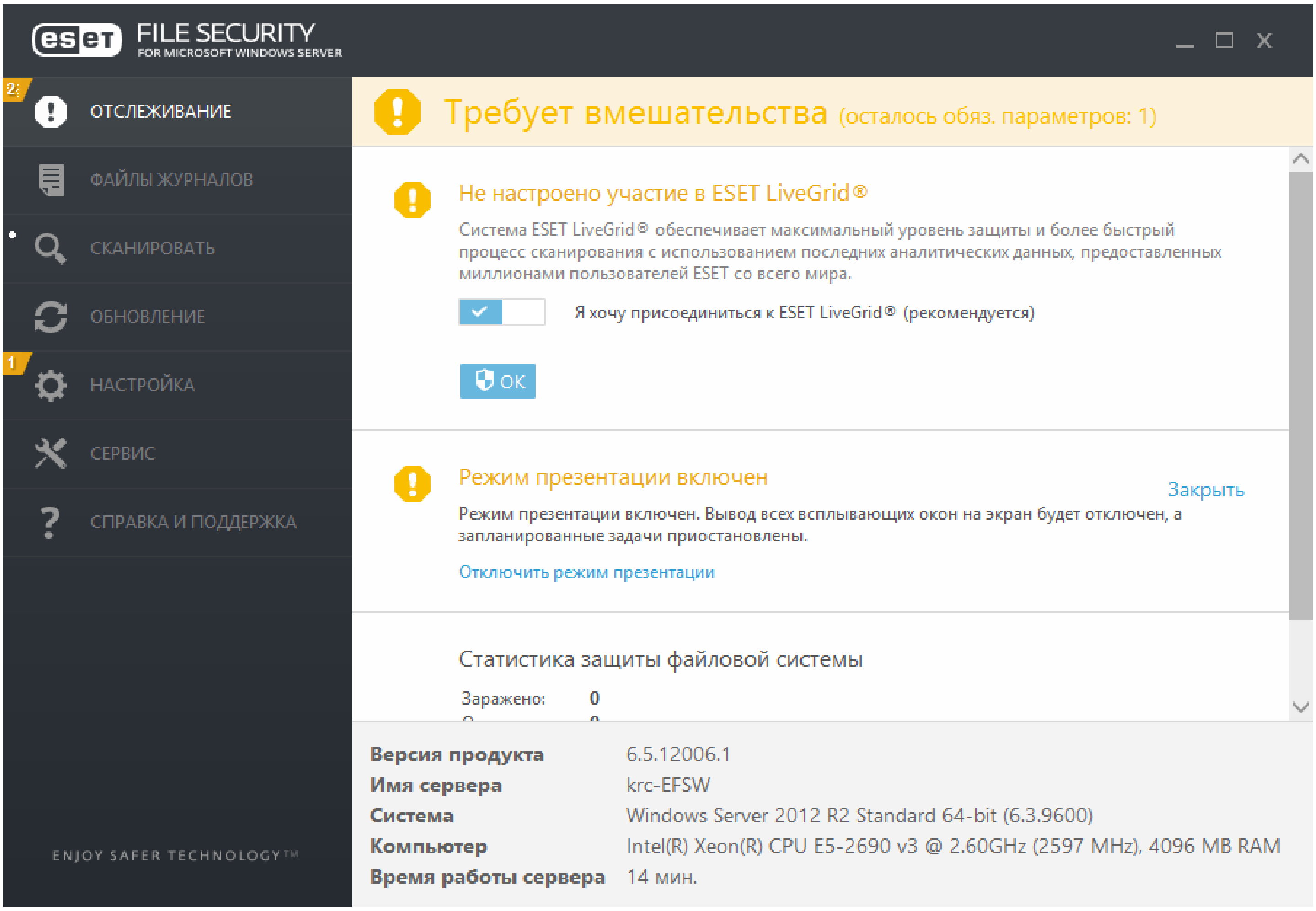
6.2 Активация программы

По завершении установки вам будет предложено активировать установленный продукт.



Выберите доступный метод активации ESET File Security. См. раздел Активация ESET File Security для получения дополнительных сведений.

После активации ESET File Security на странице Мониторинг откроется главное окно программы, в котором отобразится ваше текущее состояние. Возможно, в самом начале нужно будет уделить продукту немного времени: к примеру, вам будет предложено присоединиться к ESET LiveGrid.



Кроме того, в главном окне программы отображаются уведомления о таких элементах, как обновления системы (обновления Windows) и обновления базы данных сигнатур вирусов. Когда все вопросы, требующие внимания, решены, состояние мониторинга становится зеленым и для него отображается значение **Максимальная защита**.

6.3 Сервер терминалов

Если программное обеспечение ESET File Security устанавливается на сервере Windows Server, который выступает в качестве сервера терминалов, полезно будет отключить графический интерфейс пользователя ESET File Security, чтобы предотвратить запуск программы при каждом входе пользователя в систему. Конкретные инструкции по отключению приводятся в главе Отключение графического интерфейса пользователя на сервере терминалов.

6.4 ESET AV Remover

Для удаления сторонних антивирусных программ рекомендуется использовать средство ESET AV Remover. Для этого выполните следующие действия:

1. Загрузите средство ESET AV Remover со страницы загрузки утилит веб-сайта ESET.
2. Чтобы принять условия лицензионного соглашения и начать поиск в системе, нажмите кнопку **Я принимаю, начать поиск**.
3. Чтобы удалить установленные на компьютере антивирусные программы, щелкните элемент **Запустить средство удаления**.

Список сторонних антивирусных программ, которые можно удалить с помощью средства ESET AV Removal, см. в этой статье базы знаний.

6.5 Обновление до новой версии

Новые версии ESET File Security выпускаются для реализации улучшений или исправления проблем, которые не могут быть устранены автоматическим обновлением модулей программы. Можно использовать следующие методы обновления.

- Вручную — загрузка и установка новой версии поверх используемой. Для этого необходимо просто запустить программу установки и выполнить установку привычным способом, при этом ESET File Security автоматически перенесет существующую конфигурацию. Эта процедура рекомендуется в том случае, если ESET File Security работает на одном сервере. Применяется для обновления с любых более старых версий до версий 6.x.
- Удаленно — для использования в крупных сетевых средах под управлением ESET Remote Administrator. Этот способ полезен в тех случаях, когда ESET File Security работает на нескольких серверах. Применяется для обновления с версий 4.x. до версий 6.x.
- С помощью мастера кластеров ESET — этот способ также можно использовать для обновления. Этот способ рекомендуется, если программа ESET File Security используется как минимум на двух серверах. Применяется для обновления с версий 4.x. до версий 6.x. Кроме того, после обновления можно продолжить использование всех возможностей кластера ESET.

ПРИМЕЧАНИЕ.
В процессе обновления программы ESET File Security потребуется перезагрузка сервера.

ПРИМЕЧАНИЕ.
По завершении обновления ESET File Security рекомендуется проверить все параметры и убедиться, что они настроены правильно и в соответствии с вашими потребностями.

6.5.1 Обновление с помощью ERA

ESET Remote Administrator позволяет обновлять несколько серверов, на которых работают более ранние версии программы ESET File Security. Преимуществом данного способа является возможность одновременного обновления большого количества серверов, при котором все экземпляры программы ESET File Security имеют одинаковые настройки (если это необходимо).

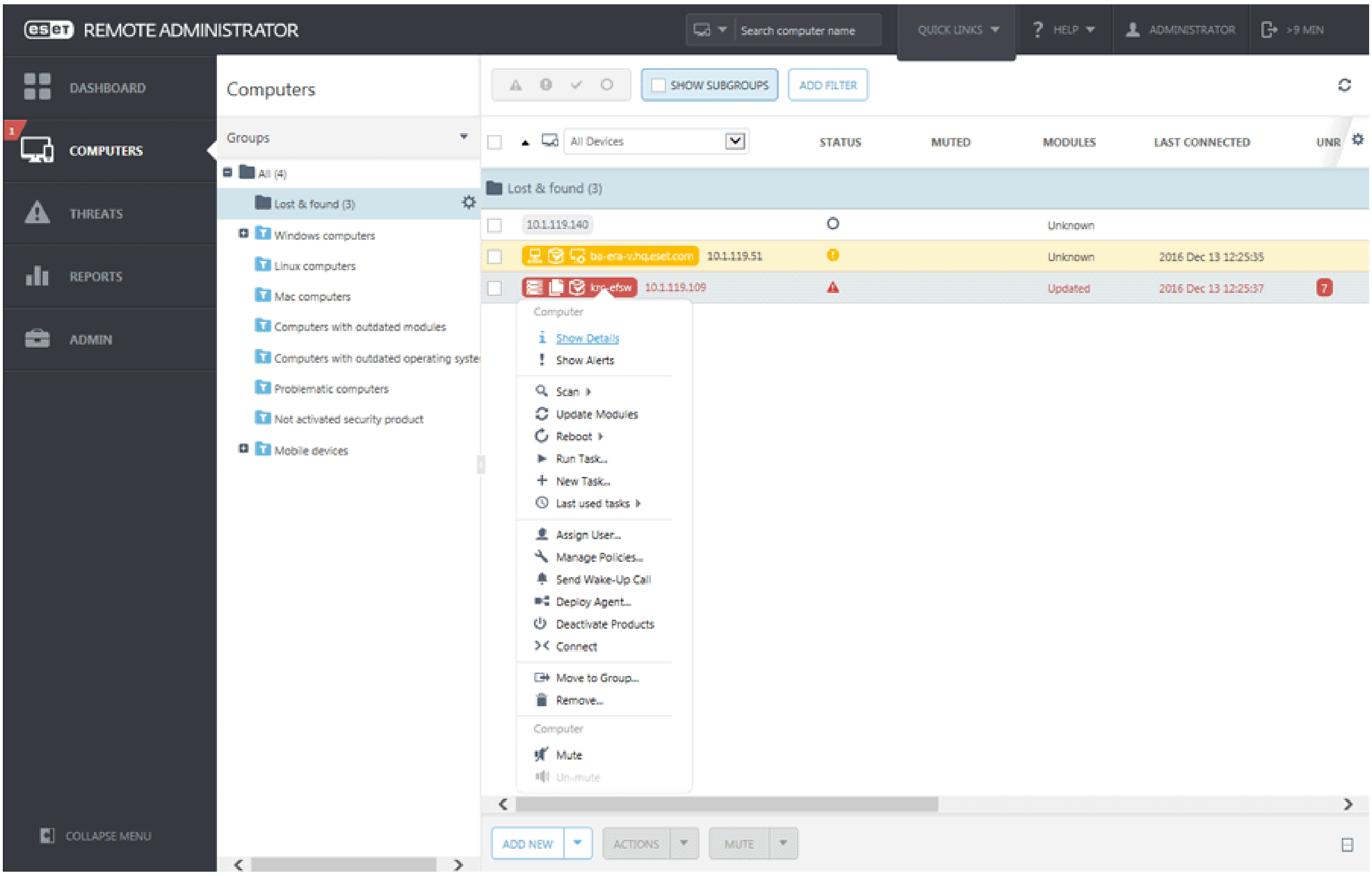
ПРИМЕЧАНИЕ.
Применяется для обновления с версий 4.x. до версий 6.x.

Процедура требует выполнения следующих действий:

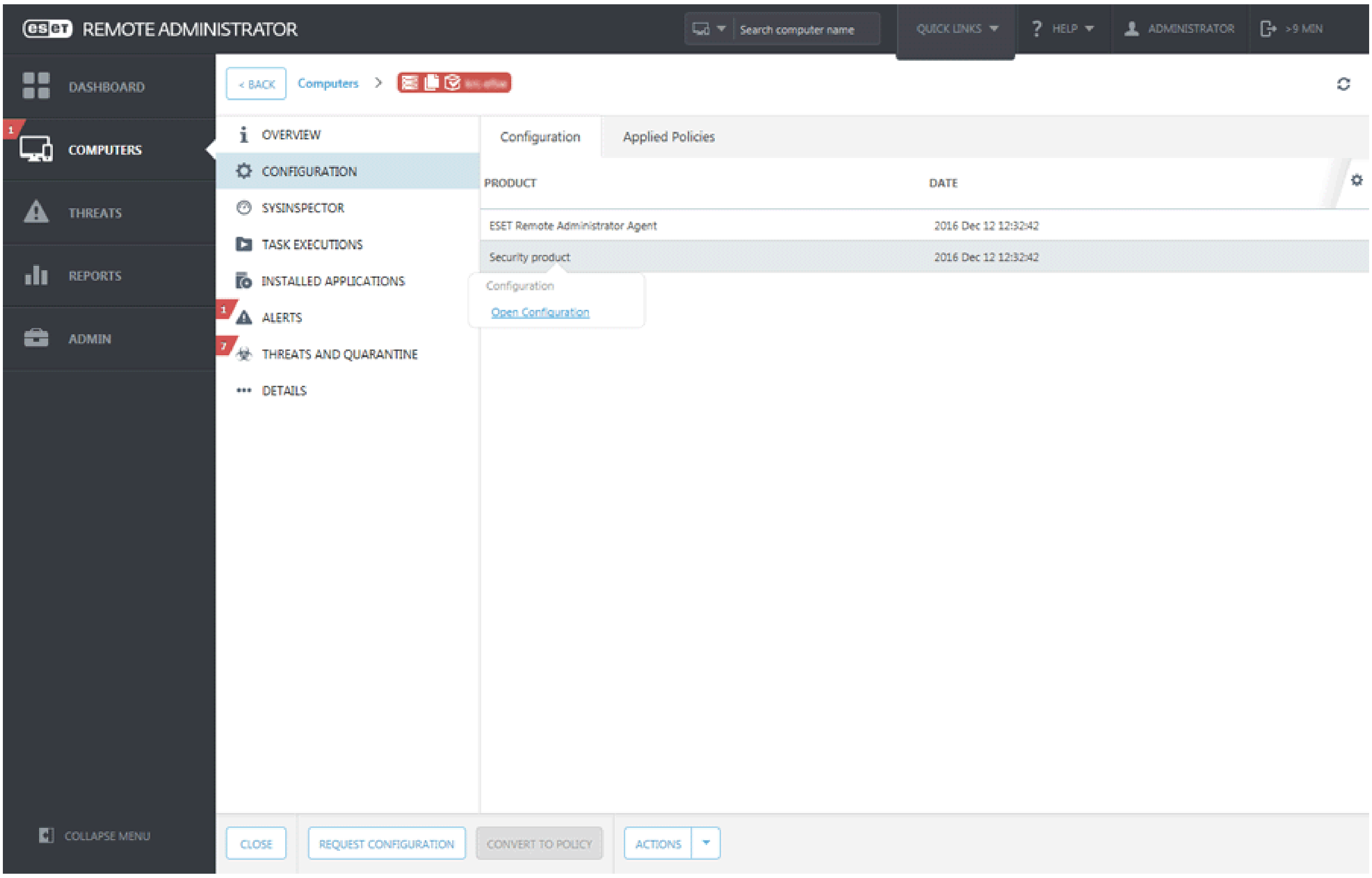
- **Обновите первый сервер** вручную путем установки последней версии программы ESET File Security поверх существующей версии, чтобы полностью сохранить конфигурацию, в том числе правилаи т. д. Это действие выполняется локально на сервере, на котором работает программа ESET File Security.
- **Запросите конфигурацию** программы ESET File Security, обновленной до версии 6.х., и **преобразуйте ее в политику** в ERA. Впоследствии эта политика будет применяться ко всем обновленным серверам. Эти и последующие действия выполняются удаленно в ERA.
- Запустите задачу **удаления программного обеспечения** на всех серверах, на которых работает старая версия ESET File Security.
- Запустите задачу **установки программного обеспечения** на всех серверах, на которых должна работать новая версия ESET File Security.
- **Назначьте политику конфигурации** для всех серверов, на которых работает новая версия программы ESET File Security.

Пошаговая процедура:

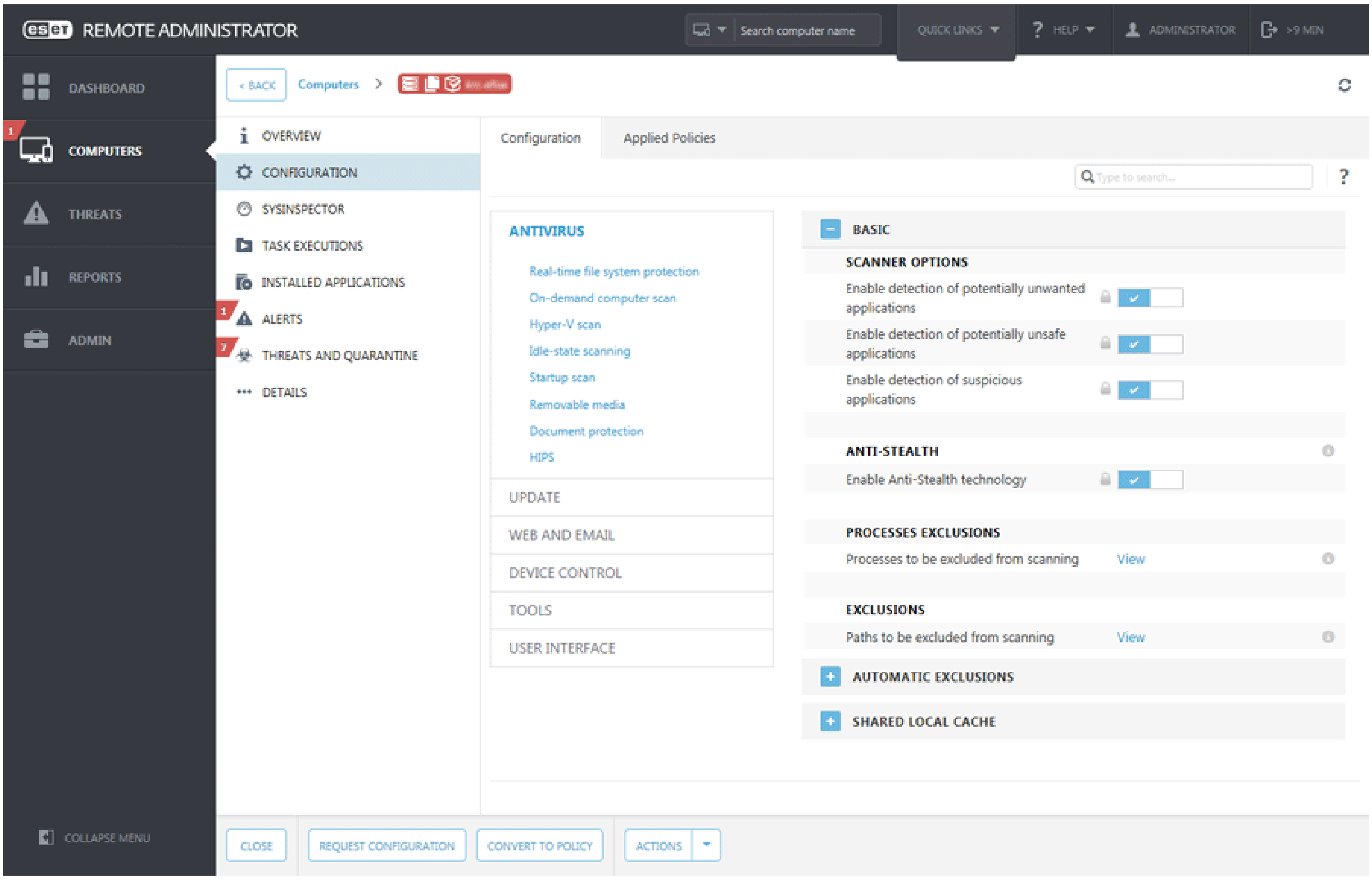
1. Войдите на один из серверов, на которых работает программа ESET File Security, и обновите ее, загрузив и установив новую версию поверх существующей. Следуйте [инструкциям по обычной установке](). При установке исходная конфигурация старой версии программы ESET File Security будет полностью сохранена.
2. Откройте **веб-консоль ERA**, выберите клиентский компьютер в статической или динамической группе, а затем щелкните **Показать подробности**.



3. Перейдите на вкладку Конфигурация и нажмите кнопку **Запросить конфигурацию**, чтобы собрать всю конфигурацию управляемого продукта. Получение конфигурации может занять некоторое время. После появления в списке последней конфигурации щелкните **Программа по обеспечению безопасности** и выберите **Открыть конфигурацию**.



4. Создайте политику конфигурации, нажав кнопку **Преобразовать в политику**. Укажите **имя** для новой политики и нажмите кнопку **Готово**.



5. Перейдите в **Администрирование** > **Клиентские задачи** и выберите задачу Удаление программного обеспечения. При создании задачи по удалению рекомендуется перезагрузить сервер после удаления. Для этого установите флажок **Выполнить автоматическую перезагрузку при необходимости**. Создав задачу, добавьте все целевые компьютеры, на которых необходимо выполнить удаление.

6. Убедитесь, что программа ESET File Security удалена на всех целевых компьютерах.

7. Создайте задачу Установка программного обеспечения, чтобы установить новую версию программы ESET File Security на все целевые компьютеры.

8. **Назначьте политику конфигурации** для всех серверов, на которых работает ESET File Security (по возможности сделайте это для группы серверов).

6.5.2 Обновление с помощью кластера ESET

Создание кластера ESET позволяет обновить несколько серверов, на которых установлены более старые версии программы ESET File Security. Этот способ является альтернативой обновлению с помощью ERA. Если в вашей среде есть два и более серверов с программой ESET File Security, рекомендуется использовать способ с применением кластера ESET. Другим преимуществом этого способа обновления является возможность дальнейшего использования кластера ESET для синхронизации конфигурации программы ESET File Security на всех узлах-участниках.

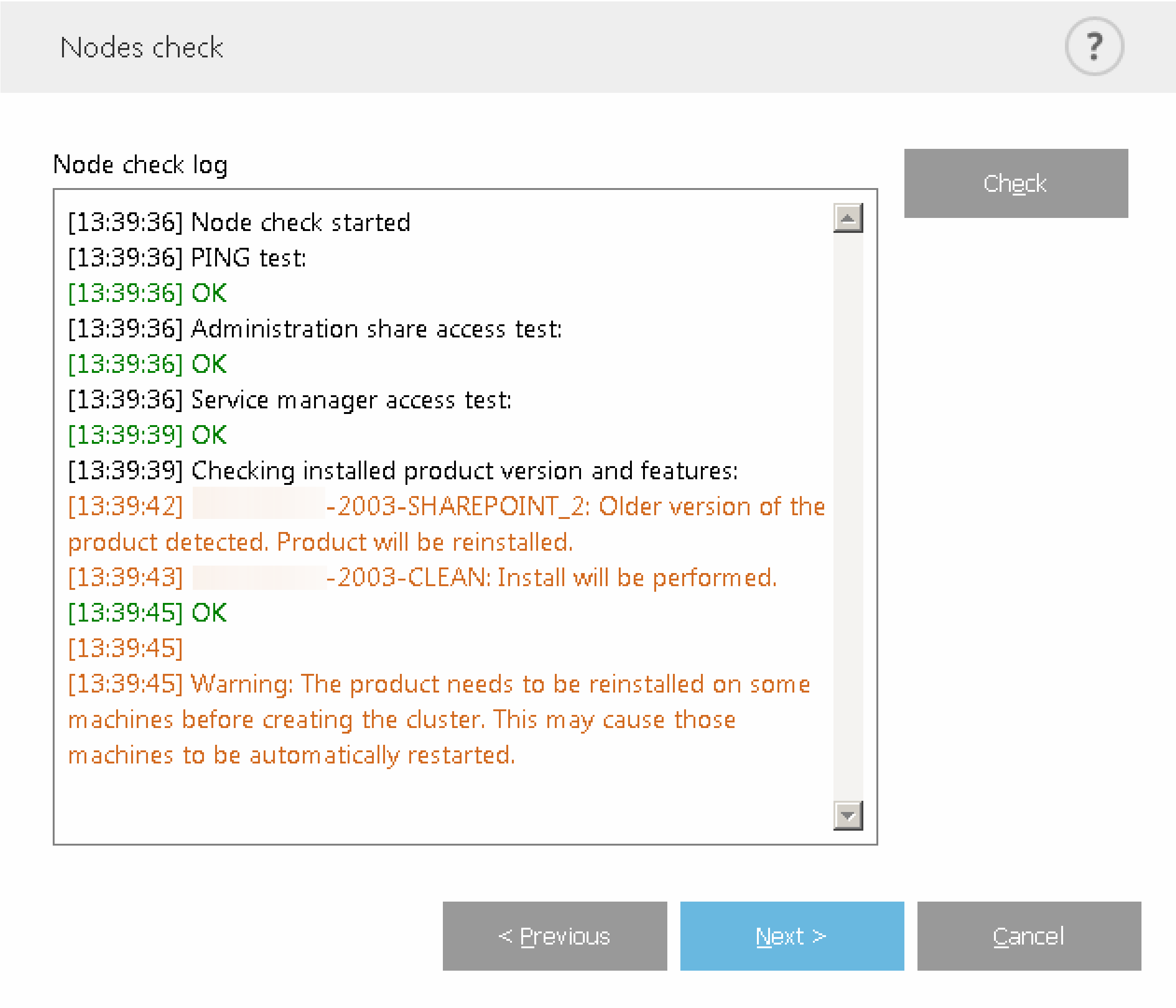
ПРИМЕЧАНИЕ.
Применяется для обновления с версий 4.x. до версий 6.x.

Чтобы выполнить обновление с помощью этого способа, выполните следующие действия.

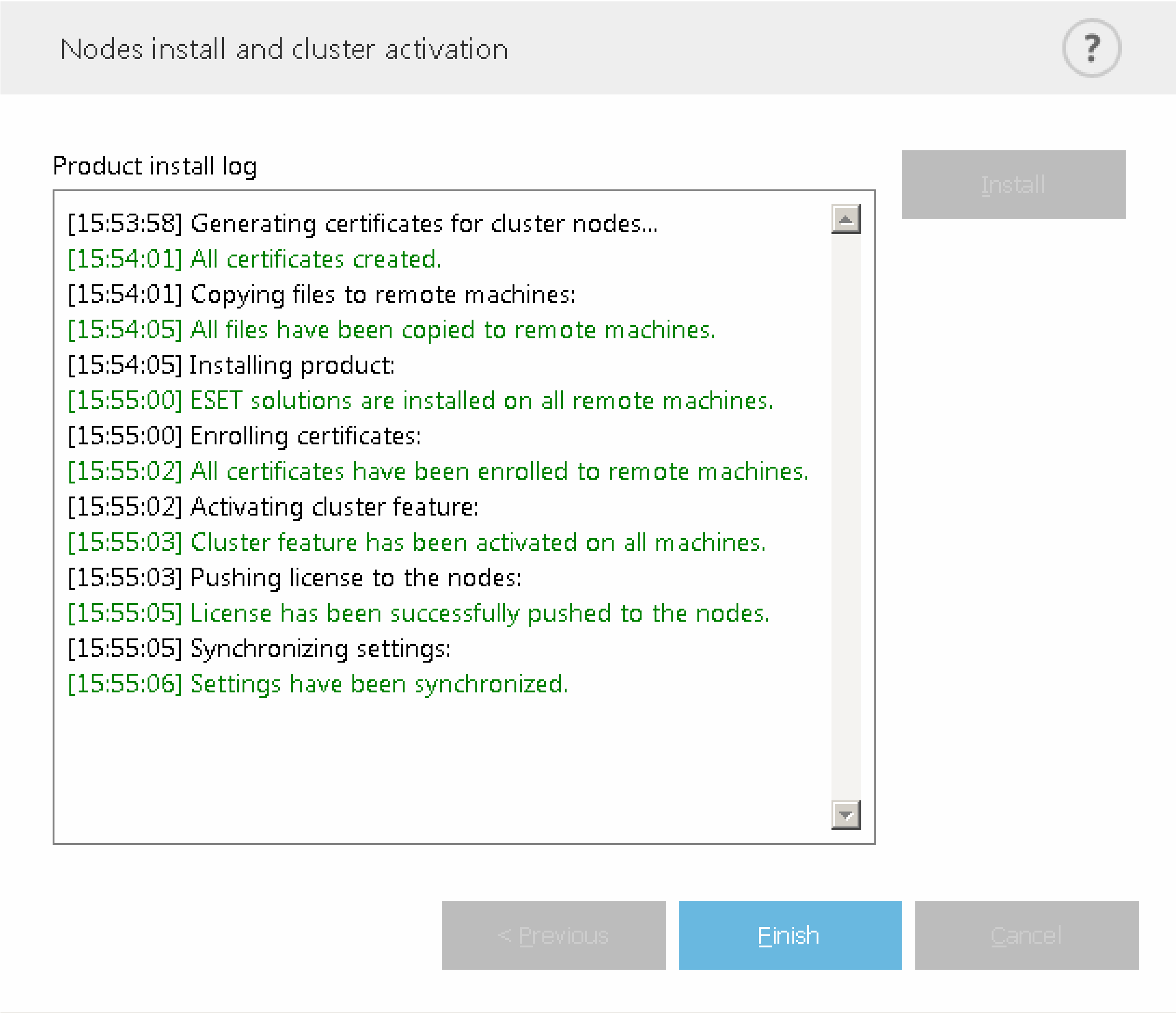
1. Войдите на один из серверов, на которых работает программа ESET File Security, и обновите ее, загрузив и установив новую версию поверх существующей. Следуйте инструкциям по обычной установке. При установке исходная конфигурация старой версии программы ESET File Security будет полностью сохранена.

2. Запустите [мастер кластеров ESET](#) и добавьте узлы кластера (серверы, на которых необходимо обновить ESET File Security). При необходимости можно добавить другие серверы, на которых еще не установлена программа ESET File Security (на них будет выполнена установка). При указании [имени кластера и типа установки](#) рекомендуется оставить значения по умолчанию (убедитесь, что установлен флажок **Передать лицензию на узлы без активированного продукта**).

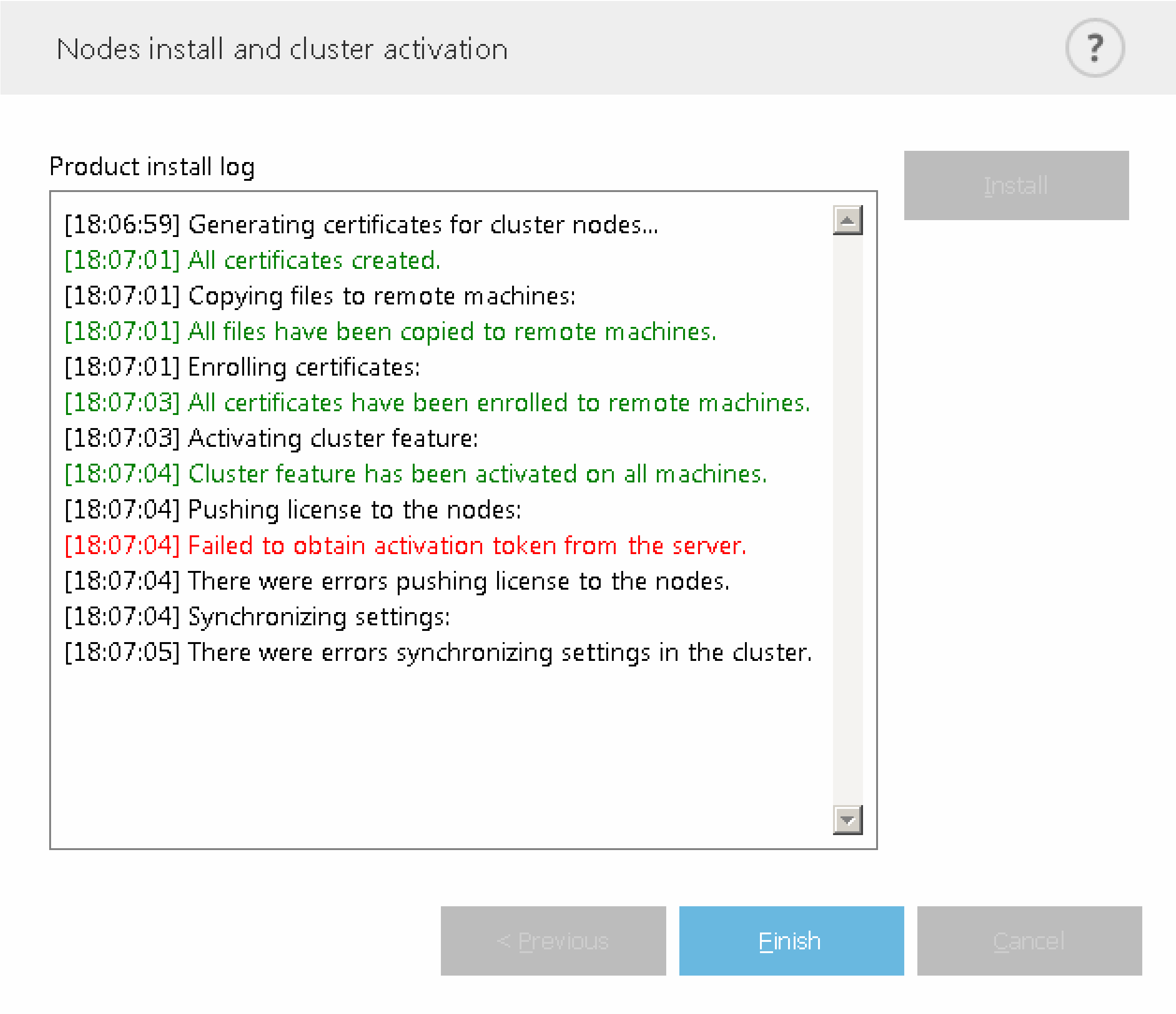
3. Просмотрите экран **Журнал проверки узлов**. На нем будет отображаться список серверов, на которых установлены более старые версии программы, а также уведомление о том, что продукт будет переустановлен. Программа ESET File Security будет также установлена на все добавленные серверы, на которых она еще не установлена.



4. На экране **Установка узлов и активация кластера** отобразится ход установки. В случае успешного завершения установки результат должен выглядеть следующим образом:



В случае неправильной настройки сети или службы DNS может отобразиться следующее сообщение об ошибке: **Не удалось получить от сервера маркер активации**. Попробуйте снова запустить мастер кластеров ESET. В результате этого старый кластер будет удален, а вместо него будет создан новый (без необходимости переустановки программы), и в этот раз активация должна завершиться успешно. Если это не поможет, проверьте параметры сети и службы DNS.



7. Руководство для начинающих

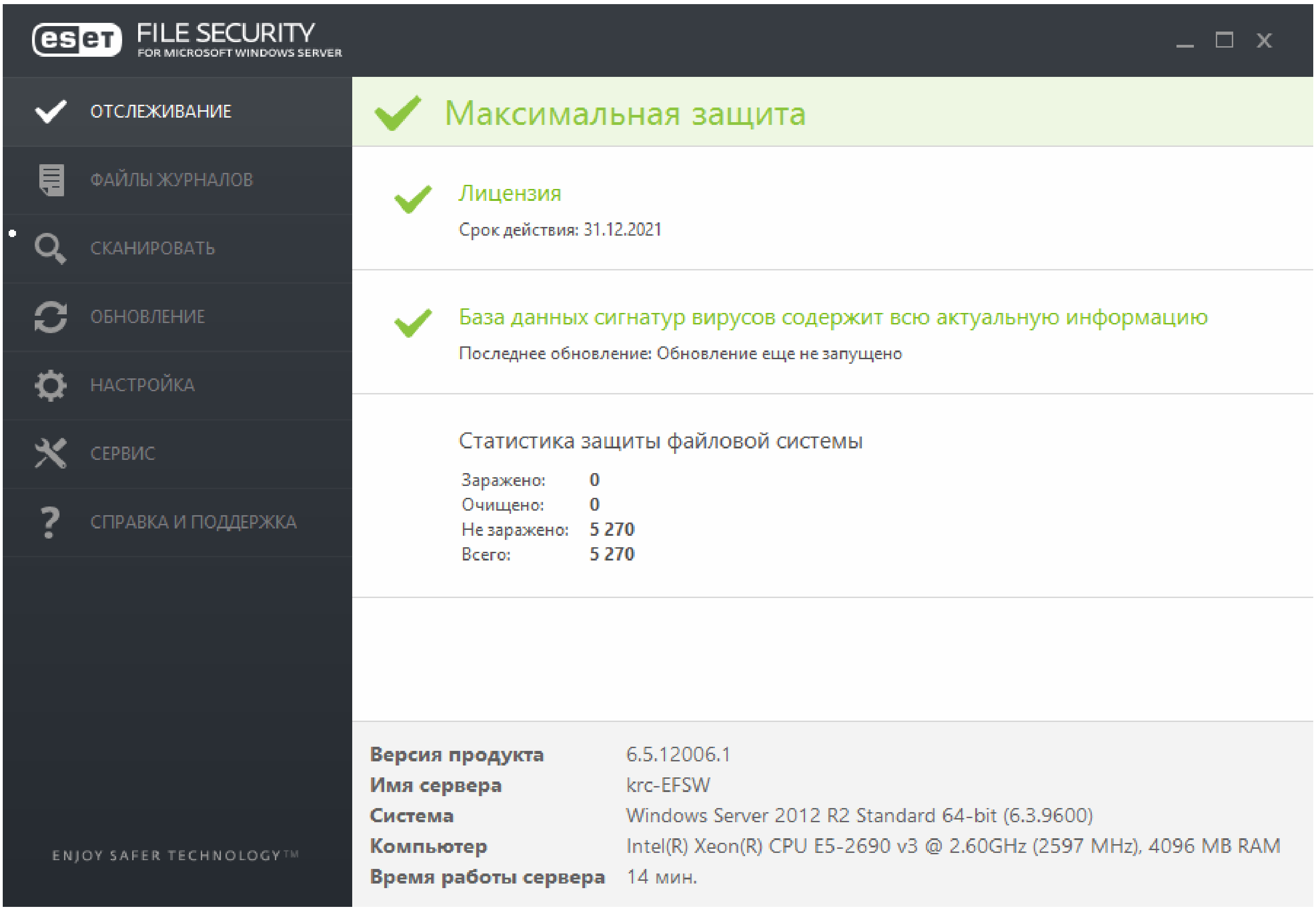
Этот раздел содержит обзор приложения ESET File Security, основных пунктов меню, функций и основных параметров.

- Отслеживание
- Файлы журналов
- Сканирование
- Обновление
- Настройка
- Служебные программы
- Справка и поддержка

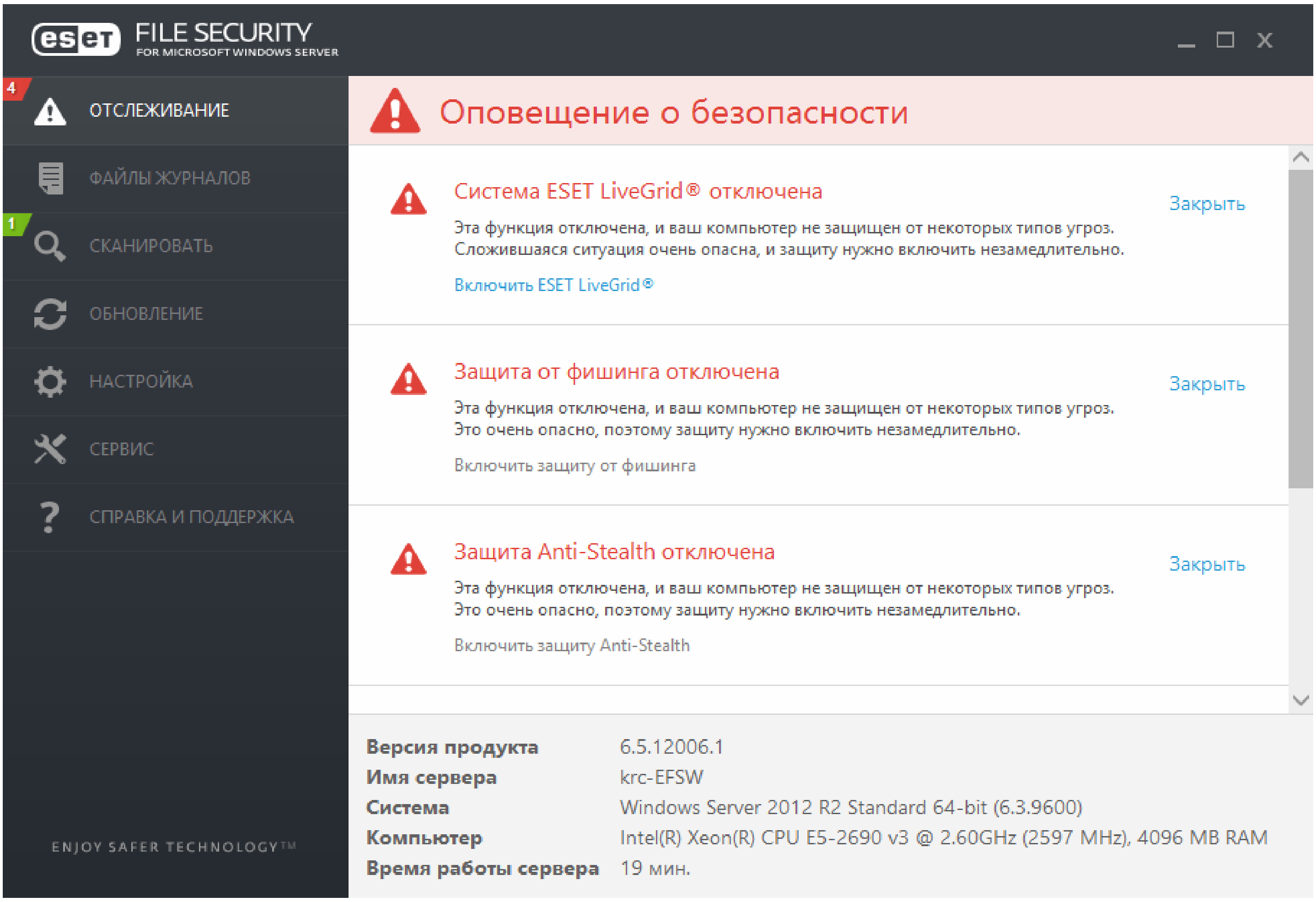
7.1 Отслеживание

Состояние защиты, отображаемое в разделе **Мониторинг**, информирует о текущем уровне защиты компьютера. В основном окне отображается сводная информация о работе ESET File Security.

Зеленый значок **Максимальная защита** означает, что обеспечивается максимальная степень защиты. В окне состояния также отображаются ссылки на часто используемые функции программы ESET File Security и информация о последнем обновлении.



Модули, работающие правильно, обозначаются зеленым флажком. Модули, работающие неправильно, обозначаются красным восклицательным знаком или оранжевым значком уведомления. В верхней части окна выводятся дополнительные сведения о модуле. Кроме того, предлагается решение проблемы. Для того чтобы изменить состояние отдельного модуля, выберите в главном меню пункт **Настройка** и щелкните нужный модуль.



Красный значок показывает наличие критических проблем, из-за которых максимальная степень защиты компьютера не обеспечивается. Отобразится красный значок, указывающий на следующие сценарии:

- **Защита файловой системы в режиме реального времени приостановлена**: щелкните **Включить защиту в режиме реального времени** на вкладке **Отслеживание** или повторно включите параметр **Защита файловой системы в режиме реального времени** на вкладке Настройки главного окна программы.
- **База данных сигнатур вирусов устарела**: программа использует устаревшую базу данных сигнатур вирусов.
- **Продукт не активирован** или **Срок действия лицензии истек**: об этих проблемах свидетельствует красный значок состояния защиты. С этого момента программа больше не сможет выполнять обновления. Для продления лицензии следуйте инструкциям в окне предупреждения.

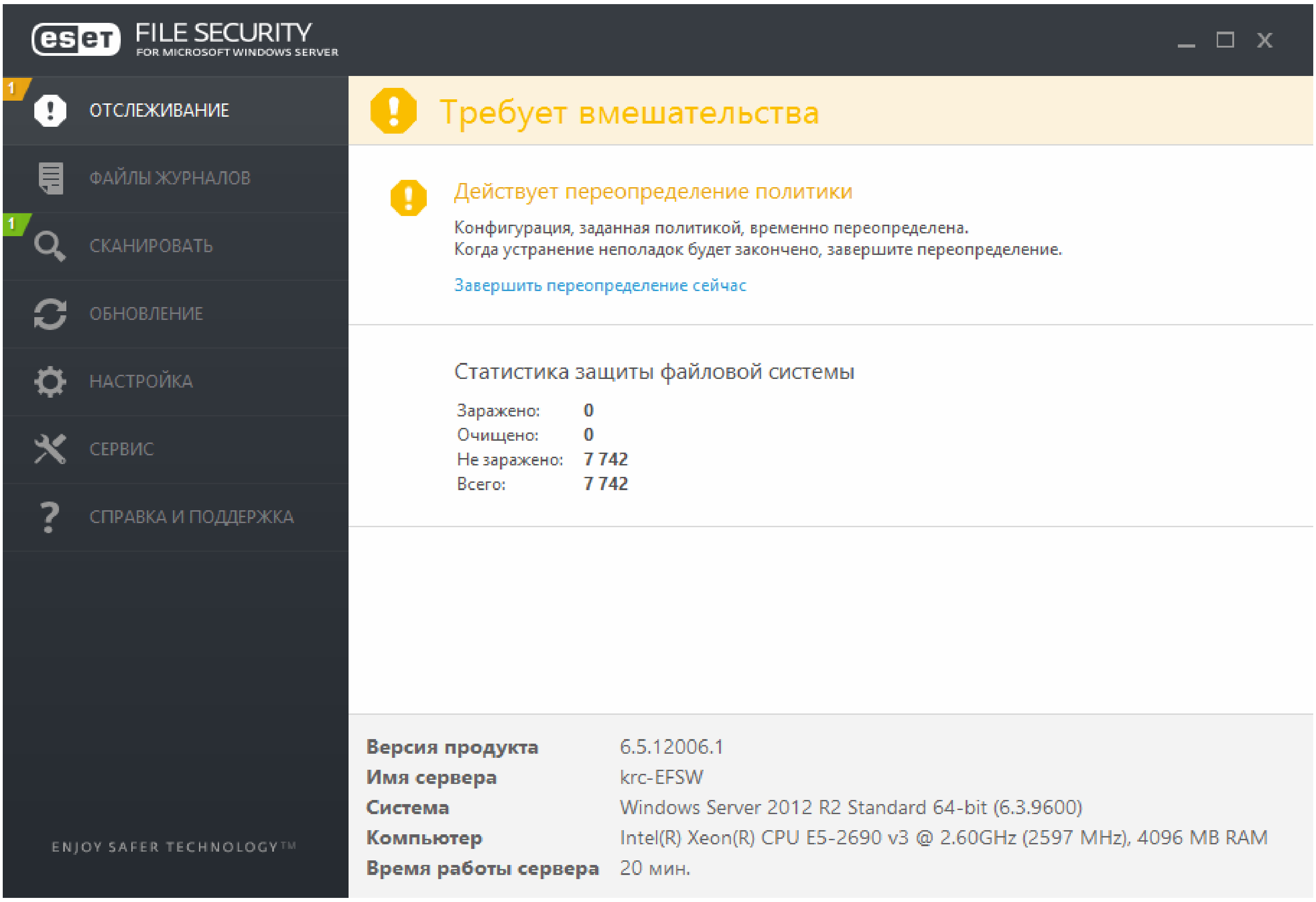
ПРИМЕЧАНИЕ.

Если вы управляете программой ESET File Security с помощью решения ERA и назначили этой программе политику, ссылка на состояние блокируется (отображается как неактивная) в зависимости от того, какие функции включает в себя политика.

Оранжевый значок указывает на то, что продукт ESET требует вашего внимания в связи с некритичной проблемой. Отобразится оранжевый значок, сигнализирующий о следующих сценариях:

- **Защита доступа в Интернет приостановлена**: щелкните **Включить защиту доступа в Интернет** на вкладке **Отслеживание** или повторно включите параметр **Защита доступа в Интернет** на панели Настройки главного окна программы.

- **Режим презентации включен**: вывод всех всплывающих окон на экран будет отключен, а запланированные задачи приостановлены.
- **Срок действия лицензии скоро закончится**: об этой проблеме свидетельствует появление восклицательного знака на значке состояния защиты. После окончания срока действия лицензии программа больше не сможет выполнять обновления, а значок состояния защиты станет красным.
- Действует переопределение политики: конфигурация, заданная политикой, временно переопределена, возможно, до завершения устранения неполадок.



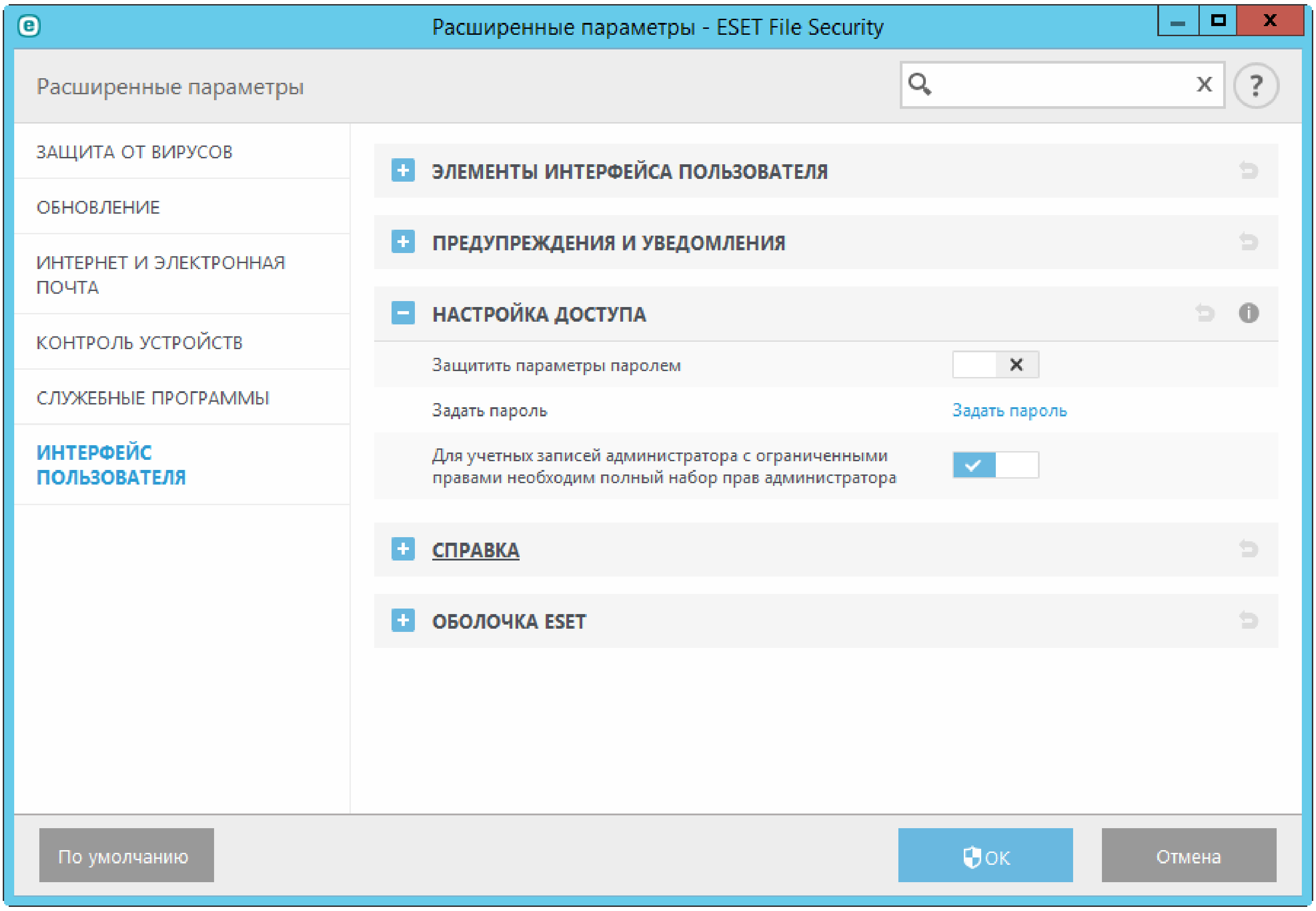
На странице «Мониторинг» также содержится информация о вашей системе, включая следующее:

Версия продукта — номер версии приложения ESET File Security.
Имя сервера — имя хоста или полное доменное имя компьютера.
Система — информация об операционной системе.
Компьютер — сведения об оборудовании.
Время работы сервера — информация о том, сколько система работает без остановки на данный момент. По сути, это антоним слова «простой».

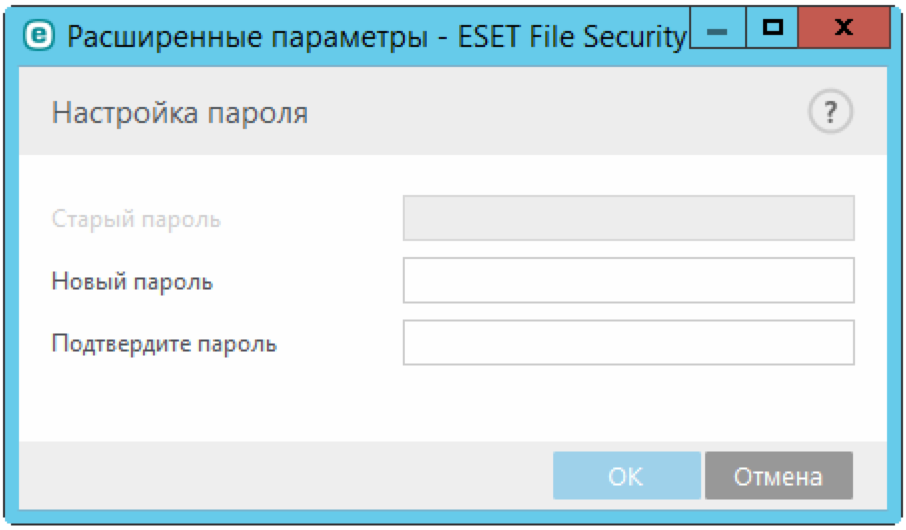
Если предложенные решения не позволяют устранить проблему, выберите пункт **Справка и поддержка** для доступа к файлам справки или поиска в базе знаний ESET. Если же помощь все еще нужна, можно отправить запрос в службу поддержки клиентов ESET. Ее специалисты оперативно ответят на ваши вопросы и помогут найти решение.

7.1.1 Защита настроек

Параметры ESET File Security могут иметь большое значение с точки зрения политики безопасности вашей организации. Несанкционированное изменение параметров способно нарушить стабильность работы системы и ослабить ее защиту. Чтобы открыть параметры настройки **интерфейса**, в главном меню выберите пункт **Настройка** и щелкните элемент **Дополнительные настройки** или нажмите клавишу **F5**. Выберите элементы **Интерфейс** > **Настройка доступа**, выберите пункт **Защитить параметры паролем** и нажмите кнопку **Установить пароль**.

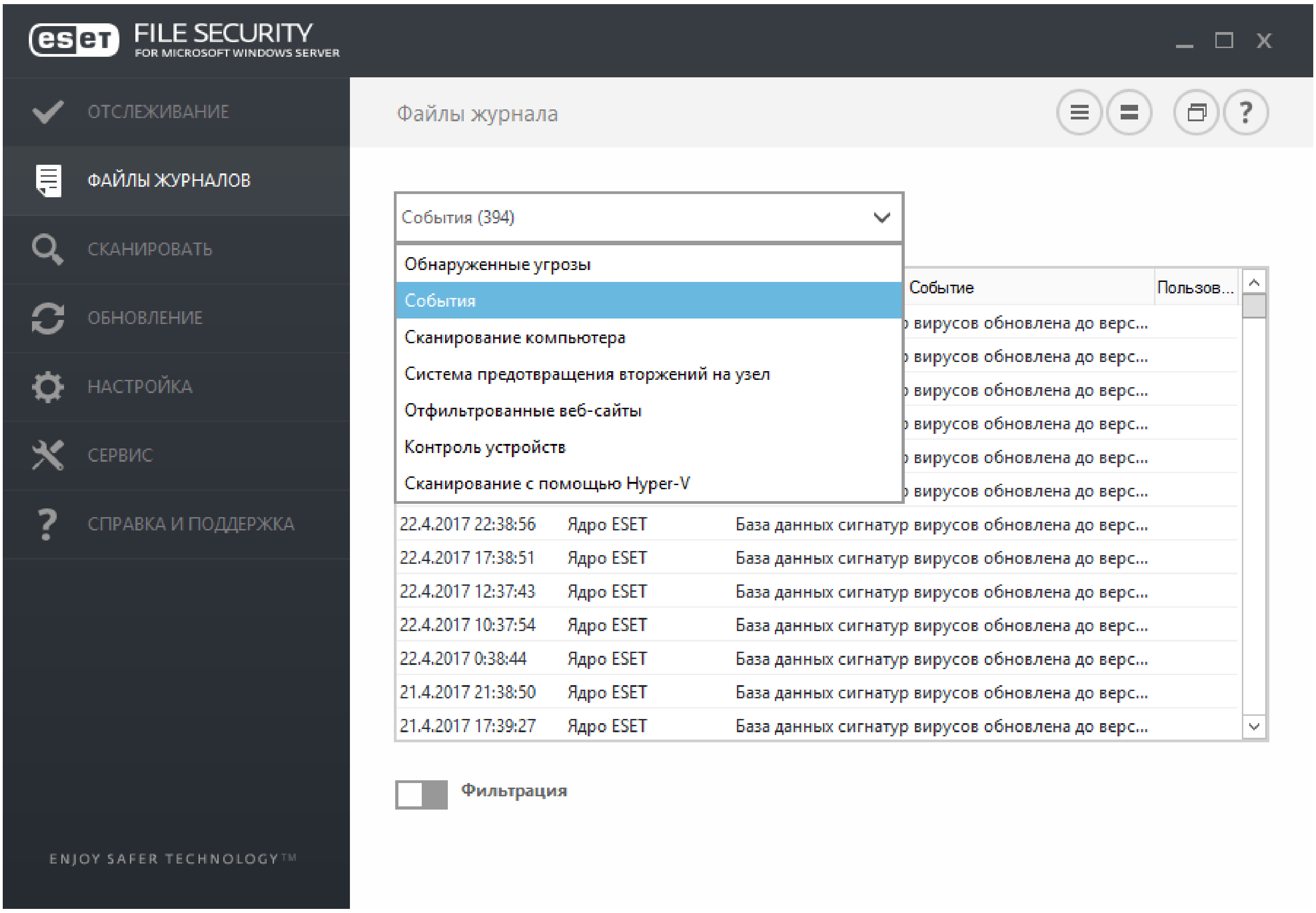


Введите пароль в поля **Новый пароль** и **Подтвердите пароль** и нажмите кнопку **ОК**. Этот пароль будет необходим для внесения в будущем любых изменений в ESET File Security.



7.2 Файлы журналов

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



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

- **Обнаруженные угрозы**: журнал угроз содержит подробную информацию о заражениях, обнаруженных модулями ESET File Security. Регистрируется информация о времени обнаружения, название угрозы, место обнаружения, выполненные действия и имя пользователя, который находился в системе при обнаружении проникновения. Дважды щелкните запись журнала для просмотра подробного содержимого в отдельном окне.

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

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

- **HIPS**: система содержит записи о правилах, помеченных для внесения в журнал. Протокол показывает приложение, которое вызвало операцию, результат (было ли правило разрешено или запрещено) и имя созданного правила.

- **Отфильтрованные веб-сайты**: этот список используется для просмотра списка веб-сайтов, заблокированных функцией защиты доступа в Интернет. В этих журналах отображается время, URL-адрес, пользователь и приложение, с помощью которого установлено соединение с тем или иным веб-сайтом.

- **Контроль устройств**: содержит список подключенных к компьютеру съемных носителей и устройств. Сведения об устройствах в этот журнал вносятся только на основании правила контроля устройств. Запись об устройстве, которое не отвечает условиям правила, в журнале не создается. Здесь отображаются и такие сведения, как тип устройства, серийный номер, имя поставщика и размер носителя (при его наличии).

- **Сканирование с помощью Hyper-V**: содержит список результатов сканирования Hyper-V. Чтобы получить подробную информацию о той или иной операции сканирования, дважды щелкните соответствующую запись.

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

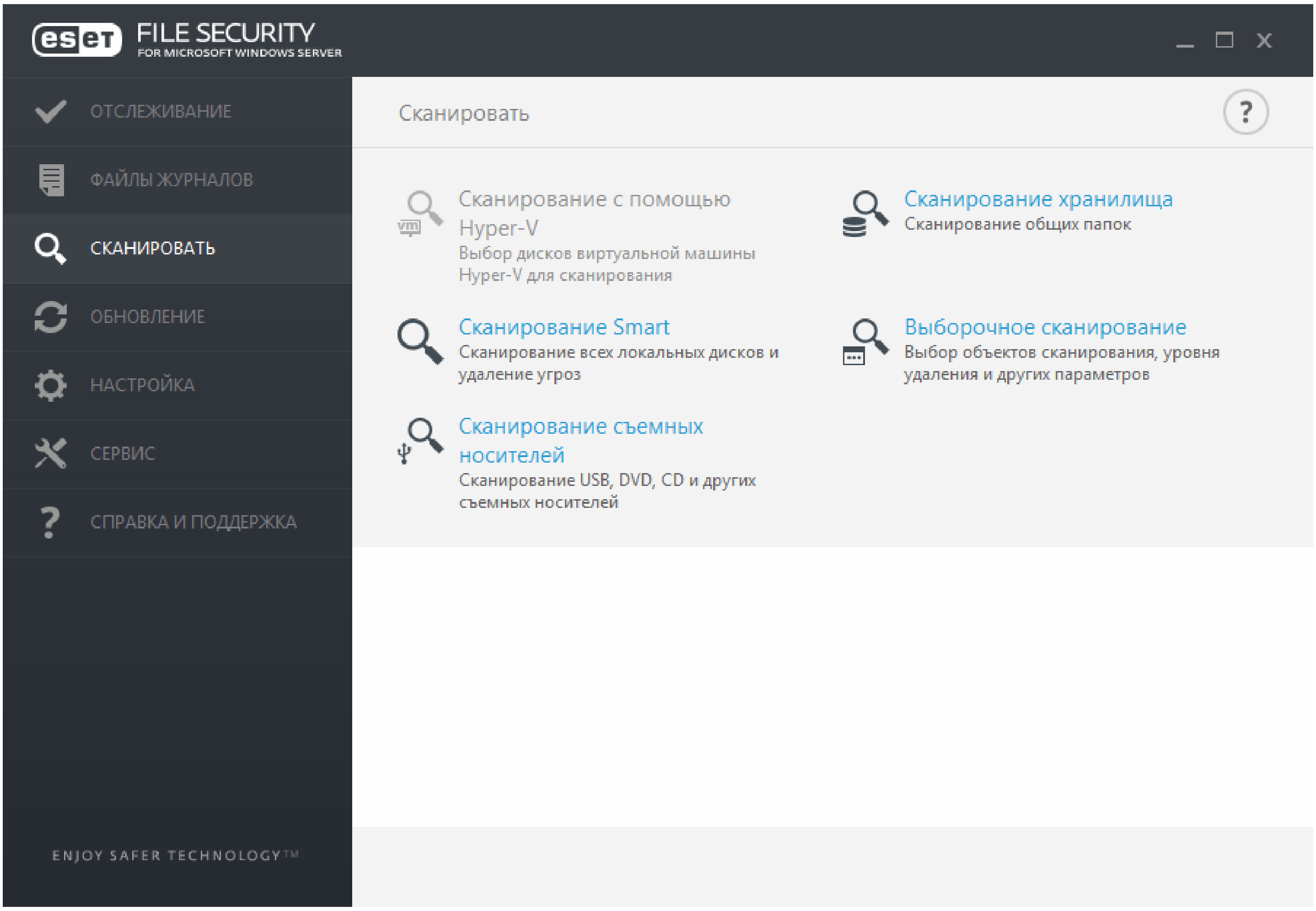
Щелкните переключатель **Фильтрация**, чтобы открыть окно Фильтрация журнала, в котором можно задать критерии фильтрации.

Для просмотра приведенных ниже элементов контекстного меню щелкните правой кнопкой мыши определенную запись.

- **Показать**: просмотр в новом окне более подробной информации о выбранном журнале (как и при двойном щелчке).
- **Фильтрация одинаковых записей**: активация фильтра журнала, который показывает только записи одного выбранного типа.
- **Фильтр...**: при выборе этого параметра в окне Фильтрация журнала будет можно задать критерии фильтрации для определенных записей журнала.
- **Включить фильтр**: активация настроек фильтра. При первой активации фильтрации необходимо задать настройки.
- **Отключить фильтр**: отключение фильтрации (такое же действие, как и при использовании переключателя внизу).
- **Копировать**: копирование выделенных записей в буфер обмена.
- **Копировать все**: копируется информация из всех записей в окне.
- **Удалить**: удаление выбранных записей (для этого необходимы права администратора).
- **Удалить все**: удаление всех записей в окне (для этого необходимы права администратора).
- **Экспорт...**: экспорт информации выбранных записей в XML-файл.
- **Экспорт всего...**: экспорт всей информации в окне в XML-файл.
- **Найти...**: этот параметр открывает окно Поиск в журнале и позволяет определить критерии поиска. С помощью функции поиска можно найти определенную запись даже при включенной фильтрации.
- **Найти далее**: поиск следующего вхождения, соответствующего заданным критериям поиска.
- **Найти ранее**: поиск предыдущих вхождений.
- **Прокрутить журнал**: установите этот флажок, чтобы выполнялась автоматическая прокрутка старых журналов, а на экран в окне **Файлы журнала** выводились активные журналы.

7.3 Сканирование

Модуль сканирования по требованию является важной частью ESET File Security. Он используется для сканирования файлов и папок на компьютере. Для обеспечения безопасности сети принципиально важно выполнять сканирование компьютера регулярно, а не только при возникновении подозрений. Рекомендуется выполнять регулярные (например, раз в месяц) операции тщательного сканирования системы на предмет обнаружения вирусов, которые не были обнаружены при помощи функции защиты файловой системы в реальном времени. Это могло произойти, если в момент появления угрозы защита файловой системы в режиме реального времени была отключена, база данных сигнатур вирусов была устаревшей или же файл не был распознан при первом сохранении на диск.



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

Дополнительные сведения о процессе сканирования см. в главе Ход сканирования.

Сканирование хранилища

Сканирование всех общих папок на локальном сервере. Если элемент **Сканирование хранилища** недоступен, это означает, что на сервере нет общих папок.

Сканирование Hyper-V

Этот параметр отображается в меню, только если диспетчер Hyper-V установлен на том же сервере, на котором выполняется средство ESET File Security. Сканирование Hyper-V позволяет сканировать диски виртуальных машин (ВМ) на сервере Microsoft Hyper-V Server без необходимости установки каких-либо агентов на соответствующие виртуальные машины. Дополнительные сведения (в том числе о поддерживаемых операционных системах и ограничениях) см. в разделе Сканирование Hyper-V.

Сканирование Smart

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

Выборочное сканирование

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

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

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

Сканирование съемных носителей

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

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

Повторить последнее сканирование

Повторение последней операции сканирования с точно такими же настройками.

> **ПРИМЕЧАНИЕ.**
> Рекомендуется сканировать компьютер не реже одного раза в месяц. Сканирование можно настроить как запланированную задачу в меню **Сервис** > **Планировщик**.

7.3.1 Сканирование Hyper-V

Этот тип сканирования позволяет сканировать диски сервера Microsoft Hyper-V Server, то есть виртуальных машин (ВМ), без необходимости установки каких-либо агентов на соответствующих виртуальных машинах. Продукт обеспечения безопасности ESET устанавливается с использованием прав администратора сервера Hyper-V.

Текущая версия функции сканирования Hyper-V поддерживает сканирование активных и неактивных виртуальных систем в Hyper-V. Поддерживаемые типы сканирования для разных основных систем Windows Hyper-V и состояний виртуальной системы показаны ниже.

Виртуальные системы с функцией Hyper-V	Windows Server 2008 R2 Hyper-V	Windows Server 2012 Hyper-V	Windows Server 2012 R2 Hyper-V	Windows Server 2016 Hyper-V
Активная ВМ	нет сканирования	только чтение	только чтение	только чтение
Неактивная ВМ	только чтение/ очистка	только чтение/ очистка	только чтение/ очистка	только чтение/ очистка

Требования к оборудованию

На сервере не должно возникать проблем с производительностью из-за работы виртуальных машин. Сканирование использует в основном ресурсы ЦП.
Для сканирования подключенных к Интернету виртуальных машин требуется наличие свободного места на диске. Объем доступного места на диске должен быть по крайней мере вдвое больше пространства, используемого контрольными точками/моментальными снимками и виртуальными дисками.

Определенные ограничения

- Сканирование хранилищ RAID, составных томов и динамических дисков не поддерживается, так как таков характер динамических дисков. Поэтому динамические диски, если возможно, рекомендуется не использовать в виртуальных машинах.
- Сканируется всегда только текущая виртуальная машина. Сканирование не затрагивает ее контрольные точки и моментальные снимки.
- Сейчас решение ESET File Security не поддерживает работу системы Hyper-V на сервере в кластере.
- Виртуальные машины на узле Hyper-V, находящемся под управлением Windows Server 2008 R2, можно сканировать лишь в режиме только для чтения (**Без очистки**) вне зависимости от того, какой уровень очистки выбран в разделе Параметры ThreatSense.

ПРИМЕЧАНИЕ.
Хотя ESET Security поддерживает сканирование MBR-секторов виртуального диска, из способов сканирования для данных объектов поддерживается лишь сканирование в режиме только для чтения. Этот параметр можно изменить, последовательно щелкнув элементы **Дополнительные настройки** > **Защита от вирусов** > **Сканирование Hyper-V** > Параметры ThreatSense > **Загрузочные секторы**.

Подлежащая сканированию виртуальная машина не подключена к Интернету: **выключенное** состояние

ESET File Security использует управление Hyper-V для обнаружения виртуальных дисков и подключения к ним. Таким образом, программа ESET File Security имеет такой же доступ к содержимому виртуальных дисков, что и к содержимому любого обычного диска.

Подлежащая сканированию виртуальная машина подключена к Интернету: **запущена**, **приостановлена**, **сохранена**

Решение ESET File Security использует управление Hyper-V для обнаружения виртуальных дисков. Подключение к этим дискам невозможно. Поэтому решение ESET File Security создает контрольную точку/ моментальный снимок виртуальной машины, а затем подключается к ней. После сканирования контрольная точка или моментальный снимок удаляется. Это означает, что сканирование в режиме только для чтения возможно, потому что на запущенные виртуальные машины сканирование не влияет.

Выделите продукту ESET Security до одной минуты на создание моментального снимка или контрольной точки в ходе сканирования. Примите это к сведению при выполнении сканирования Hyper-V на большом количестве виртуальных машин.

Принципы именования

Модуль сканирования Hyper-V использует следующее соглашение об именовании:
`Имя_виртуальной_машины\DiskX\VolumeY`

где X — это номер диска, а Y — номер тома.
Например, `Computer\Disk0\Volume1`.

Числовой суффикс соответствует порядку обнаружения, который идентичен порядку, отображаемому в диспетчере дисков виртуальной машины.
Такой принцип именования используется в древовидном списке объектов, подлежащих сканированию, а также в индикаторе выполнения и файлах журналов.

Выполнение сканирования

Существует три варианта сканирования.

- По требованию: щелкните **Сканирование Hyper-V** для просмотра списка виртуальных машин и томов, доступных для сканирования.
- Выберите виртуальные машины, диски или тома, которые нужно просканировать, и нажмите кнопку **Сканировать**.
- С помощью планировщика.
- С помощью ESET Remote Administrator в качестве клиентской задачи под названием Сканирование сервера.

Кроме того, можно запустить несколько процессов сканирования Hyper-V одновременно.

После завершения сканирования вы получите уведомление со ссылкой на файлы журнала.

Возможные проблемы

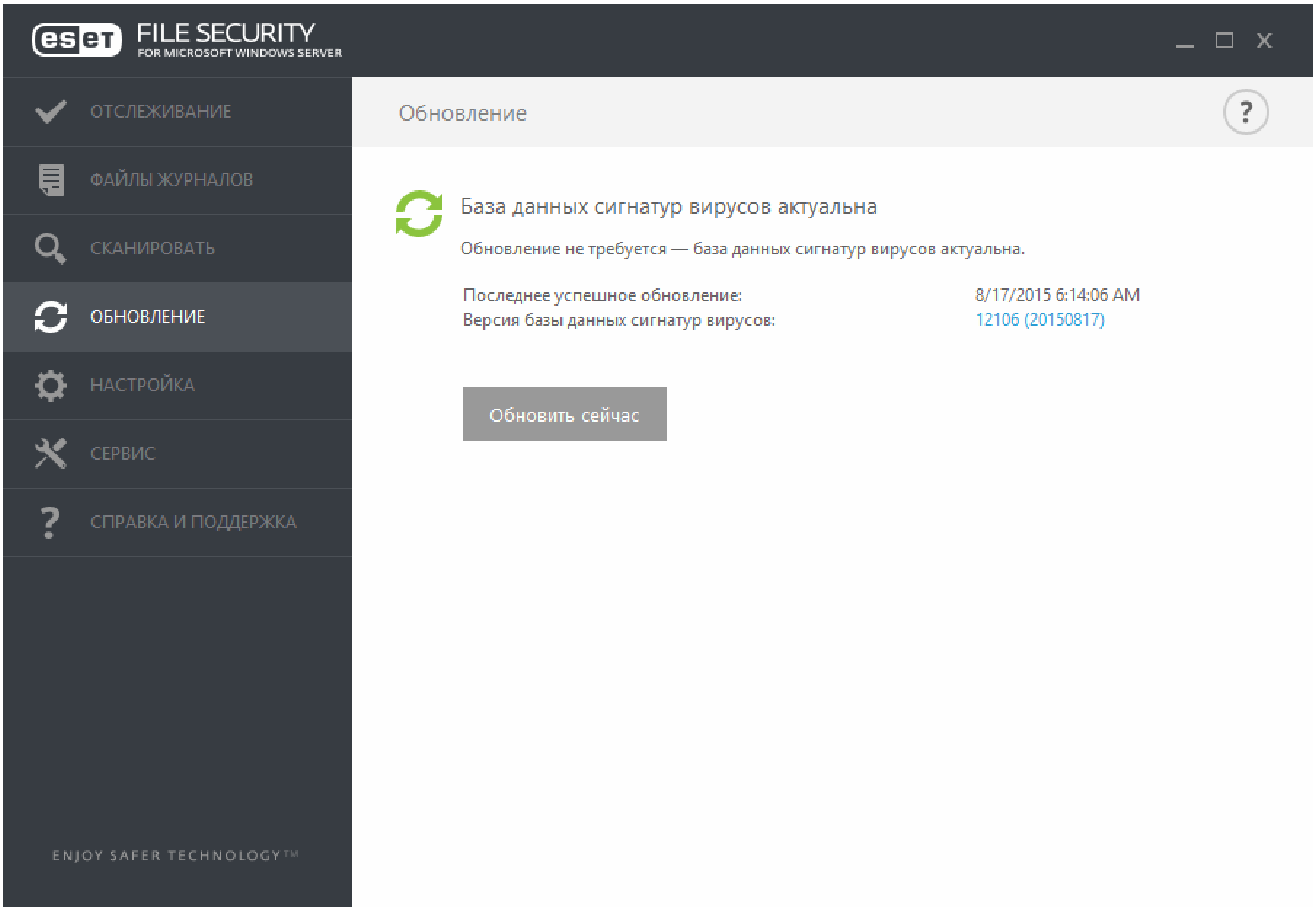
- В случае сканирования виртуальной машины, подключенной к Интернету, необходимо создать контрольную точку/моментальный снимок соответствующей виртуальной машины. При этом в процессе создания точки или снимка некоторые основные действия виртуальной машины могут быть ограничены или отключены.
- В случае сканирования виртуальной машины, не подключенной к Интернету, вы не сможете включить ее до завершения сканирования.
- Диспетчер Hyper-V позволяет присвоить двум разным виртуальным машинам одинаковые имена, и это может стать проблемой, когда, просматривая журналы сканирования, вы пытаетесь различить компьютеры.

7.4 Обновление

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

Выберите пункт «Обновить» в главном меню программы, чтобы просмотреть информацию о текущем состоянии обновления системы, в том числе дату и время последнего успешно выполненного обновления. Также в основном окне указывается версия базы данных сигнатур вирусов. Номер версии обновления представляет собой активную ссылку на сведения о сигнатурах, добавленных в заданном обновлении.

Чтобы проверить наличие обновлений, щелкните **Обновить сейчас**. Обновление базы данных сигнатур вирусов и компонентов программы является важнейшей частью обеспечения полной защиты компьютера от вредоносного кода.



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

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

Процесс обновления

После нажатия кнопки **Обновить сейчас** начнется процесс загрузки, а также отобразится ход обновления. Чтобы прервать обновление, нажмите кнопку **Отменить обновление**.

ВАЖНО!

Если загрузка завершилась нормально, то 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. В противном случае на экран будет выведено одно из следующих сообщений.

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

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

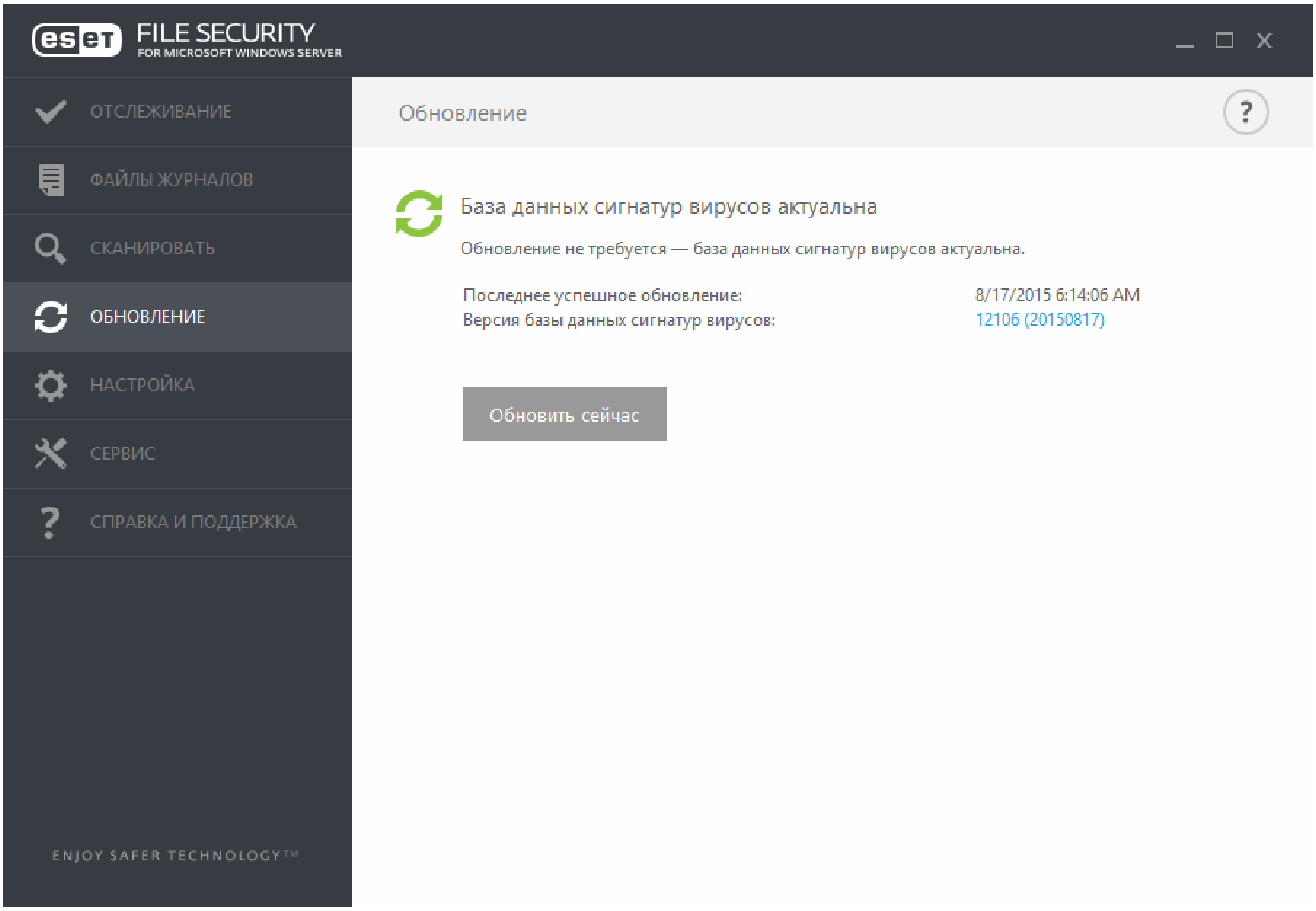
Недействительная лицензия: в разделе параметров обновления введен неправильный лицензионный ключ. Рекомендуется проверить данные аутентификации. В окне **Дополнительные настройки** (нажмите F5 на клавиатуре) содержатся расширенные параметры обновления. В главном меню последовательно щелкните элементы **Справка и поддержка** > **Управление лицензией** и введите новый лицензионный ключ.

При загрузке файлов обновлений произошла ошибка: возможная причина этой ошибки — 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 поставщику услуг Интернета, чтобы выяснить, имеется ли активное подключение к Интернету.

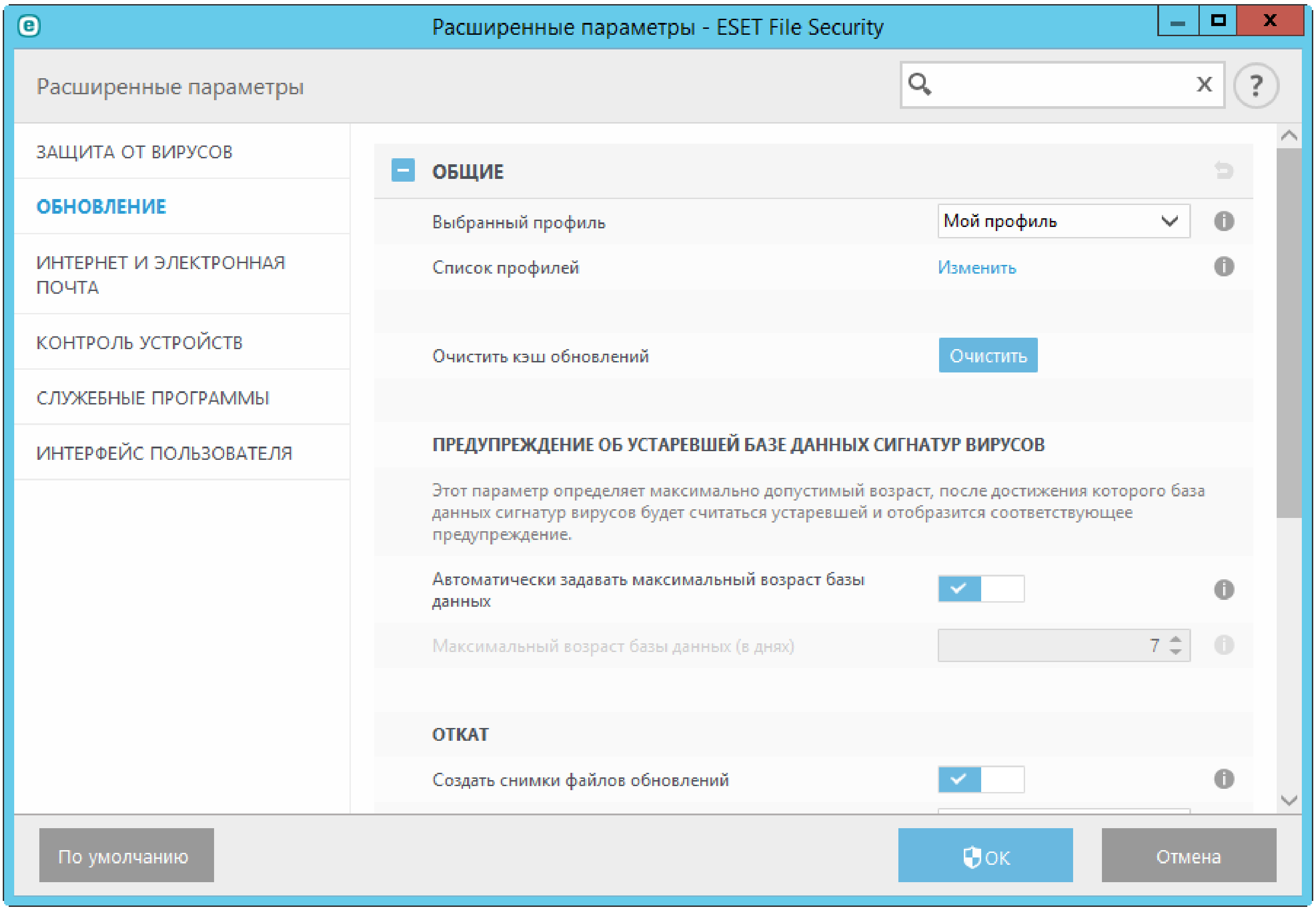
ПРИМЕЧАНИЕ.
Дополнительные сведения можно найти в этой статье базы знаний.

7.4.1 Настройка обновления базы данных вирусов

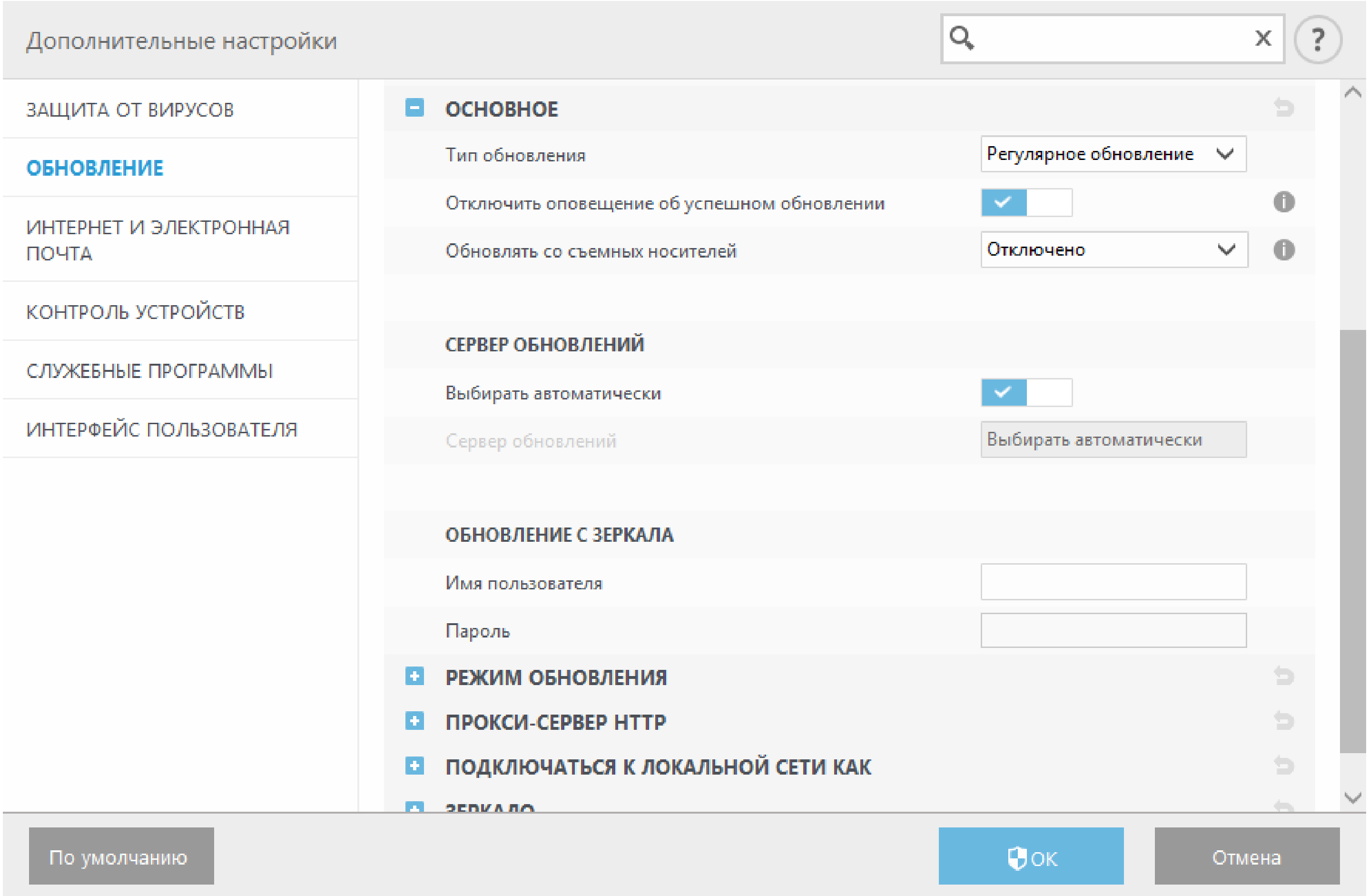
Обновление базы данных сигнатур вирусов и компонентов программы является важнейшей частью обеспечения полной защиты компьютера от злонамеренного кода. Уделите особенное внимание изучению конфигурации и работы этого процесса. В главном меню выберите пункт **Обновление**, после чего щелкните элемент **Обновить**,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



Настроить параметры обновления можно в окне **Дополнительные настройки** (нажмите клавишу F5 на клавиатуре). Для настройки расширенных параметров обновления, таких как режим обновления, доступ через прокси-сервер, подключение к локальной сети и создание копий сигнатур вирусов (зеркал), нажмите **Обновление** > **Профили**. При возникновении проблем с обновлением нажмите кнопку **Очистить**, чтобы удалить из кэша временные файлы обновления.



По умолчанию в меню **Сервер обновлений** задан параметр **Выбирать автоматически**. Параметр **Выбирать автоматически** означает, что сервер, с которого загружаются обновления сигнатур вирусов, выбирается автоматически. Рекомендуется оставить параметры по умолчанию. Чтобы отключить отображение уведомлений на панели задач в правом нижнем углу экрана, выберите элемент **Отключить уведомления о завершении обновления**.



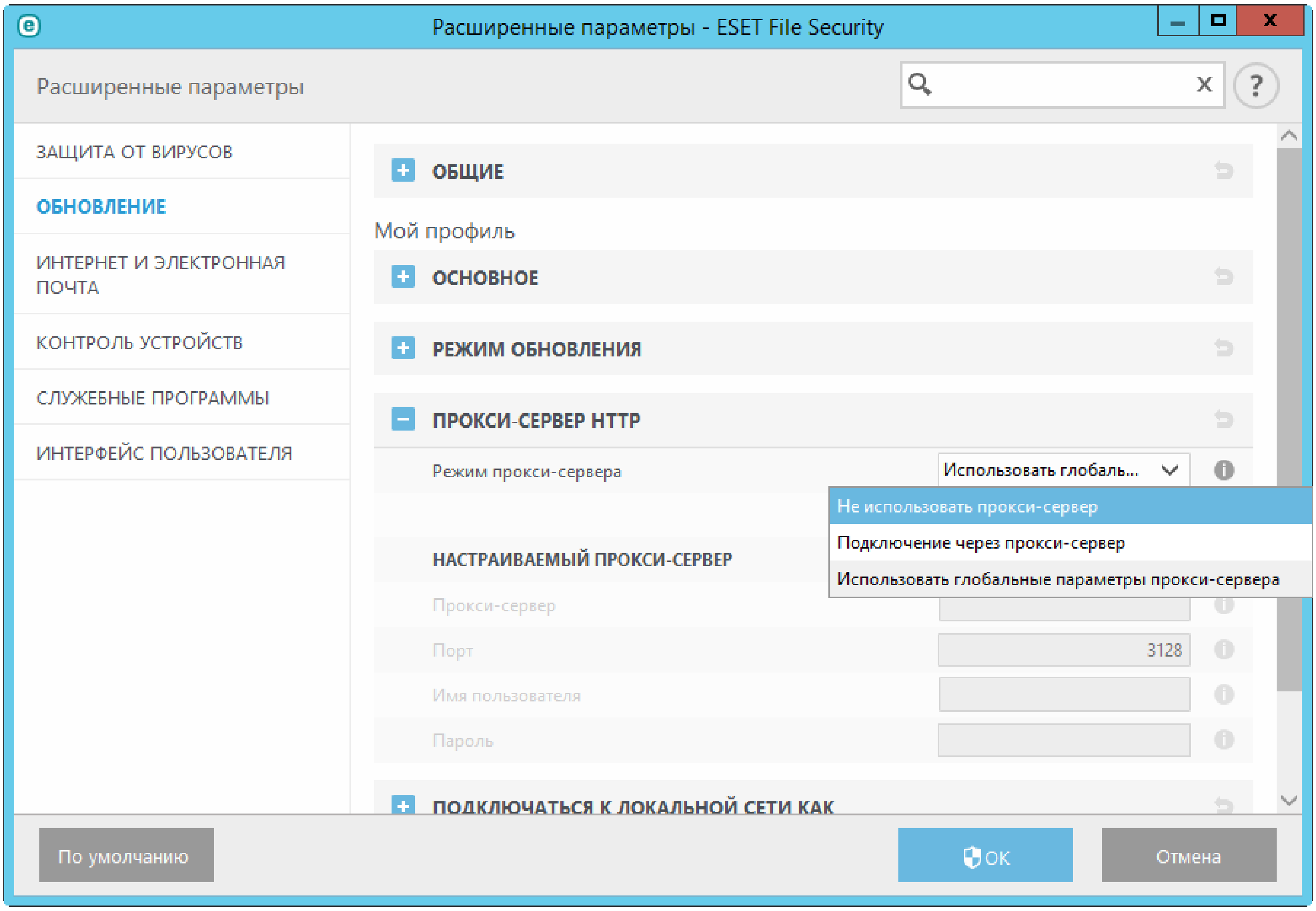
Чтобы использовать программу наилучшим образом, необходимо включить ее автоматическое обновление. Это возможно только в случае, если в разделе **Справка и поддержка** > **Активировать лицензию** введен правильный **Лицензионный ключ**.

Вы можете активировать продукт сразу после установки или в любое другое время. Дополнительные сведения об активации см. в статье Активация ESET File Security. Информацию о лицензии, полученную вместе с программой ESET, необходимо ввести в окне «Сведения о лицензии».

7.4.2 Настройка обновлений на прокси-сервере

Если прокси-сервер используется для подключения к Интернету в системе, в которой установлено приложение ESET File Security, параметры прокси-сервера нужно настроить в разделе **Дополнительные настройки**. Для доступа к окну настройки прокси-сервера нажмите клавишу F5, чтобы открыть окно **Дополнительные настройки**, и выберите пункты **Обновление** > **Профили** > **Прокси-сервер HTTP**.

В раскрывающемся меню **Режим прокси-сервера** выберите элемент **Подключение через прокси-сервер** и введите данные прокси-сервера: **прокси-сервер** (IP-адрес), **номер** порта и **имя пользователя** и **пароль** (если применимо).



Если вы забыли данные прокси-сервера, можно выбрать в раскрывающемся меню пункт **Использовать глобальные параметры прокси-сервера**, чтобы автоматически обнаружить параметры прокси-сервера.

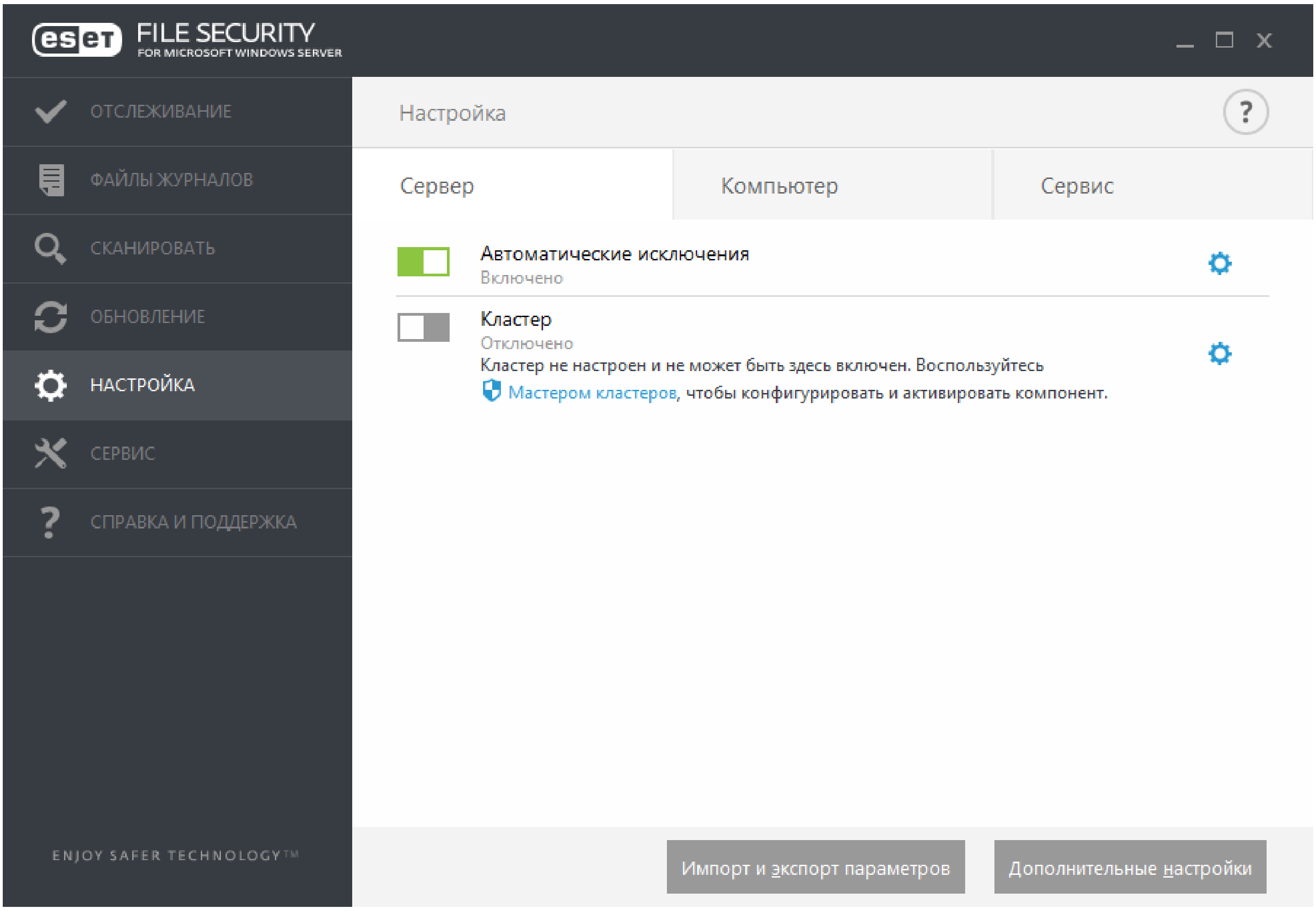
ПРИМЕЧАНИЕ.
Параметры прокси-сервера для различных профилей обновления могут различаться. В этом случае следует сконфигурировать разные профили обновлений в разделе **Дополнительные настройки** нажатием кнопки **Обновление** > **Профиль**.

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.

7.5 Настройка

Меню **Настройка** содержит следующие разделы.

- Сервер
- Компьютер
- Сервис



Чтобы временно отключить тот или иной модуль, щелкните зеленый переключатель возле нужного модуля. Обратите внимание, что это может привести к ослаблению защиты вашего компьютера.
Чтобы возобновить защиту отключенного компонента безопасности, щелкните красный переключатель , и компонент снова будет включен.
Чтобы открыть дополнительные настройки конкретного компонента безопасности, щелкните значок шестеренки .

Чтобы получить доступ к дополнительным настройкам компонентов, щелкните элемент **Дополнительные настройки** или нажмите клавишу **F5**.

В нижней части окна настройки есть дополнительные параметры. Чтобы загрузить параметры настройки из файла конфигурации в формате *XML* или сохранить текущие параметры настройки в файл конфигурации, воспользуйтесь функцией **Импорт и экспорт параметров**. Для получения дополнительных сведений см. раздел Импорт и экспорт параметров.

7.5.1 Сервер

Отобразится список компонентов, которые можно включить или отключить с помощью переключателя . Чтобы выполнить настройку отдельного элемента, щелкните значок шестеренки .

- Автоматические исключения. Эта функция выявляет критически важные файлы серверных приложений и серверной операционной системы и автоматически добавляет их в список Исключения. Эта функция позволяет свести к минимуму риск возможных конфликтов и улучшить общую производительность сервера при работе антивирусного ПО.
- Чтобы настроить кластер ESET, щелкните пункт **Мастер кластеров**. Сведения о настройке кластера ESET с помощью этого мастера см. здесь.

Чтобы получить доступ к более подробным настройкам, щелкните элемент **Дополнительные настройки** или нажмите клавишу **F5**.

В нижней части окна настройки есть дополнительные параметры. Чтобы загрузить параметры настройки из файла конфигурации в формате *XML* или сохранить текущие параметры настройки в файл конфигурации, воспользуйтесь функцией **Импорт и экспорт параметров**. Для получения дополнительных сведений см. раздел Импорт и экспорт параметров.

7.5.2 Компьютер

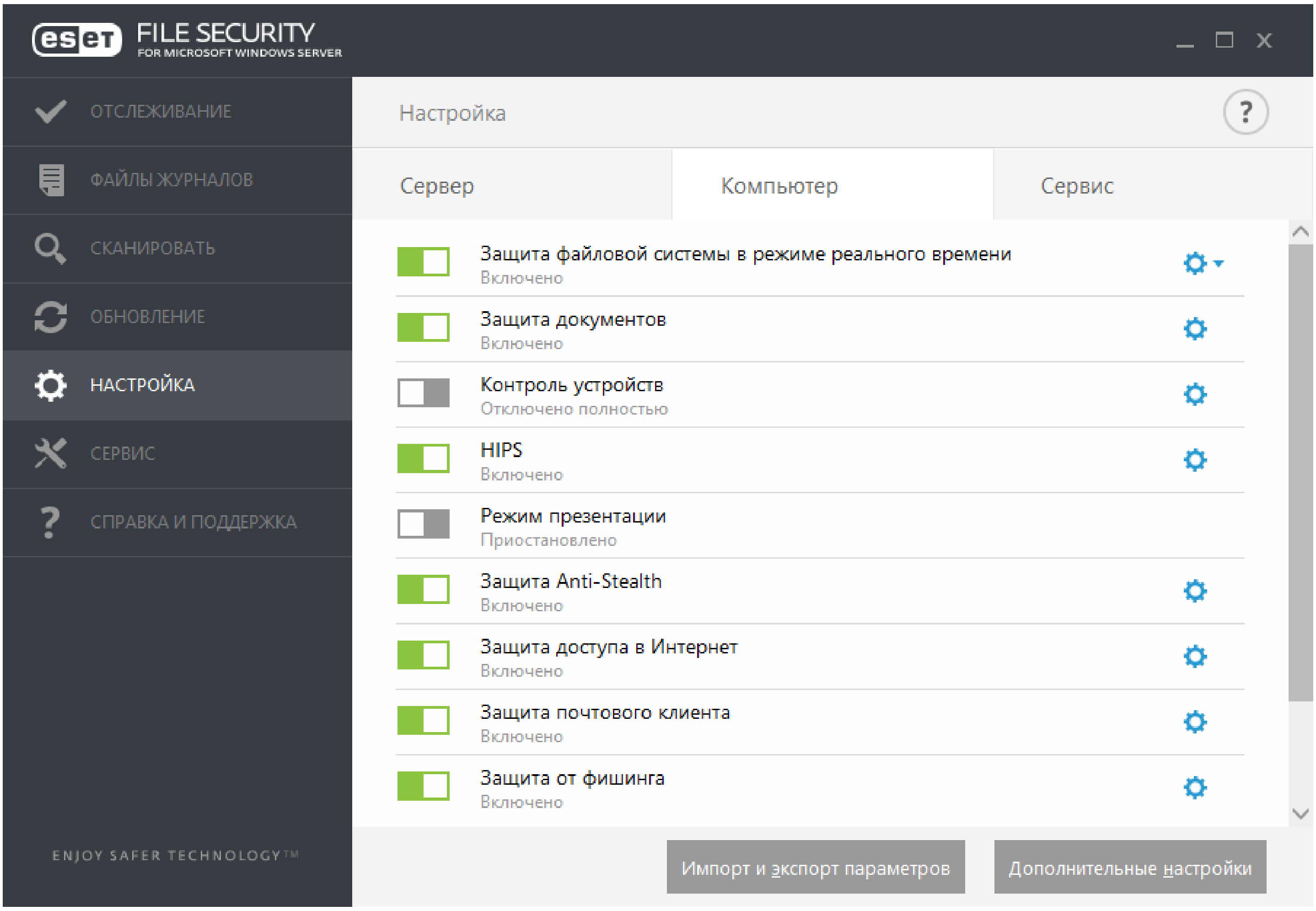
ESET File Security располагает всеми необходимыми компонентами, чтобы обеспечить надежную защиту сервера как компьютера. Каждый компонент отвечает за отдельный тип защиты, например: защита от вирусов и шпионских программ, защита файловой системы в режиме реального времени, защита доступа в Интернет, защита почтового клиента и защита от фишинга и т. д.

Доступ к разделу **Компьютер** можно получить, последовательно выбрав элементы **Настройка** > **Компьютер**. Отобразится список компонентов, которые можно включить или отключить с помощью переключателя . Чтобы выполнить настройку отдельного элемента, щелкните значок шестеренки .

Для **защиты в режиме реального времени** также предусмотрен параметр **Изменить исключения**, при выборе которого открывается окно настройки Исключения, в котором можно исключить файлы и папки из сканирования.

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

В модуле **Компьютер** можно включать, отключать и настраивать следующие компоненты.



- **Защита файловой системы в реальном времени**: при открытии, создании или исполнении файлов они сканируются на наличие вредоносного кода.
- **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.

ПРИМЕЧАНИЕ.
Защита документов отключена по умолчанию. Если необходимо, ее можно включить, щелкнув значок переключателя.

- **Контроль устройств** — 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.
- **HIPS** — система предотвращения вторжений на узел (HIPS) отслеживает события, происходящие в операционной системе, и реагирует на них в соответствии с настраиваемым набором правил.
- **Режим презентации** — функция для пользователей, которым необходимо отсутствие каких-либо перерывов при использовании программного обеспечения и отвлекающих внимание всплывающих окон, а также требуется свести к минимуму потребление ресурсов процессора. После включения режима презентации на экран будет выведено предупреждение (о потенциальной угрозе безопасности), а для оформления главного окна будет применен оранжевый цвет.
- **Защита Anti-Stealth** — обеспечивает обнаружение опасных программ, например руткитов, способных скрывать свое присутствие от операционной системы. Это значит, что такие программы невозможно обнаружить с помощью обычных методов проверки.
- **Защита доступа в Интернет**: если этот параметр включен, весь трафик по протоколам HTTP и HTTPS сканируется на наличие вредоносных программ.
- **Защита клиента электронной почты** — обеспечивает контроль обмена данными по протоколам POP3 и IMAP.

- **Защита от фишинга**: защита от попыток незаконных веб-сайтов, выдающих себя за законные, получить пароли, банковские данные и прочую конфиденциальную информацию.

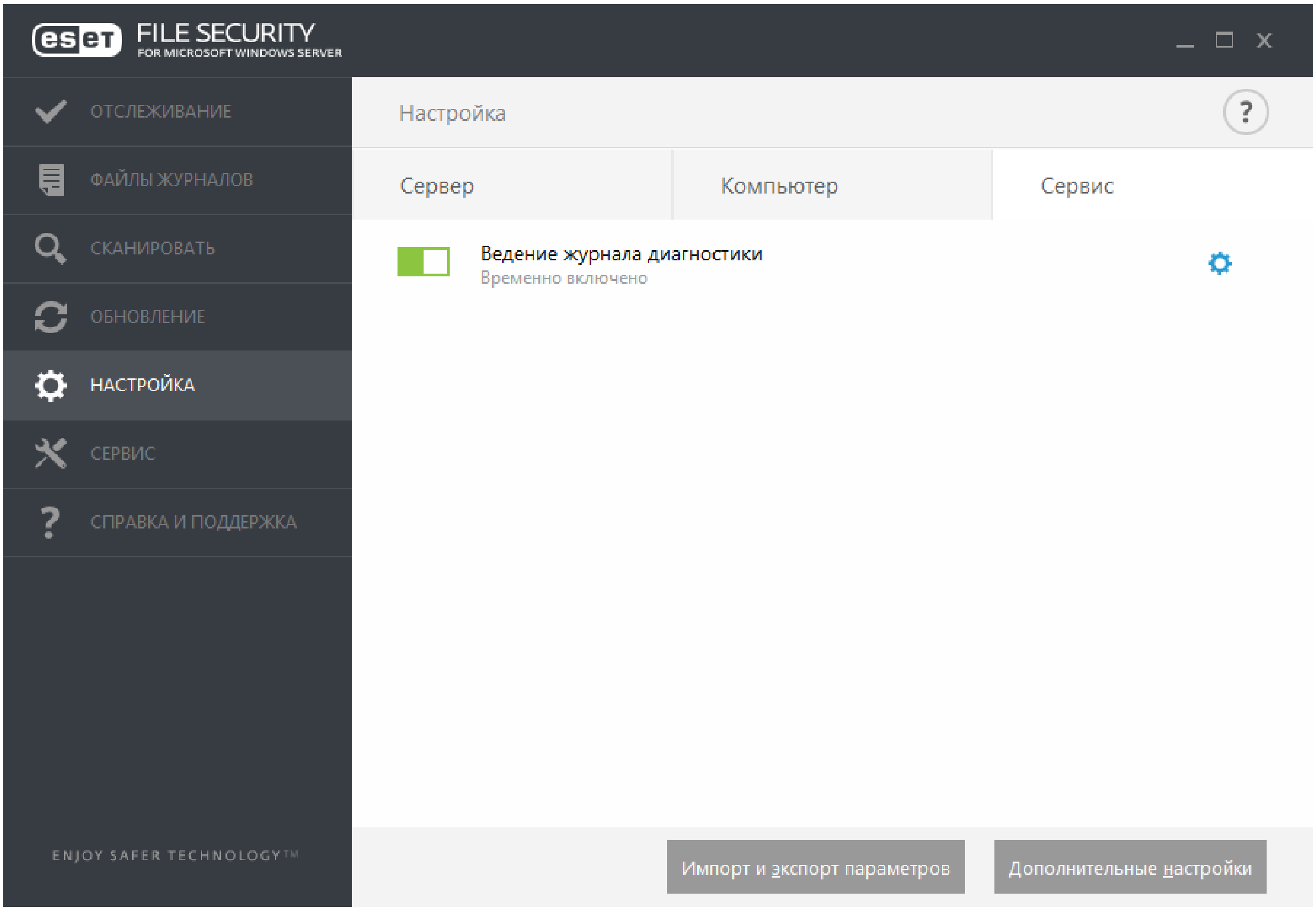
В нижней части окна настройки есть дополнительные параметры. Чтобы загрузить параметры настройки из файла конфигурации в формате *XML* или сохранить текущие параметры настройки в файл конфигурации, воспользуйтесь функцией **Импорт и экспорт параметров**. Для получения дополнительных сведений см. раздел Импорт и экспорт параметров.

Чтобы получить доступ к более подробным настройкам, щелкните элемент **Дополнительные настройки** или нажмите клавишу **F5**.

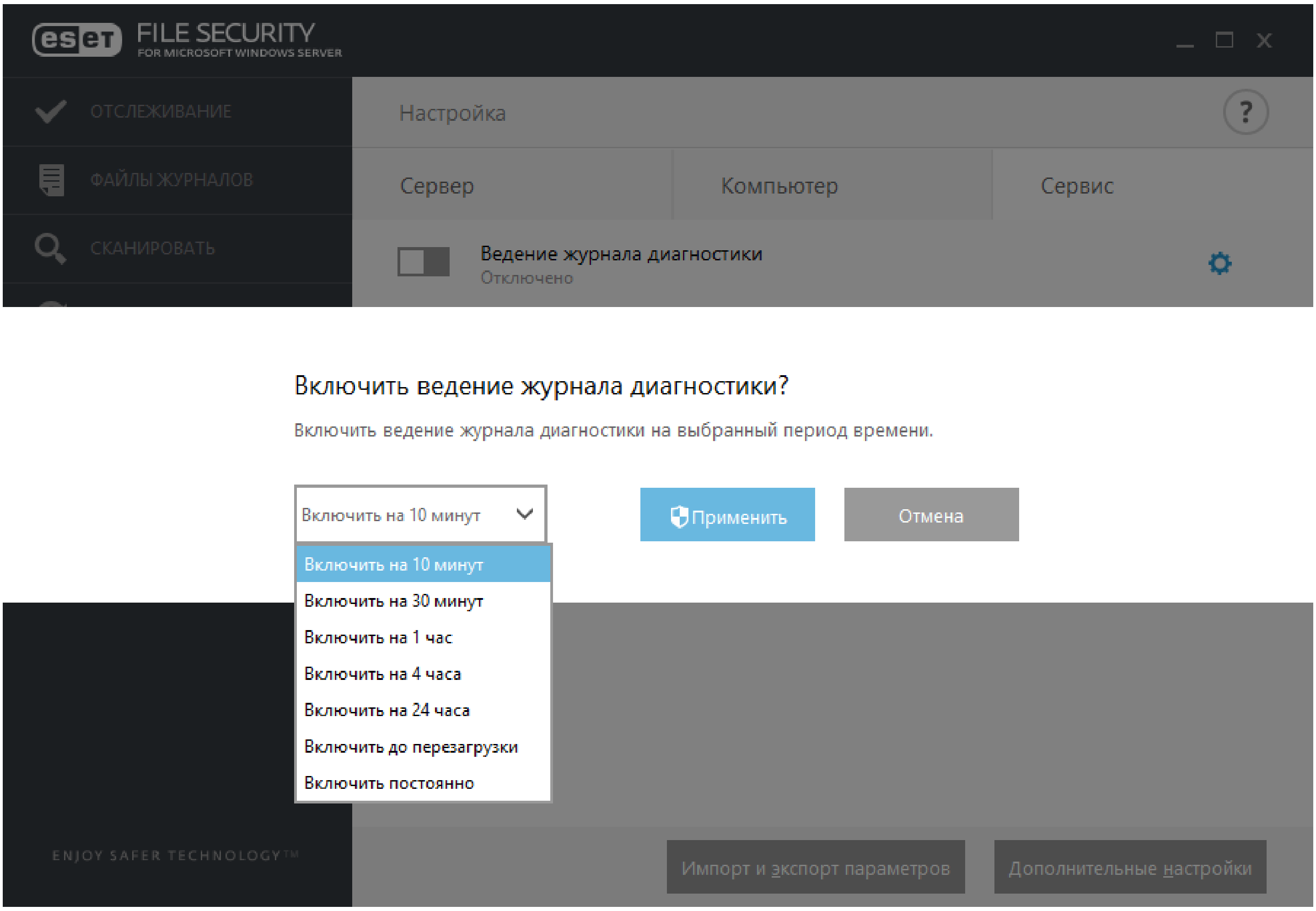
7.5.3 Сервис

Ведение журнала диагностики: если щелкнуть переключатель, чтобы включить ведение журнала диагностики, можно выбрать период, на протяжении которого эта функция должна оставаться включенной (10 минут, 30 минут, 1 час, 4 часа, 24 часа, до следующей перезагрузки сервера или постоянно).

Если щелкнуть значок шестеренки ( ), откроется окно **Дополнительные настройки**, в котором можно указать, какие компоненты будут делать записи в журналах диагностики, когда ведение журналов диагностики включено.



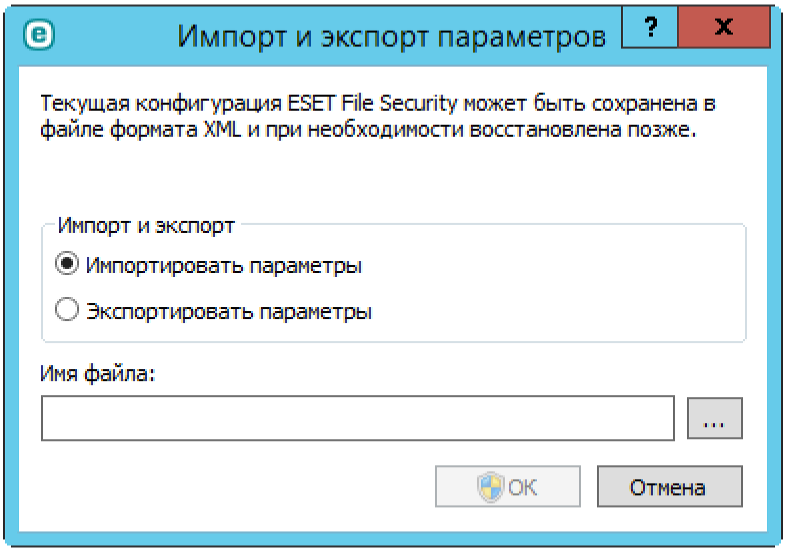
* **Включить** ведение журнала диагностики на выбранный период времени.



7.5.4 Импорт и экспорт параметров

Нажмите **Настройки** > **Импорт и экспорт параметров** для доступа к параметрам импорта и экспорта ESET File Security.

И для импорта, и для экспорта используются файлы в формате *XML*. Функции импорта и экспорта полезны, если нужно сделать резервную копию текущей конфигурации программы ESET File Security. С помощью этой резервной копии можно впоследствии применить те же параметры на других компьютерах.



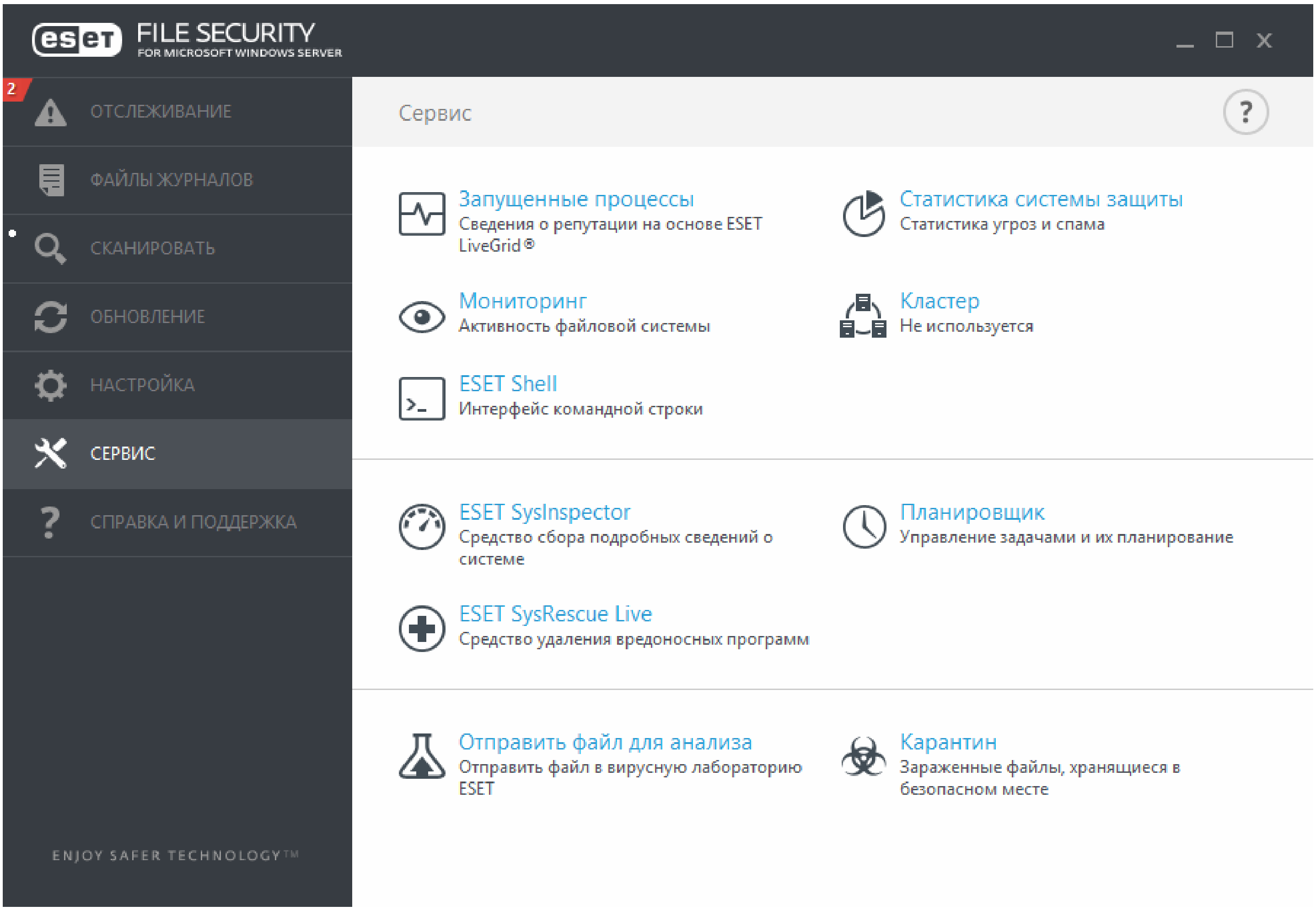
ПРИМЕЧАНИЕ.

При экспорте параметров может возникнуть ошибка, если у вас нет права для записи экспортируемого файла в указанный каталог.

7.6 Сервис

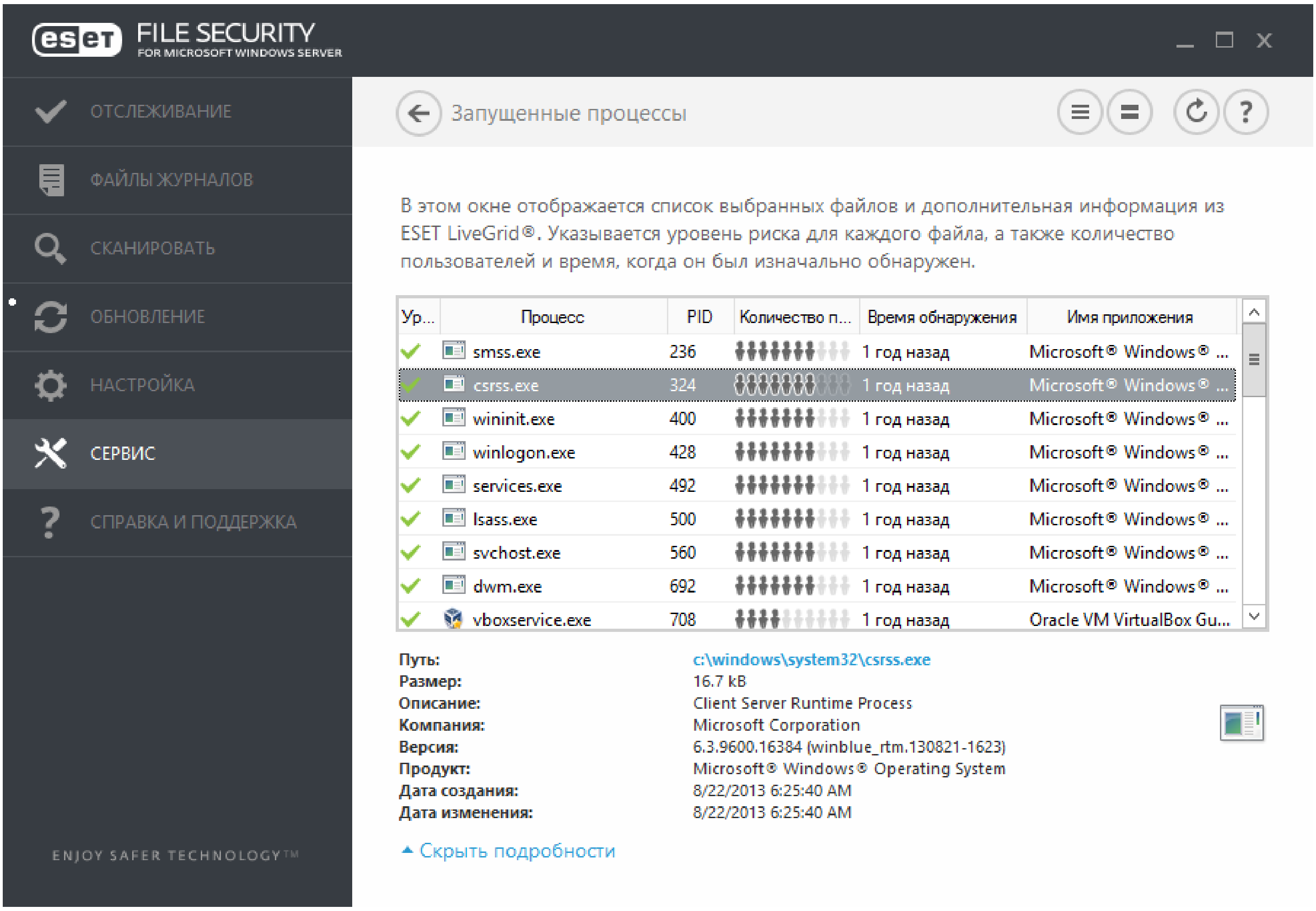
В меню «Сервис» доступны модули, которые позволяют упростить процесс администрирования программы и содержат дополнительные возможности. В этом меню представлены следующие служебные программы.

- Запущенные процессы
- Мониторинг
- Статистика системы защиты
- Кластер
- Оболочка ESET
- ESET SysInspector
- ESET SysRescue Live
- Планировщик
- Отправка образца на анализ
- Карантин



7.6.1 Запущенные процессы

В разделе «Запущенные процессы» отображаются выполняемые на компьютере программы или процессы. Кроме того, эта функция позволяет оперативно и непрерывно уведомлять компанию ESET о новых заражениях. ESET File Security предоставляет подробные сведения о запущенных процессах для защиты пользователей с помощью технологии [ESET LiveGrid](#).



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

Процесс: имя образа программы или процесса, запущенных в настоящий момент на компьютере. Для просмотра всех запущенных на компьютере процессов можно использовать также диспетчер задач Windows. Чтобы открыть диспетчер задач, щелкните правой кнопкой мыши в пустой области на панели задач и выберите пункт «Диспетчер задач» или одновременно нажмите клавиши **Ctrl+Shift+Esc** на клавиатуре.

Идентификатор процесса: идентификатор процессов, запущенных в операционных системах Windows.

ПРИМЕЧАНИЕ.

Известные приложения, помеченные как Безопасно (зеленый), точно являются безопасными (внесены в «белый» список) и исключаются из сканирования, благодаря чему увеличивается скорость сканирования компьютера по запросу и улучшается защита файловой системы в режиме реального времени.

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

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

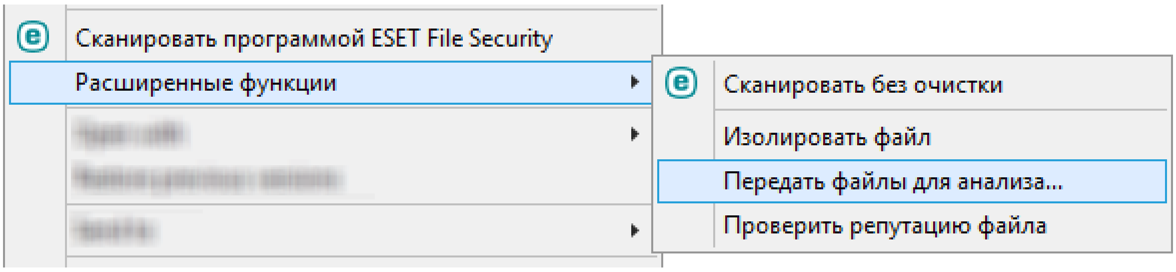
ПРИМЕЧАНИЕ.
Если для приложения выбран уровень безопасности Неизвестно (оранжевый), оно не обязательно является вредоносной программой. Обычно это просто новое приложение. Если вы не уверены в безопасности файла, воспользуйтесь функцией отправки файла на анализ, чтобы отправить файл в вирусную лабораторию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

Имя приложения: имя программы, которой принадлежит этот процесс.

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

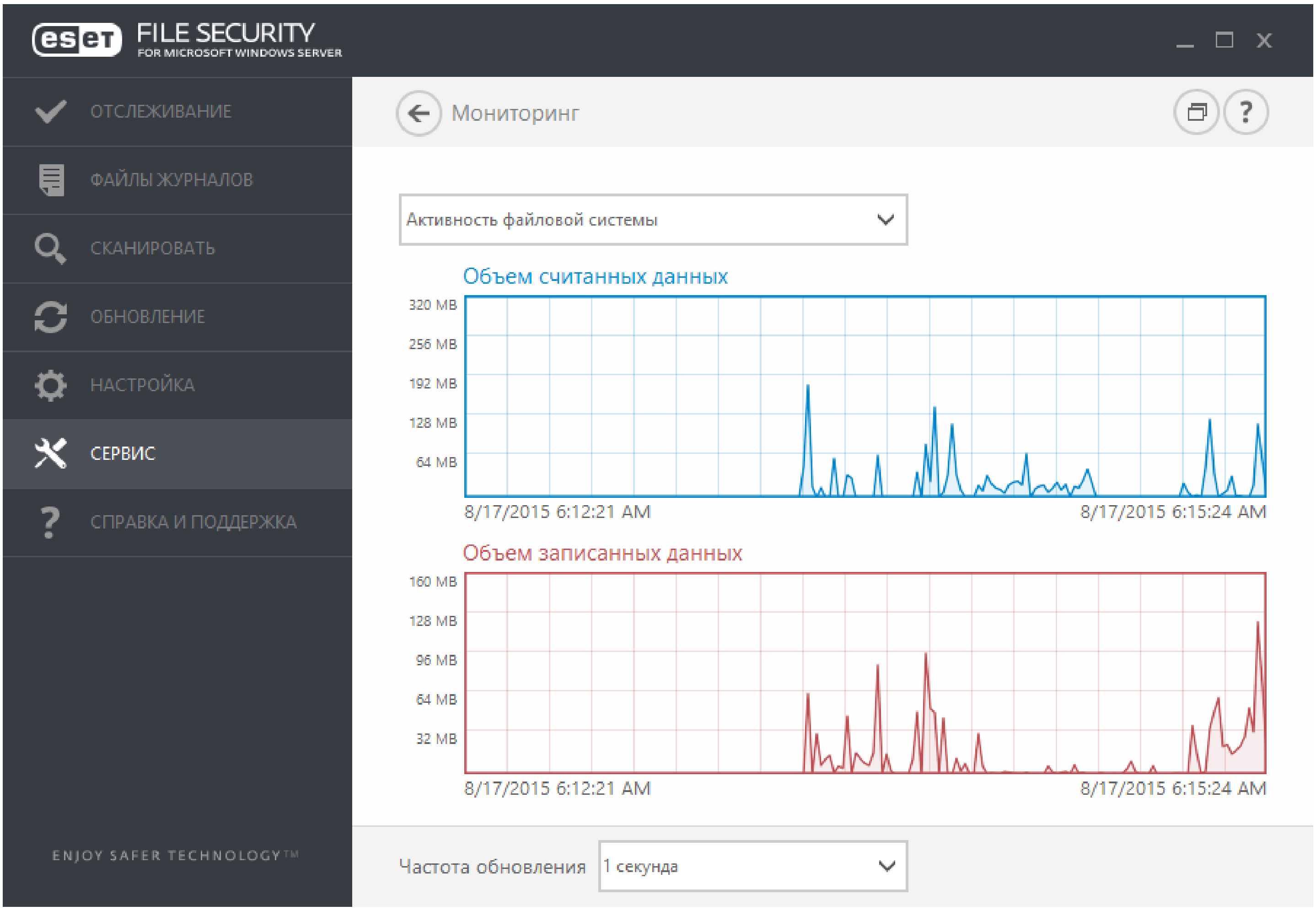
- **Путь**: расположение приложения на компьютере.
- **Размер**: размер файла в КБ (килобайтах) или МБ (мегабайтах).
- **Описание**: характеристики файла на основе его описания в операционной системе.
- **Компания**: название поставщика или процесса приложения.
- **Версия**: информация от издателя приложения.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

ПРИМЕЧАНИЕ.
Кроме того, можно проверить репутацию файлов, которые не являются запущенными программами или процессами. Для этого отметьте нужные файлы, щелкните их правой кнопкой мыши и выберите элементы **Расширенные параметры** > **Проверить репутацию файла с помощью ESET LiveGrid**.



7.6.2 Мониторинг

Чтобы отобразить текущую **активность файловой системы** в форме графика, щелкните **Сервис** > **Мониторинг**. В нижней части диаграммы находится временная шкала, на которой отображается активность файловой системы в реальном времени за выбранный временной интервал. Чтобы изменить частоту обновлений, воспользуйтесь раскрывающимся меню **Частота обновления**.



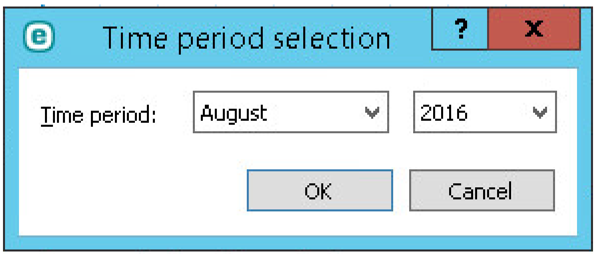
Доступны указанные ниже варианты.

- **1 секунда**: график обновляется каждую секунду, временная шкала охватывает последние 10 минут.
- **1 минута (последние 24 часа)**: график обновляется каждую минуту, временная шкала охватывает последние 24 часа.
- **1 час (последний месяц)**: график обновляется каждый час, временная шкала охватывает последний месяц.
- **1 час (выбранный месяц)**: график обновляется каждый час, временная шкала охватывает выбранный месяц. Чтобы выбрать другой месяц, нажмите кнопку **Изменить месяц**.

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

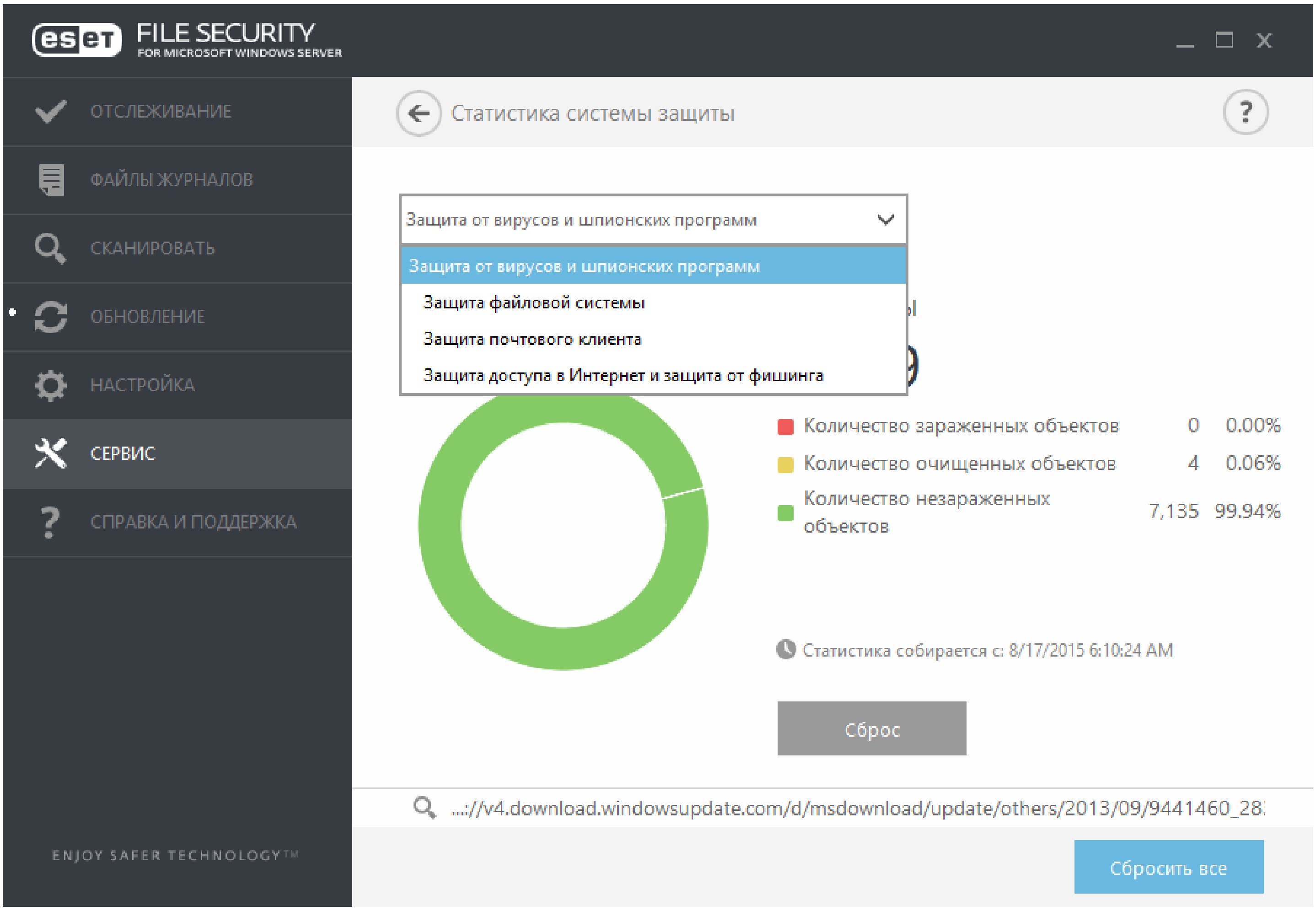
7.6.2.1 Выбор периода времени

Выберите месяц (и год), за который на графике нужно отобразить **активность файловой системы** на графике.



7.6.3 Статистика системы защиты

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



Доступны следующие статистические диаграммы.

- **Защита от вирусов и шпионских программ**: отображение общего количества зараженных и очищенных объектов.
- **Защита файловой системы**: отображение только тех объектов, которые считываются из файловой системы или записываются в нее.
- **Защита клиента электронной почты**: отображение только объектов, отправленных или полученных почтовыми клиентами.
- **Защита доступа в Интернет и защита от фишинга**: отображение только объектов, загруженных веб-браузерами.

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

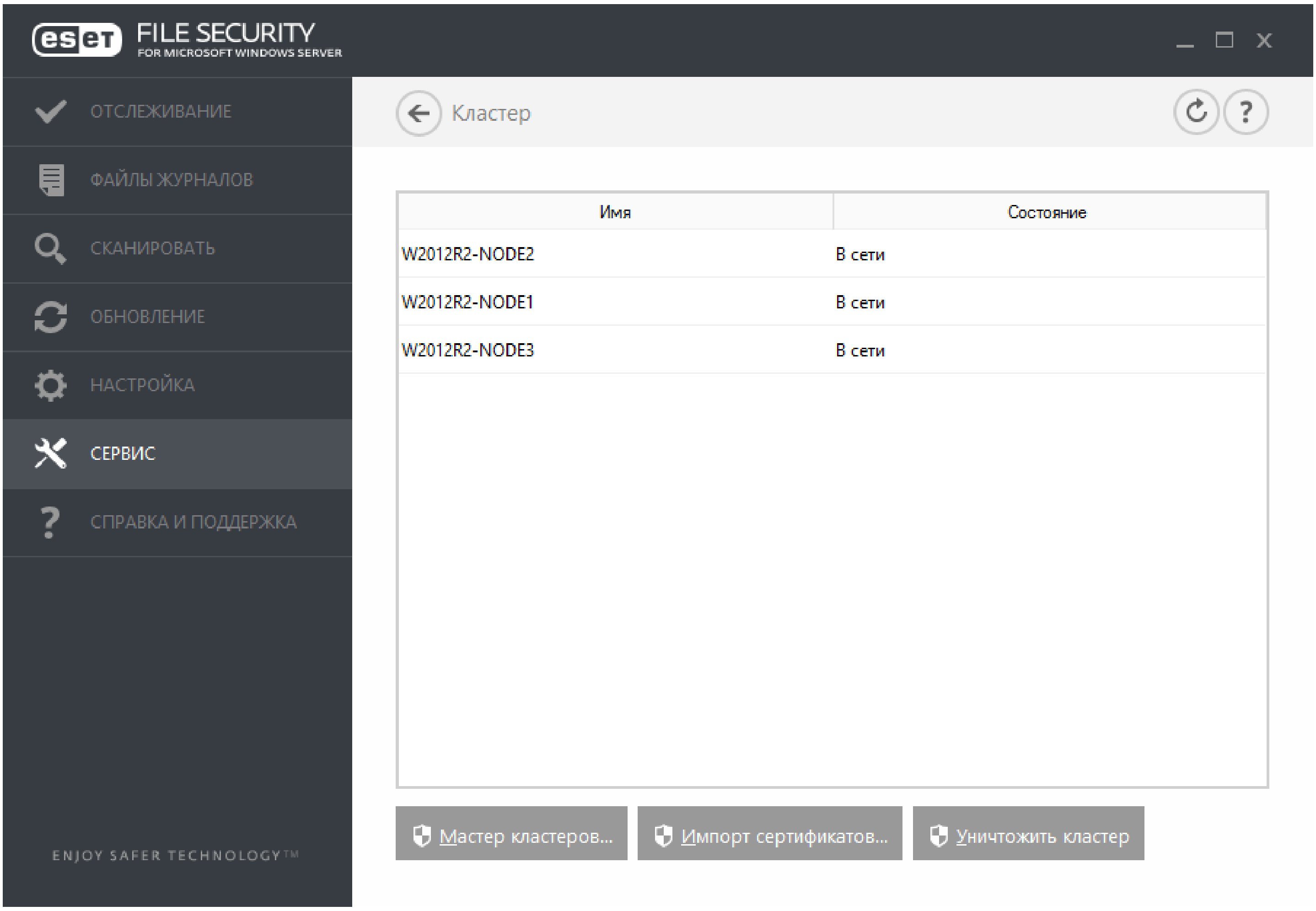
7.6.4 Кластер

Кластер ESET — это одноранговая (P2P) инфраструктура взаимодействия линейки продуктов ESET для Microsoft Windows Server.

Эта инфраструктура позволяет серверным продуктам ESET взаимодействовать друг с другом и обмениваться данными, например сведениями о конфигурации и оповещениями а также синхронизировать данные, необходимые для правильной работы группы экземпляров продуктов. Примером такой группы является группа узлов в отказоустойчивом кластере Windows или кластере балансировки сетевой нагрузки (NLB) с продуктом ESET, установленным там, где необходима одинаковая конфигурация продукта во всем кластере. Кластер ESET обеспечивает однообразие конфигурации в нескольких экземплярах.

ПРИМЕЧАНИЕ.
Настройки интерфейса разных узлов кластера ESET не синхронизируются.

К странице состояния кластера ESET можно получить доступ из главного меню, последовательно щелкнув элементы **Сервис** > **Кластер**. При правильной настройке страница состояния должна выглядеть следующим образом.



Чтобы настроить кластер ESET, щелкните пункт **Мастер кластеров**. Сведения о настройке кластера ESET с помощью этого мастера см. здесь.

Есть два способа добавления узлов при настройке кластера ESET: автоматически, с помощью существующего отказоустойчивого кластера Windows (или кластера NLB), или вручную, путем поиска компьютеров, относящихся к рабочей группе или домену.

Автообнаружение — автоматическое обнаружение узлов, уже входящих в отказоустойчивый кластер Windows или кластер NLB, и добавление их в кластер ESET.
Обзор — узлы можно добавить вручную. Для этого нужно ввести имена серверов (участников одной рабочей группы или одного домена).

> **ПРИМЕЧАНИЕ.**
> Чтобы использовать кластер ESET, серверы не должны являться участниками отказоустойчивого кластера Windows или кластера NLB. Чтобы можно было использовать кластеры ESET, наличие отказоустойчивого кластера Windows или кластера NLB в среде не требуется.

После добавления узлов в кластер ESET необходимо выполнить установку ESET File Security на каждом их них. Это выполняется автоматически в процессе настройки кластера ESET.

Учетные данные, необходимые для удаленной установки программы ESET File Security на других узлах кластера:
- **сценарий домена** — учетные данные администратора домена;
- **сценарий рабочей группы** — необходимо убедиться, что все узлы используют одинаковые учетные данные локального администратора.

В кластере ESET можно использовать также узлы, которые добавляются автоматически как участники существующего отказоустойчивого кластера Windows или кластера NLB, вместе с узлами, добавляемыми вручную (если они относятся к одному домену).

> **ПРИМЕЧАНИЕ.**
> Использовать узлы домена вместе с узлами рабочей группы невозможно.

Еще одним требованием для работы кластера ESET является включение параметра **Общий доступ к файлам и принтерам** в брандмауэре Windows перед началом установки решений ESET File Security на узлы кластера ESET.

Кластер ESET можно удалить, выбрав команду **Уничтожить кластер**. В журнал событий каждого узла будет добавлена запись об уничтожении кластера ESET. После этого все правила файервола ESET будут удалены из брандмауэра Windows. Уже существующие узлы будут возвращены в прежнее состояние, и их можно будет снова использовать в другом кластере ESET, если необходимо.

> **ПРИМЕЧАНИЕ.**
> Создание кластера ESET между ESET File Security и ESET File Security для Linux не поддерживается.

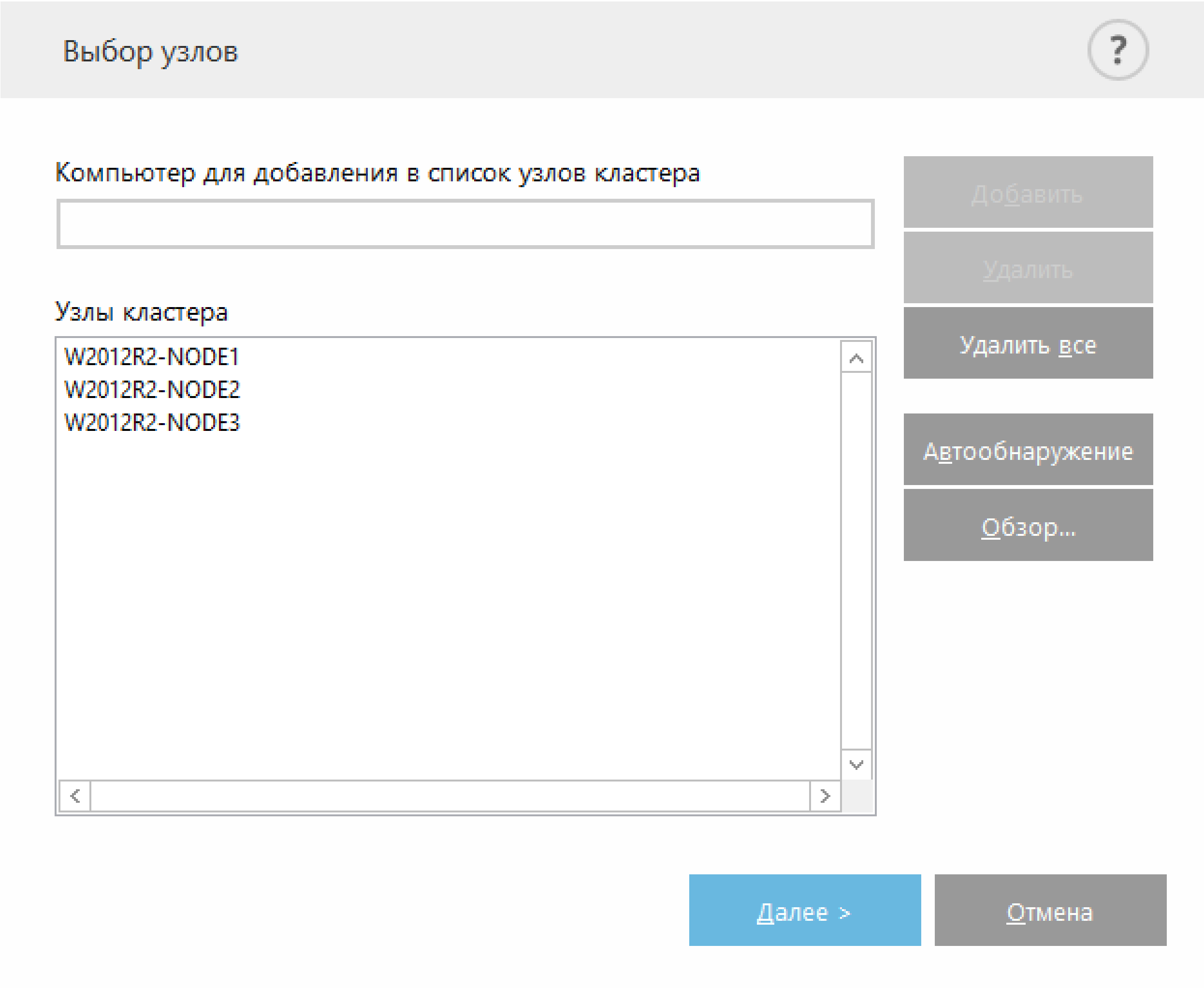
Добавление новых узлов в кластер ESET можно выполнить в любой момент, запустив **Мастер кластеров** в соответствии с описаниями выше или здесь.

7.6.4.1 Мастер кластеров — стр. 1

При настройке кластера ESET необходимо начать с добавления узлов. Чтобы добавить узлы, можно использовать функцию **Автоопределение** или команду **Обзор**. Кроме того, в текстовом поле можно ввести имя сервера и нажать кнопку **Добавить**.

Функция **Автоопределение** автоматически добавляет узлы из существующего отказоустойчивого кластера Windows или кластера NLB. Для автоматического добавления узлов сервер, который используется для создания кластера ESET, должен являться участником этого отказоустойчивого кластера Windows или кластера NLB. В свойствах кластера NLB должна быть включена функция **Разрешить удаленный контроль**, чтобы кластер ESET мог правильно определять узлы. Получив список недавно добавленных узлов, вы можете удалить ненужные узлы.

Чтобы найти и выбрать компьютеры в домене или рабочей группы, щелкните элемент **Обзор**. Этот способ позволяет добавить узлы в кластер ESET вручную. Кроме того, чтобы добавить узлы, можно ввести имя хоста, который необходимо добавить, и нажать кнопку **Добавить**.



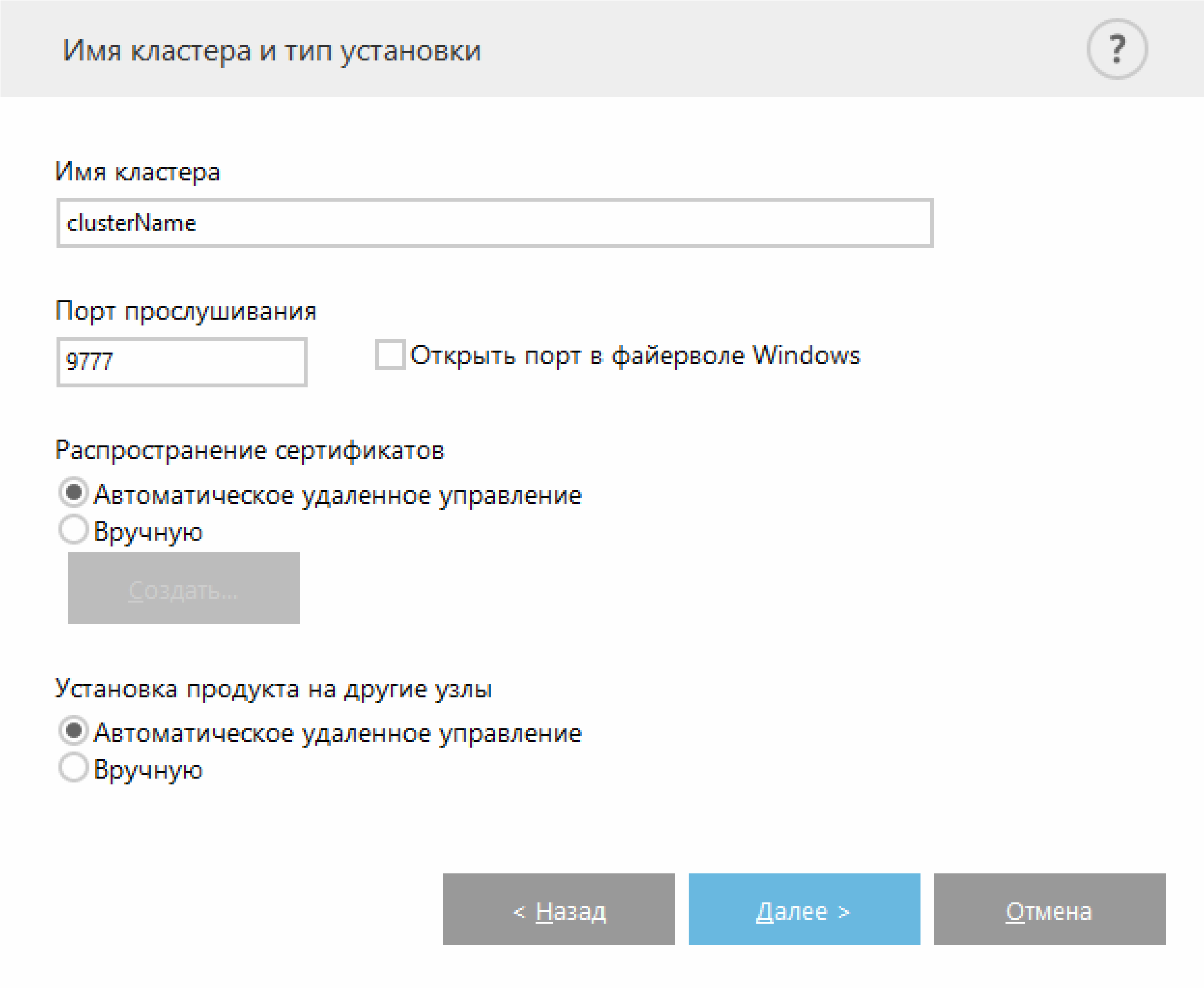
Чтобы изменить **узлы кластера** в списке, выберите узел, который следует удалить, и используйте команду **Удалить**, а чтобы полностью очистить список, выберите команду **Удалить все**.

Если кластер ESET уже используется, в него можно добавить новые узлы в любой момент. Для этого необходимо выполнить действия, описанные выше.

ПРИМЕЧАНИЕ.
Все узлы, добавляемые в список, должны находиться в сети и быть доступны. По умолчанию в списке находится узел Localhost.

7.6.4.2 Мастер кластеров — стр. 2

Выберите имя кластера и режим распространения сертификатов и укажите, нужно ли устанавливать продукт на другие узлы.



Имя кластера: введите имя кластера.
Прослушивающий порт: порт по умолчанию — 9777.
Открыть порт в брандмауэре Windows: если установлен этот флажок, в брандмауэре Windows создается правило.

Распространение сертификатов
Автоматическое удаленное управление: сертификат будет установлен автоматически.
Вручную: после нажатия кнопки **Создать** откроется окно просмотра, в котором нужно выбрать папку для хранения сертификатов. Создается корневой сертификат, а также сертификат для каждого узла, включая тот, с которого настраивается кластер ESET (локальный компьютер). Затем можно зарегистрировать сертификат на локальном компьютере, нажав кнопку **Да**. В дальнейшем необходимо будет импортировать сертификаты вручную, как описано здесь.

Установка продукта на другие узлы
Автоматическое удаленное управление: установка ESET File Security на каждый узел будет выполнена автоматически (если операционная система узла поддерживает архитектуру, которой соответствует продукт).
Вручную: этот параметр дает возможность установить программу ESET File Security вручную (например, если на некоторых узлах используется другая архитектура ОС).

Передать лицензию на узлы без активированного продукта: если выбран этот параметр, ESET Security автоматически активирует решения ESET, которые установлены на узлах и не лицензированы.

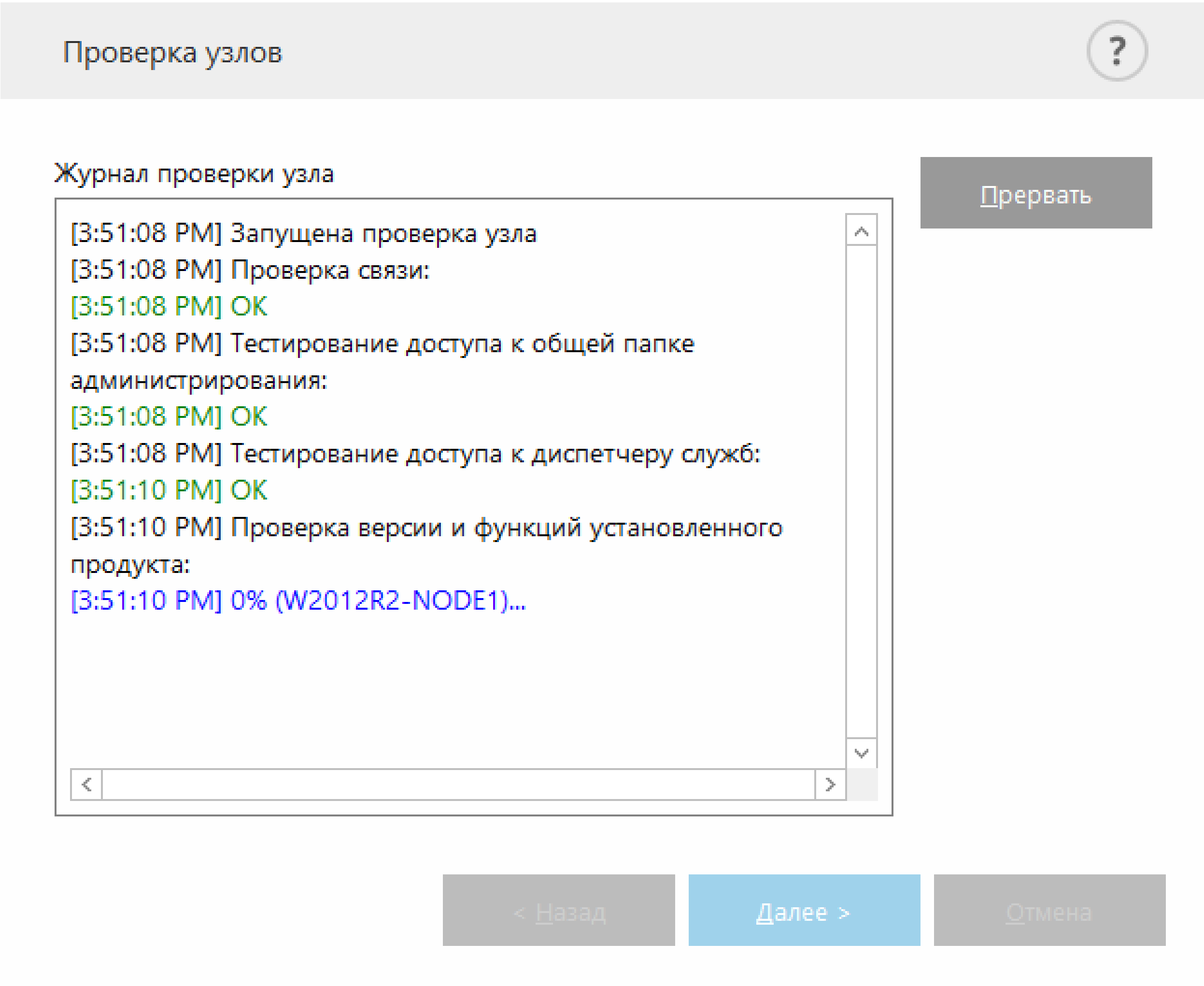
ПРИМЕЧАНИЕ.

Если необходимо создать кластер ESET с разными архитектурами ОС (32- и 64-разрядная), программу ESET File Security следует установить вручную. Используемые операционные системы определяются на следующих этапах, и эта информация отображается в окне журнала.

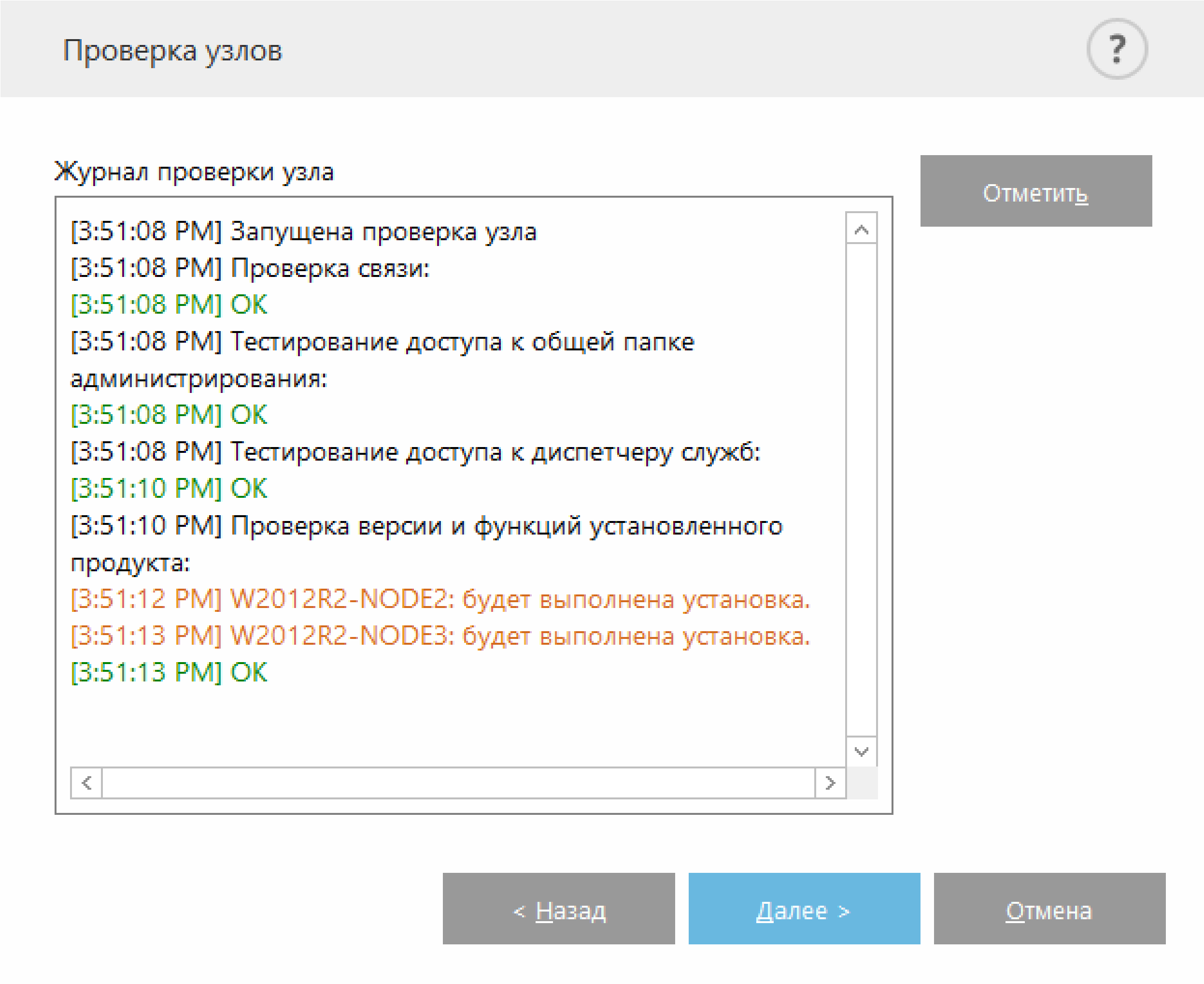
7.6.4.3 Мастер кластеров — стр. 3

После указания деталей установки выполняется проверка узлов. В **журнале проверки узла** будут отображены следующие сведения:

- проверка подключения всех существующих узлов к сети;
- проверка доступности новых узлов;
- проверка подключения узла к сети;
- проверка доступности общих ресурсов администратора;
- проверка возможности удаленного выполнения;
- подтверждение правильности установленных версий программы (или того, что программа не установлена);
- проверка наличия новых сертификатов.

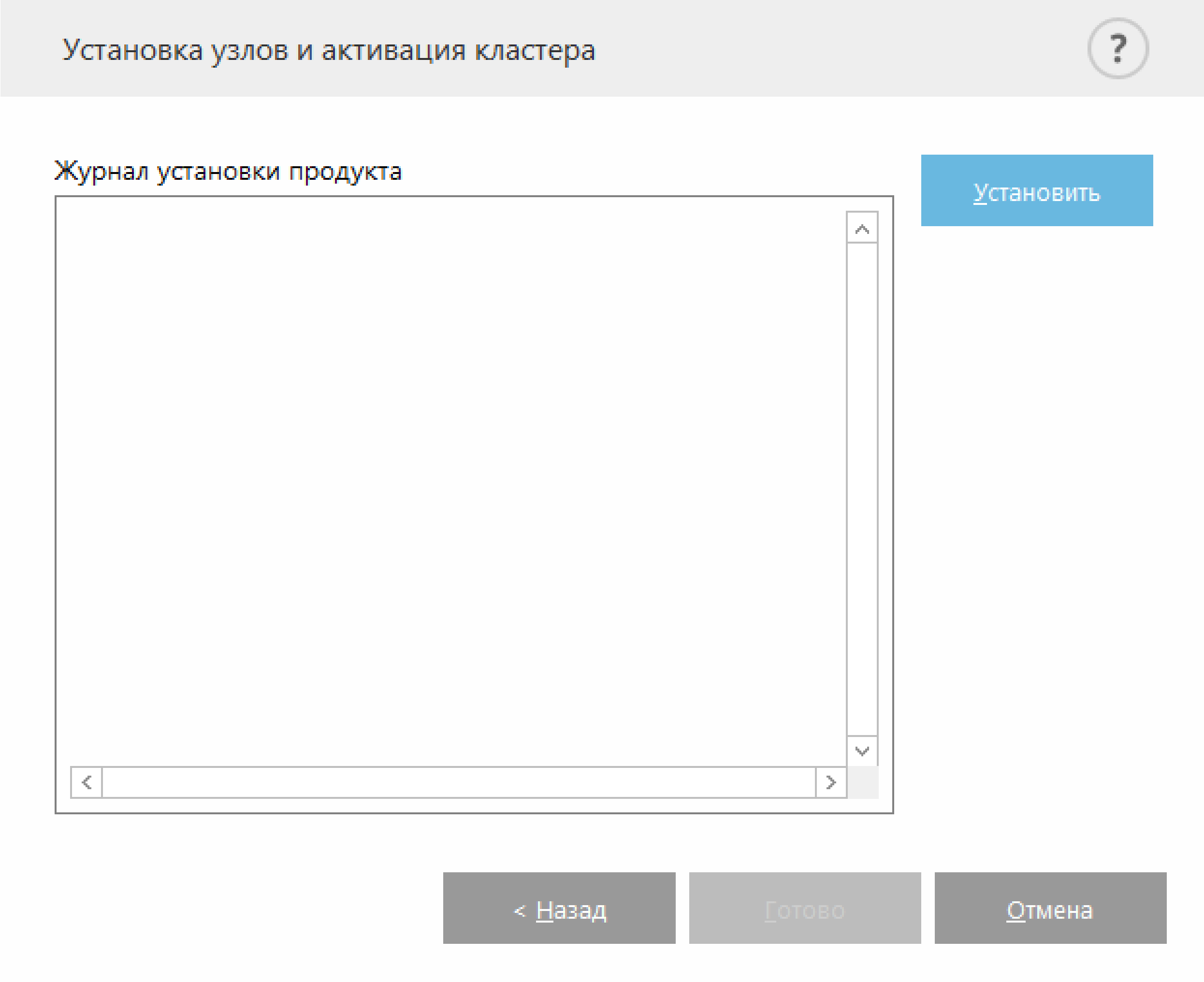


После завершения проверки узлов отобразится следующий отчет.



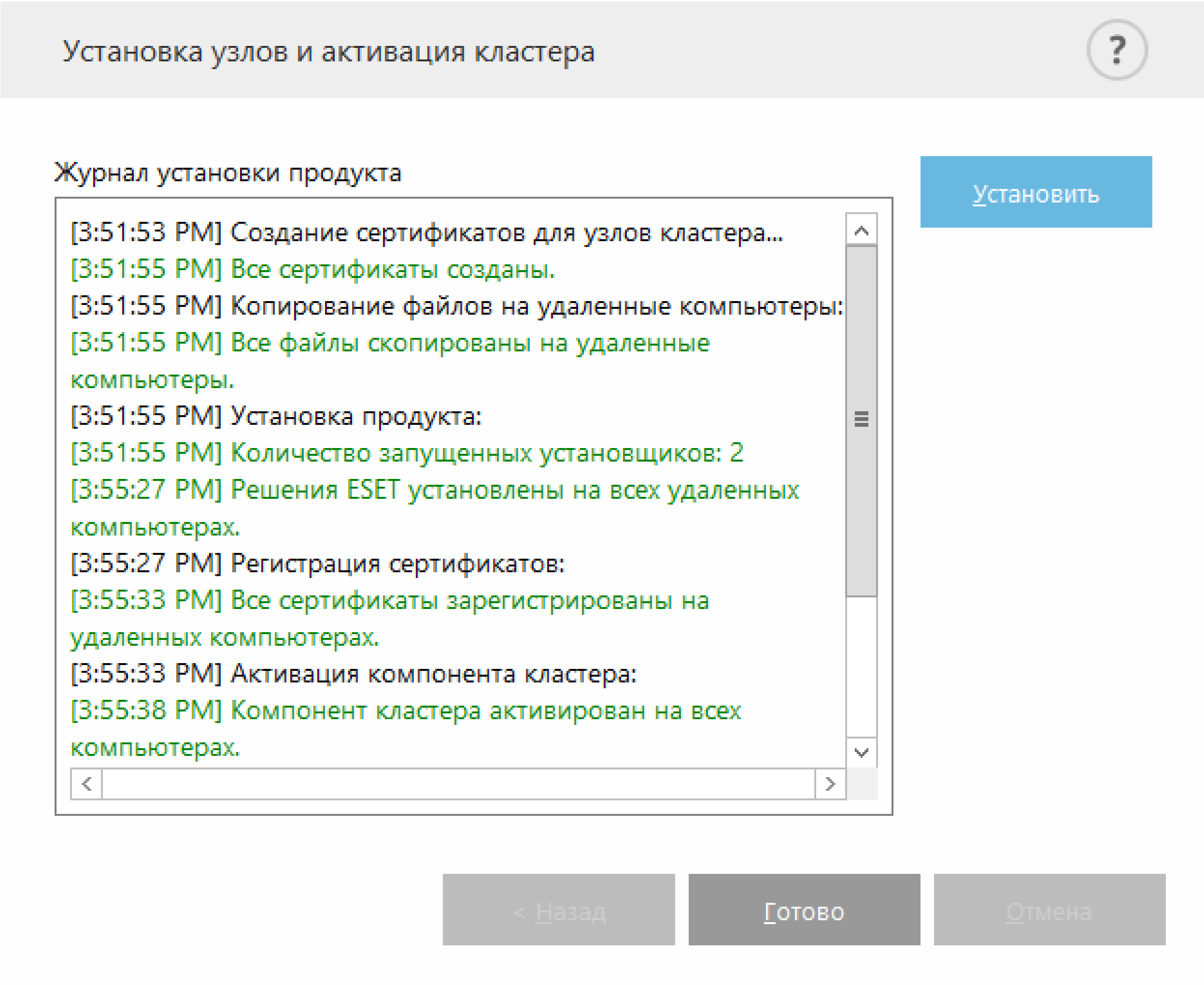
7.6.4.4 Мастер кластеров — стр. 4

Если установка программы на удаленный компьютер выполняется в процессе инициализации кластера ESET, мастер попытается найти установочный файл в каталоге *%ProgramData\ESET\<имя_продукта>\Installer*. Если установочный файл не найден в этом каталоге, отображается запрос на поиск его вручную.

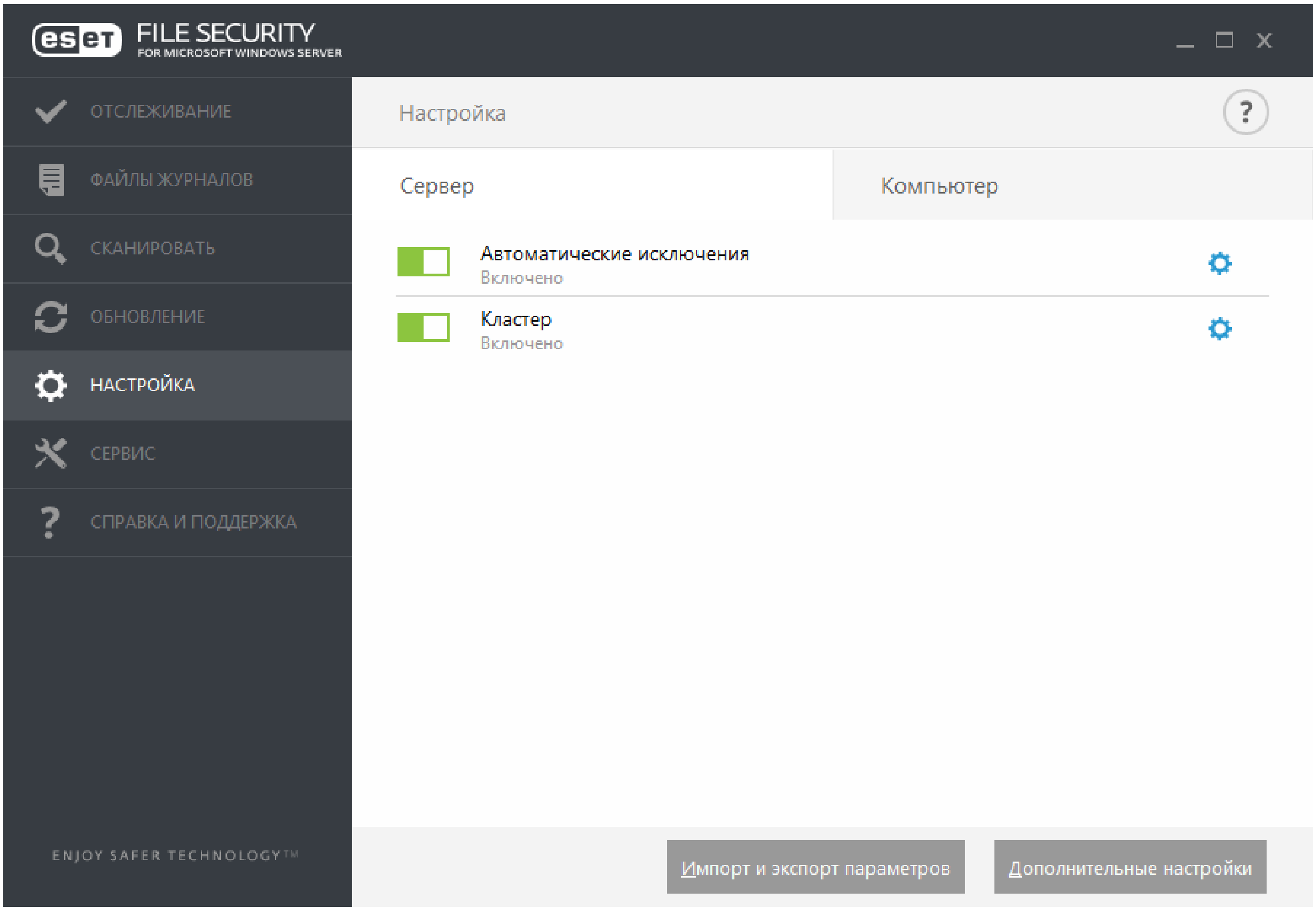


ПРИМЕЧАНИЕ.
Если выполняется автоматическая удаленная установка на узел с другой архитектурой (конфликт между 32- и 64-разрядной платформами), это будет обнаружено и для такого узла будет предложено выполнить установку вручную.

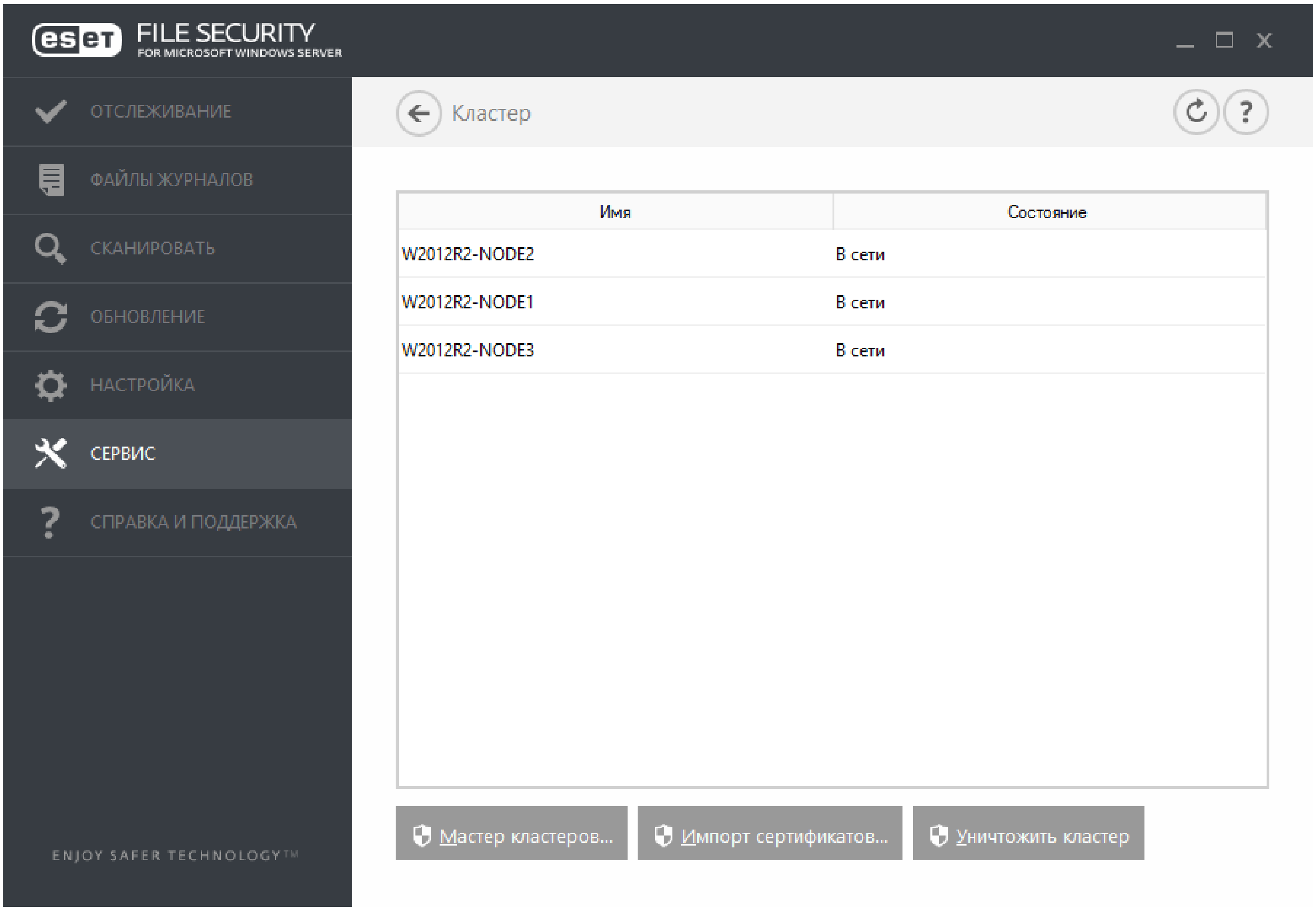
ПРИМЕЧАНИЕ.
Если на некоторых узлах уже установлена более старая версия ESET File Security, будет выдано уведомление о том, что на эти компьютеры необходимо установить новейшую версию. Обновление программы ESET File Security может вызвать автоматический перезапуск.



После правильной настройки кластера ESET он будет отображаться как включенный на странице **Настройка** > **Сервер**.



Кроме того, текущее состояние можно проверить на странице состояния кластера (**Служебные программы** > **Кластер**).



Импорт сертификатов — перейдите к папке, содержащей сертификаты (создается при использовании мастера кластеров). Выберите файл сертификата и нажмите кнопку **Открыть**.

7.6.5 Оболочка ESET

eShell (сокращение от «ESET Shell») — это интерфейс командной строки для ESET File Security. Это альтернатива графическому интерфейсу. В eShell есть все функции и возможности, обычно предоставляемые графическим интерфейсом. eShell позволяет конфигурировать и администрировать всю программу, не используя графический интерфейс.

В дополнение ко всем функциям, которые доступны в графическом интерфейсе пользователя, этот интерфейс также предлагает возможности автоматизации за счет выполнения сценариев, которые позволяют конфигурировать, изменять конфигурацию и выполнять какие-либо действия. Кроме того, интерфейс eShell может быть полезен тем пользователям, которые предпочитают командную строку графическому интерфейсу.

eShell может запускаться в двух режимах.

- Интерактивный режим полезен, когда нужно именно работать с eShell (а не просто выполнять одну команду), например при изменении конфигурации, просмотре журналов и т. д. Кроме того, интерактивный режим можно применять, если пользователю еще не знакомы все команды. Интерактивный режим упростит навигацию по интерфейсу eShell. В нем также отображаются доступные команды, которые можно использовать в рамках определенного контекста.

- Режим единичной команды/пакетный режим: этот режим можно использовать, если нужно только выполнить какую-либо команду, не входя в интерактивный режим eShell. Это можно сделать через командную строку Windows. Для этого введите `eshell` и укажите соответствующие параметры. Пример.

`eshell get status` или `eshell set antivirus status disabled`

Чтобы выполнять некоторые команды (такие как во втором примере вверху) в пакетном режиме или режиме сценария, нужно сконфигурировать определенные параметры. В противном случае появится сообщение **В доступе отказано**. Это нужно из соображений безопасности.

ПРИМЕЧАНИЕ.
Чтобы получить доступ ко всем функциям, рекомендуется запустить eShell, выбрав пункт **Запуск от имени администратора**. То же самое рекомендуется сделать при выполнении команды в командной строке Windows (cmd). Откройте командную строку, выбрав пункт **Запуск от имени администратора**. Если вы не сможете запустить командную строку от имени администратора, вы не сможете выполнять команды из-за отсутствия разрешений.

ПРИМЕЧАНИЕ.
Изменения настроек необходимы для разрешения использования команд eShell в командной строке Windows. Для получения дополнительных сведений о запуске пакетных файлов воспользуйтесь этой ссылкой.

В оболочке eShell войти в интерактивный режим можно двумя способами:

- Через меню «Пуск» Windows: **Пуск** > **Все программы** > **ESET** > **ESET File Security** > **Оболочка ESET**

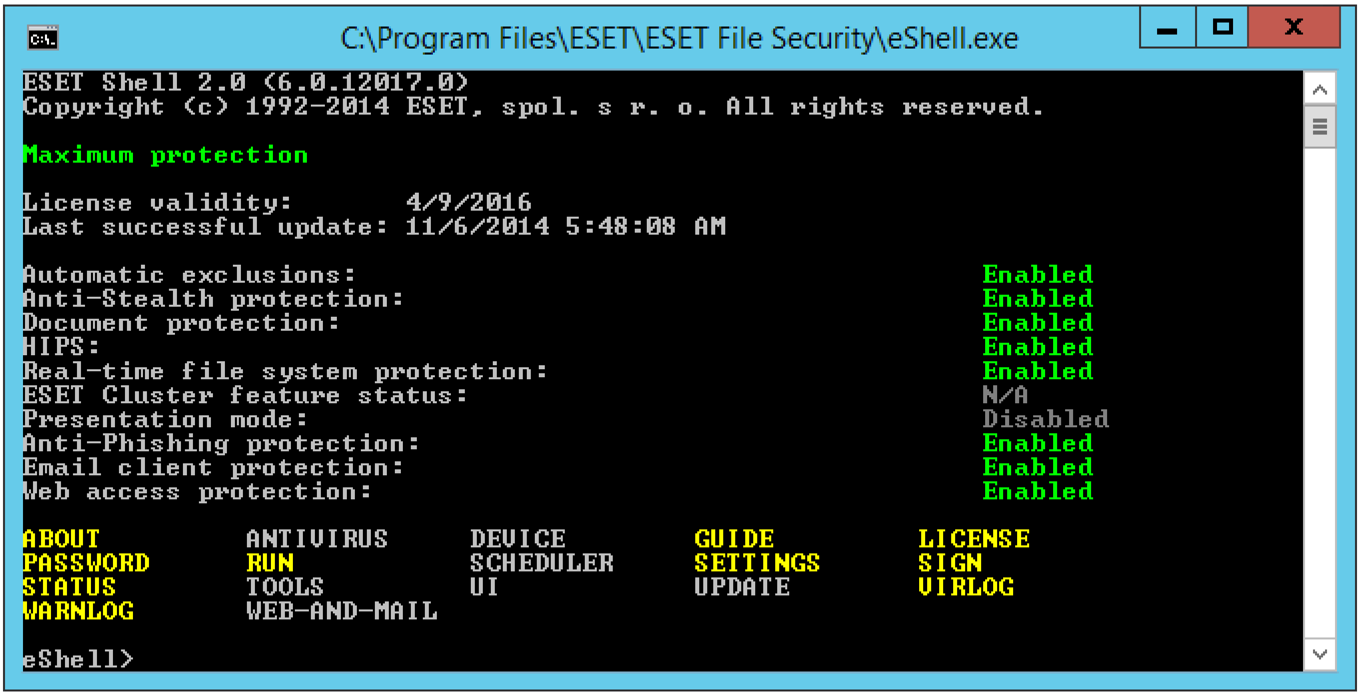
- Через командную строку Windows. Для этого нужно ввести в ней `eshell` и нажать клавишу **ВВОД**.

ВАЖНО!
Причиной возникновения ошибки `'eshell' is not recognized as an internal or external command` является то, что ваша система не загрузила новые переменные среды после установки ESET File Security. Откройте новую командную строку и попробуйте запустить eShell еще раз. Если ошибка не исчезла или у вас остается базовая установка программы ESET File Security, запустите eShell с применением абсолютного пути, например `"%PROGRAMFILES%\ESET\ESET File Security\eShell.exe"` (необходимо использовать кавычки "", чтобы команда работала).

При первом запуске eShell в интерактивном режиме на экран будет выведено окно первого запуска.

ПРИМЕЧАНИЕ.
При необходимости в дальнейшем вывести на экран окно первого запуска введите команду `guide` . В нем приводятся основные примеры использования eShell с синтаксисом, префиксами, путями команд, сокращенными формами, псевдонимами и т. д.

При следующем запуске eShell отобразится приведенное ниже окно.



ПРИМЕЧАНИЕ.
Команды можно вводить без учета регистра, используя как прописные, так и строчные буквы, и это не повлияет на их выполнение.

Настройка eShell

Вы можете настроить eShell в контексте `ui eshell`. Вы можете сконфигурировать псевдонимы, цвета, язык, политику выполнения сценариев, настройки скрытых команд и многое другое.

7.6.5.1 Использование

Синтаксис
Для правильного функционирования команд необходимо соблюдать правильный синтаксис при их форматировании, при этом структура команды может включать в себя префикс, контекст, аргументы, параметры и т. д. Ниже приведен общий синтаксис, используемый в интерфейсе eShell.

[<префикс>] [<путь команды>] <команда> [<аргументы>]

Пример (команда активирует защиту документов)
`SET ANTIVIRUS DOCUMENT STATUS ENABLED`

`SET` — префикс.
`ANTIVIRUS DOCUMENT` — путь к конкретной команде, контекст, к которому данная команда относится.
`STATUS` — непосредственно команда.
`ENABLED` — аргумент для команды.

Если использовать `?` как аргумент для команды, на экран будет выведен синтаксис непосредственно для этой команды. Например, `STATUS ?` отображает синтаксис команды `STATUS`.

СИНТАКСИС

```
[get] | status
set status enabled | disabled
```

Видно, что конструкция `[get]` заключена в скобки. Это указывает на то, что префикс `get` используется в команде `status` по умолчанию. Это означает, что при выполнении команды `status` без указания префикса используется префикс по умолчанию (в данном случае префикс `get status`). Использование команд без префиксов позволяет сэкономить время на ввод данных. Обычно `get` является префиксом по умолчанию для большинства команд, но нужно точно знать префикс по умолчанию для конкретной команды и иметь уверенность в том, что он соответствует задаче, которую необходимо выполнить.

ПРИМЕЧАНИЕ.
В командах не учитывается регистр, можно использовать как прописные, так и строчные буквы, и это не влияет на их выполнение.

Префикс/операция
Префикс — это операция. Префикс `GET` предоставляет сведения о том, как сконфигурирована определенная функция ESET File Security, или указывает на состояние (например, `GET ANTIVIRUS STATUS` покажет текущее состояние защиты). Префикс `SET` конфигурирует функциональность или меняет состояние (`SET ANTIVIRUS STATUS ENABLED` активирует защиту).

Ниже приведены префиксы, которые можно использовать в интерфейсе eShell. Команда может поддерживать или не поддерживать какие-либо из следующих префиксов.

`GET` : возвращается текущий параметр/состояние.
`SET` : задается значение или состояние.
`SELECT` : выбирается элемент.
`ADD` : добавляется элемент.
`REMOVE` : удаляется элемент.
`CLEAR` : удаляются все элементы или файлы.
`START` : запускается действие.
`STOP` : останавливается действие.
`PAUSE` : приостанавливается действие.
`RESUME` : возобновляется действие.
`RESTORE` : восстанавливаются параметры/объект/файл по умолчанию.
`SEND` : отправляется объект или файл.
`IMPORT` : выполняется импорт из файла.
`EXPORT` : выполняется экспорт в файл.

Такие префиксы, как `GET` и `SET` используются со многими командами, но в некоторых командах (например, `EXIT`) префикс не используется.

Путь команды/контекст
Команды размещаются в контекстах, которые образуют древовидную структуру. Верхний уровень древовидной структуры является корневым. При запуске eShell открывается именно корневой уровень.

```
eShell>
```

Можно либо выполнять команды непосредственно здесь или вводить имя контекста, чтобы перемещаться по древовидной структуре. Например, при вводе контекста `TOOLS` на экран будут выведены все команды и подчиненные контексты, доступные в данном контексте.

Желтым цветом обозначены команды, которые можно выполнять, а серым — подчиненные контексты, в которые можно войти. В подчиненном контексте содержатся дальнейшие команды.

Если нужно вернуться на более высокий уровень, следует использовать `..` (две точки). Например, предположим, что мы находимся здесь.

```
eShell antivirus startup>
```

Введите `..` для перехода вверх на один уровень, на этот:

```
eShell antivirus>
```

Если же необходимо вернуться на корневой уровень с уровня `eShell antivirus startup>` (отделен от корневого уровня двумя уровнями) просто введите `.. ..` (две точки, пробел, еще две точки). Это позволит перейти на два уровня вверх, то есть к корневому контексту в данном случае. Чтобы вернуться прямо в корневой контекст из уровня любой глубины древовидной структуры контекстов, используйте обратную косую черту `\`. Если нужно перейти к какому-либо контексту верхнего уровня, используйте соответствующее число `..` для перехода на необходимый уровень, а в качестве разделителя используйте пробел. Например, если нужно подняться на три уровня вверх, введите `.. .. ..`

Путь указывается относительно текущего контекста. Если команда содержится в текущем контексте, путь вводить не нужно. Например, для выполнения команды `GET ANTIVIRUS STATUS` введите

`GET ANTIVIRUS STATUS` при нахождении в корневом контексте (командная строка показывает `eShell>`)
`GET STATUS` при нахождении в контексте `ANTIVIRUS` (командная строка показывает `eShell antivirus>`)
`.. GET STATUS` при нахождении в контексте `ANTIVIRUS STARTUP` (командная строка содержит слова `eShell antivirus startup>`)

ПРИМЕЧАНИЕ.
Вы можете использовать одну точку — `.` вместо двух — `..` так как одна точка является сокращением для двух. Например:

`. GET STATUS` при нахождении в контексте `ANTIVIRUS STARTUP` (командная строка содержит слова `eShell antivirus startup>`)

Аргумент
Аргумент — это действие, которое выполняется для конкретной команды. Например, команда `CLEAN-LEVEL` (размещенная в `ANTIVIRUS REALTIME ENGINE`) может использоваться с такими аргументами:

`no` — без очистки;
`normal` — обычная очистка;
`strict` : тщательная очистка.

Другой пример: аргументы `ENABLED` или `DISABLED`, которые используются для включения и отключения определенной функции или функциональности.

Сокращенная форма/краткие команды
eShell позволяет сокращать контексты, команды и аргументы (при условии, что аргумент является параметром или альтернативным вариантом). Невозможно сократить префикс или аргумент, который является конкретным значением, таким как число, имя или путь.

ПРИМЕЧАНИЕ.
Вы можете использовать цифры `1` и `0` вместо аргументов `enabled` и `disabled`. Например:

```
set status enabled    =>   set stat 1
set status disabled    =>   set stat 0
```

Примеры краткой формы

```
set status enabled    =>   set stat en
add antivirus common scanner-excludes C:\path\file.ext    =>   add ant com scann C:\path\file.ext
```

Если две команды или два контекста начинаются с одних и тех же букв (например, ABOUT и ANTIVIRUS, и вводится A в качестве сокращенной команды), eShell не сможет решить, какую из этих двух команд необходимо выполнить. Поэтому на экран будет выведено сообщение об ошибке и список команд, начинающихся на букву A, из которого можно выбрать необходимое.

```
eShell>a
The following command is not unique: a

The following commands are available in this context:
    ABOUT: показывает информацию о программе.
    ANTIVIRUS: изменяет антивирус контекста.
```

При добавлении еще одной или нескольких букв (например, AB вместо просто A) eShell выполнит ABOUT , так как теперь эта команда является уникальной.

ПРИМЕЧАНИЕ.
Чтобы команда выполнялась надлежащим образом, рекомендуется не сокращать команды, аргументы и т. д. и использовать их полную форму. В этом случае все будет выполнено именно так, как нужно, и удастся избежать нежелательных ошибок. Это особенно верно для пакетных файлов/сценариев.

Автозаполнение
Эта новая функция, представленная в eShell 2.0 eShell, очень похожа на функцию автозаполнения в командной строке Windows. В командной строке Windows заполняются пути к файлам, а в eShell заполняются команды, контекст и имена операций. Заполнение аргументов не поддерживается. Чтобы при обычном вводе команды выполнить автозаполнение или просмотреть доступные варианты, нажмите клавишу **TAB**. Чтобы пролистать варианты назад, нажмите клавиши **SHIFT** + **TAB**. Одновременное использование сокращенной формы и автоматического заполнения не поддерживается. Используйте или одно, или другое. Например, если при вводе antivir real scan нажать клавишу **TAB**, ничего не произойдет. Эту команду лучше вводить так: введите antivir и нажмите клавишу **TAB** для автоматического ввода antivirus, затем введите «real» и нажмите **TAB**, а затем введите «scan» и опять нажмите **TAB**. Вы можете просмотреть все доступные варианты: scan-create, scan-execute, scan-open и т. д.

Псевдонимы
Псевдоним — это альтернативное название, которое может использоваться для выполнения команды (при условии, что этой команде присвоен псевдоним). Есть несколько псевдонимов по умолчанию:

(глобально) close — exit
(глобально) quit — exit
(глобально) bye — exit
warnlog — tools log events
virlog — tools log detections
antivirus on-demand log — tools log scans

Под «(глобально)» понимается, что такую команду можно использовать в любом месте вне зависимости от текущего контекста. Одной команде может быть назначено несколько псевдонимов. Например, у команды EXIT есть псевдонимы CLOSE, QUIT и BYE. Для выхода из eShell можно использовать непосредственно команду EXIT или любой из нее псевдонимов. Псевдоним VIRLOG является псевдонимом команды DETECTIONS в контексте TOOLS LOG . Таким образом команда DETECTIONS доступна из корневого контекста ROOT , что делает ее более доступной (не нужно вводить контекст TOOLS и затем LOG , и выполнять ее непосредственно в ROOT).

eShell дает пользователям возможность задавать собственные псевдонимы. Команду ALIAS можно найти в контексте UI ESHELL .

Защитить параметры паролем
Параметры ESET File Security можно защитить паролем. Пароль можно задать с помощью графического интерфейса или в eShell с помощью команды set ui access lock-password. Для выполнения некоторых команд (например, тех, что изменяют параметры или данные) этот пароль понадобится вводить в интерактивном режиме. Если вы планируете работать в eShell длительное время и не желаете постоянно вводить пароль, решение eShell может запомнить его. Для этого нужно воспользоваться командой set password . После этого он будет вводиться автоматически при каждом выполнении команды, для которой

требуется пароль. Программа eShell помнит пароль, пока вы не вышли из нее. Это значит, что команду `set password` нужно будет при запуске нового сеанса выполнить еще раз (если нужно, чтобы решение eShell запомнило пароль).

Руководство и справка
При выполнении команды `GUIDE` или `HELP` на экран выводится окно первого запуска, в котором объясняется использование eShell. Эта команда доступна в контексте `ROOT` (`eShell>`).

История команд
eShell хранит журнал выполненных ранее команд. Это распространяется только на текущий интерактивный сеанс eShell. После завершения сеанса работы eShell журнал команд удаляется. С помощью стрелок вверх и вниз на клавиатуре можно перемещаться по журналу. Обнаружив нужную команду, можно выполнить ее повторно или внести в нее изменения, причем не нужно вводить заново всю команду целиком.

CLS/очистка экрана
Команду `CLS` можно использовать для очистки экрана. Она работает точно так же, как в командной строке Windows и других аналогичных интерфейсах командной строки.

EXIT / CLOSE / QUIT / BYE
Для того чтобы закрыть eShell или выйти из этого интерфейса, можно воспользоваться любой из этих команд (`EXIT`, `CLOSE`, `QUIT` или `BYE`).

7.6.5.2 Команды

В этом разделе приведено несколько основных команд eShell с описаниями.

> **ПРИМЕЧАНИЕ.**
> В командах не учитывается регистр, можно использовать как прописные, так и строчные буквы, и это не влияет на их выполнение.

Образцы команд (присутствующие в контексте ROOT):

ABOUT

На экран выводятся сведения о программе. Отображается такая информация:

- имя и номер версии установленного решения ESET по обеспечению безопасности;
- операционная система и основные сведения об оборудовании;
- имя пользователя (в том числе домен), полное имя компьютера (полное доменное имя, если сервер входит в домен) и имя рабочего места;
- сведения об установленных компонентах решения ESET по обеспечению безопасности, в том числе номер версии каждого компонента.

ПУТЬ В КОНТЕКСТЕ

```
root
```

PASSWORD

Обычно для выполнения защищенных паролем команд предлагается ввести пароль из соображений безопасности. Это применяется к таким командам, которые отключают защиту от вирусов или могут повлиять на функциональность ESET File Security. Пользователю предлагается ввести пароль при каждом выполнении такой команды. Однако можно задать этот пароль, чтобы не вводить его каждый раз. Он будет сохранен в eShell и будет использоваться автоматически при выполнении защищенной паролем команды.

> **ПРИМЕЧАНИЕ.**
> Заданный пароль работает только в текущем интерактивном сеансе eShell. После выхода из eShell заданный пароль будет удален. При повторном запуске eShell пароль нужно задать снова.

Заданные пароли можно использовать также при выполнении неподписанных пакетных файлов и сценариев. Выполняя неподписанные пакетные файлы, задайте для политики выполнения ESET Shell значение **Полный доступ**. Ниже приведен пример такого пакетного файла.

```
eshell set password plain <yourpassword> "&" set status disabled
```

Эта соединенная команда задает пароль и отключает защиту.

ВАЖНО!
Рекомендуется использовать подписанные пакетные файлы всегда, когда возможно, чтобы пароли в пакетных файлах всегда шифровались (при использовании описанного выше способа). Дополнительные сведения см. в разделе Пакетные файлы и сценарии (в подразделе **Подписанные пакетные файлы**).

ПУТЬ В КОНТЕКСТЕ

`root`

СИНТАКСИС

`[get] | restore password`

`set password [plain <пароль>]`

ОПЕРАЦИИ

`get` : показать пароль.

`set` : задать или очистить пароль.

`restore` : очистить пароль.

АРГУМЕНТЫ

`plain` : переход ко вводу пароля как параметра.

`password` : пароль.

ПРИМЕРЫ

`set password plain <вашпароль>` : задается пароль, который будет использоваться для защищенных паролем команд.

`restore password` : очищается пароль.

ПРИМЕРЫ

`get password` — эта команда позволяет увидеть, настроен ли пароль (на экран при этом выводятся только символы «звездочка» (*), сам пароль не отображается). Если символов «звездочка» нет, это значит, что пароль не установлен.

`set password plain <вашпароль>` : эта команда позволяет задать пароль.

`restore password` : эта команда очищает заданный пароль.

STATUS

Отображается информация о текущем состоянии защиты ESET File Security (аналогично графическому интерфейсу пользователя).

ПУТЬ В КОНТЕКСТЕ

`root`

СИНТАКСИС

`[get] | restore status`

`set status disabled | enabled`

ОПЕРАЦИИ

`get` : показать состояние защиты от вирусов.

`set` : отключить или включить защиту от вирусов.

`restore` : восстановить параметры по умолчанию.

АРГУМЕНТЫ

`disabled` : отключить защиту от вирусов.

`enabled` : включить защиту от вирусов.

ПРИМЕРЫ

`get status` : отображается текущее состояние защиты.

`set status disabled` : отключается защита.

`restore status` : для защиты восстанавливаются параметры по умолчанию (включена).

VIRLOG

Это псевдоним команды `DETECTIONS` . Эта команда полезна, когда нужно просмотреть информацию об обнаруженных заражениях.

WARNLOG

Это псевдоним команды `EVENTS` . Эта команда полезна, когда нужно просмотреть информацию о различных событиях.

7.6.5.3 Пакетные файлы и сценарии

Для автоматизации работы решение eShell можно использовать как мощное средство написания сценариев. Чтобы использовать пакетный файл в решении eShell, создайте этот файл, указав в нем слово eShell и команду. Например:

```
eshell get antivirus status
```

Кроме того, команды можно, а иногда и нужно связывать. Например, если нужно получить определенную запланированную задачу, введите следующее:

```
eshell select scheduler task 4 "&" get scheduler action
```

Выбор элемента (в этом случае это четвертая задача) обычно применяется только к запущенному в это время экземпляру eShell. Если выполнять эти команды одну за другой, выполнение второй команды закончится сбоем и появится сообщение об ошибке «Не выбрано ни одной задачи, или выбранная задача больше не существует».

В целях безопасности по умолчанию для политики выполнения задано значение **Ограниченные сценарии**. Поэтому вы можете использовать решение eShell как инструмент мониторинга, однако не можете изменять конфигурацию ESET File Security с помощью скриптов. При исполнении сценария, содержащего команды, которые могут нарушить безопасность, например команды отключения защиты, отображается сообщение **Доступ запрещен**. Для исполнения команд, которые вносят изменения в конфигурацию, рекомендуется использовать подписанные пакетные файлы.

Чтобы изменить конфигурацию путем ввода одиночной команды вручную в командной строке Windows, решению eShell необходимо предоставить полный доступ (не рекомендуется). Чтобы предоставить полный доступ, введите команду`ui eshell shell-execution-policy` в интерактивном режиме в eShell или последовательно в графическом интерфейсе выберите элементы **Дополнительные настройки** > **Интерфейс пользователя** > Оболочка ESET.

Подписанные пакетные файлы
Решение eShell позволяет защищать обычные пакетные файлы (*.bat) с помощью подписи. При подписании сценариев используется тот же пароль, что и для защиты параметров. Чтобы подписать сценарий, сначала нужно включить защиту параметров. Это можно сделать с помощью графического интерфейса или в eShell с

помощью команды `set ui access lock-password`. Подписывать пакетные файлы можно сразу после установки пароля защиты параметров.

Чтобы подписать пакетный файл, запустите команду `sign <script.bat>` из корневого контекста eShell, где *script.bat* — это путь к сценарию, который нужно подписать. Введите и подтвердите пароль, который будет использоваться для подписания. Он должен совпадать с паролем защиты параметров. Подпись ставится в конце пакетного файла в форме комментария. Если сценарий уже подписан, подпись будет заменена на новую.

ПРИМЕЧАНИЕ.
При изменении ранее подписанных пакетных файлов подпись нужно ставить еще раз.

ПРИМЕЧАНИЕ.
Если изменен пароль защиты параметров, нужно подписать все сценарии еще раз. В противном случае с момента изменения пароля выполнение сценариев будет заканчиваться неудачей. Пароль, введенный при подписании сценария, должен соответствовать паролю защиты параметров в целевой системе.

Чтобы выполнить подписанный пакетный файл из командной строки Windows или как запланированную задачу, используйте такую команду:

```
eshell run <script.bat>
```

В этой команде «script.bat» — это путь к пакетному файлу. Например, `eshell run d:\myeshellscript.bat`

7.6.6 ESET SysInspector

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

В окне ESET SysInspector отображаются следующие данные о созданных журналах.

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

Доступны перечисленные далее действия.

- **Открыть**: открывает созданный журнал. Кроме того, можно щелкнуть журнал правой кнопкой мыши и выбрать в контекстном меню пункт **Показать**.
- **Сравнить**: сравнение двух существующих журналов.
- **Создать**: создание журнала. Дождитесь окончания создания журнала ESET SysInspector (в поле **Состояние** будет показано значение «Создано»).
- **Удалить**: удаление выбранных журналов из списка.

В контекстном меню, которое открывается, если щелкнуть правой кнопкой мыши один или несколько выделенных журналов, доступны перечисленные ниже действия.

- **Показать**: открытие выбранного журнала в ESET SysInspector (аналогично двойному щелчку).
- **Сравнить**: сравнение двух существующих журналов.
- **Создать**: создание журнала. Дождитесь окончания создания журнала ESET SysInspector (в поле **Состояние** будет показано значение «Создано»).
- **Удалить**: удаление выбранных журналов из списка.
- **Удалить все**: удаление всех журналов.
- **Экспорт**: экспорт журнала в обычный или заархивированный файл в формате *XML*.

7.6.6.1 Создать снимок состояния компьютера

Введите краткий комментарий, описывающий создаваемый журнал, и нажмите кнопку **Добавить**. Дождитесь окончания создания журнала ESET SysInspector (в поле «Состояние» будет показано значение **Создано**). Длительность создания журнала зависит от конфигурации оборудования и системных данных.

7.6.6.2 ESET SysInspector

7.6.6.2.1 Введение в ESET SysInspector

ESET SysInspector — это приложение, которое тщательно проверяет компьютер и отображает собранные данные в понятном виде. Представляемые данные, такие как информация об установленных драйверах и приложениях, сетевых подключениях и важных записях реестра, позволяют определить причину подозрительного поведения системы, которое может быть вызвано несовместимостью программного или аппаратного обеспечения или заражением вредоносными программами.

Существует два способа воспользоваться приложением ESET SysInspector. Во-первых, можно открыть интегрированную в ESET Security версию, а, во-вторых, загрузить самостоятельную версию (SysInspector.exe) бесплатно с веб-сайта ESET. Обе версии аналогичны по своим функциям и имеют одинаковые элементы управления программой. Единственное отличие заключается в том, как осуществляется управление результатами. И отдельная, и интегрированная версии позволяют экспортировать снимки системы в файл в формате *XML* и сохранять его на диске. Однако интегрированная версия также дает возможность хранить снимки системы прямо в разделе **Служебные программы** > **ESET SysInspector** (за исключением ESET Remote Administrator). Дополнительные сведения см. в разделе ESET SysInspector как часть ESET File Security.

Дайте ESET SysInspector некоторое время на сканирование компьютера. Этот процесс может занять от 10 секунд до нескольких минут в зависимости от конфигурации оборудования, операционной системы и количества установленных на компьютере приложений.

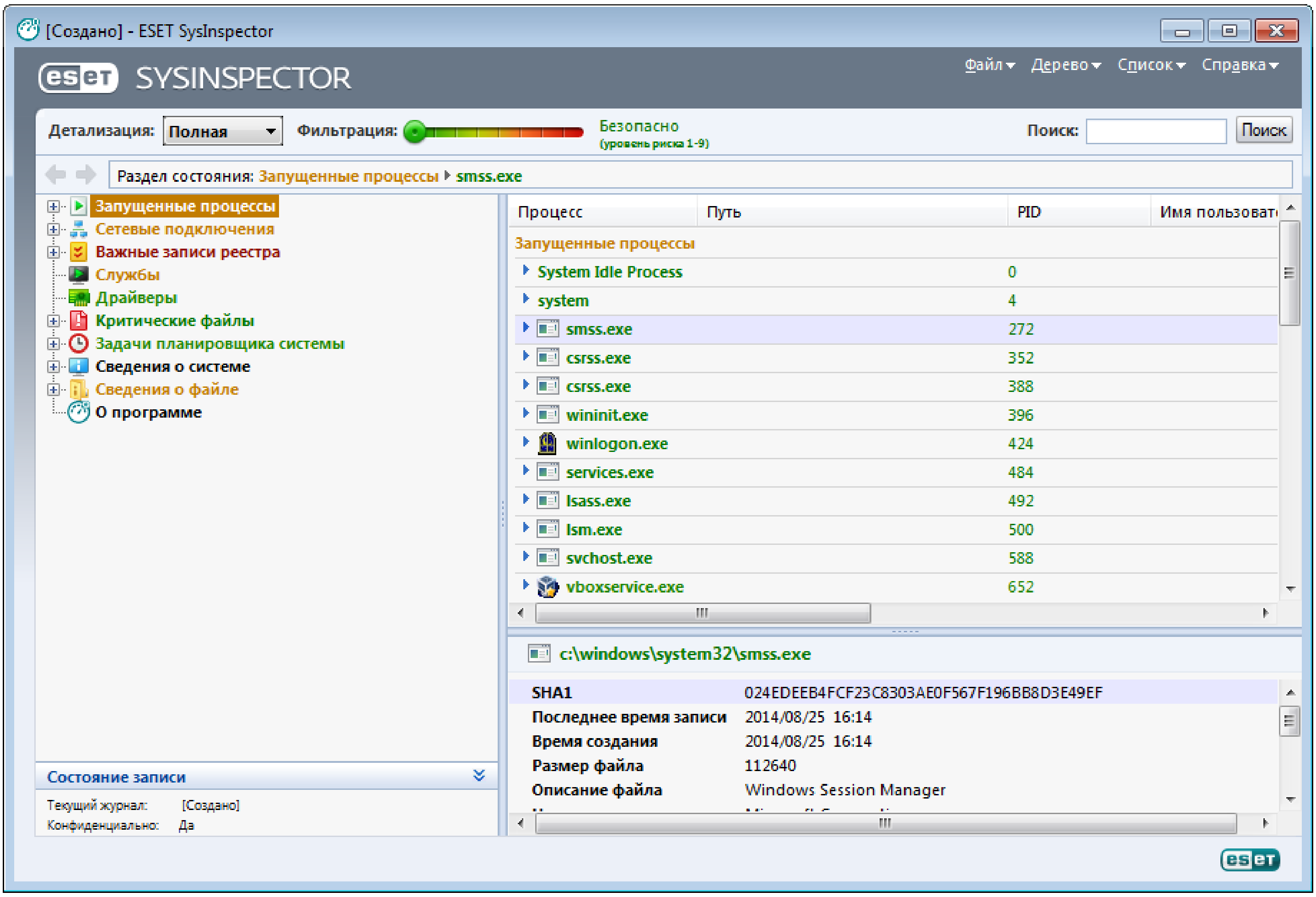
7.6.6.2.1.1 Запуск ESET SysInspector

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 File Security**).

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

7.6.6.2.2 Интерфейс пользователя и работа в приложении

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



7.6.6.2.2.1 Элементы управления программой

В этом разделе описаны все элементы управления программой, доступные в ESET SysInspector.

Файл

Если нажать **Файл**, то можно сохранить данные о текущем состоянии системы для их последующего изучения или открыть ранее сохраненный журнал. Если планируется опубликовать журнал, для его создания рекомендуется использовать пункт меню **Подходит для отправки**. В этом случае из журнала исключается конфиденциальная информация (имя текущего пользователя, имя компьютера, имя 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 свернуть все узлы, а также экспортировать выделенные разделы в сценарий службы.

Список

Содержит функции, облегчающие навигацию по программе, а также прочие функции, такие как поиск информации в Интернете.

Справка

Содержит сведения о приложении и его функциях.

Подробности

Этот параметр влияет на выводимую в главном окне программы информацию, облегчая работу с ней. В основном режиме пользователю доступна информация, необходимая для поиска решений стандартных проблем, возникающих в системе. В режиме «Среднее» программа отображает реже используемые сведения. В режиме «Полное» ESET SysInspector выводит на экран всю информацию, необходимую для решения самых нестандартных проблем.

Фильтрация

Фильтрация элементов очень удобна для поиска подозрительных файлов или записей реестра, существующие в системе. 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 будет отфильтровывать все элементы с уровнем риска, меньшим текущего уровня, и выводить на экран только те элементы, уровень подозрительности которых выше данного уровня. Если ползунок находится в крайнем правом положении, программа отображает только определенно вредоносные элементы.

Все элементы, имеющие уровень риска от 6 до 9, могут представлять угрозу для безопасности. Если вы не используете какие-либо решения по безопасности ESET, рекомендуется просканировать компьютер с помощью ESET Online Scanner после нахождения любых таких элементов программой ESET SysInspector. 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

Поиск можно использовать 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 окне 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 соответствующий файл можно удалить. Перед удалением убедитесь, что файлы действительно опасны или не являются необходимыми.

7.6.6.2.2.2 Навигация в ESET SysInspector

ESET SysInspector распределяет информацию разных типов по нескольким основным разделам, называемым узлами. Для того чтобы получить дополнительные сведения о каком-либо узле (если таковые есть), разверните его для просмотра вложенных узлов. Чтобы открыть или свернуть узел, дважды щелкните имя узла либо рядом с именем щелкните значок ⊞ или ⊟. При перемещении по древовидной структуре узлов в окне навигации о каждом из них доступны различные сведения, отображаемые в окне описания. При переходе к конкретному элементу в окне описания дополнительные сведения об этом элементе можно просмотреть в окне подробных сведений.

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, уровень риска файла и т. п.

В окне подробной информации содержатся дополнительные сведения об элементах, выбранных в окне описания, такие как 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 отображается в ESET SysInspector с символами «\??\» в начале. Эти символы обеспечивают оптимизацию до запуска таких процессов 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 можно проверить IP-адреса DNS-серверов.

В окне подробной информации содержатся дополнительные сведения об элементах, выбранных в окне описания, такие как размер файла или его хэш.

Важные записи реестра

Содержит список определенных записей реестра, которые часто бывают связаны с различными проблемами в системе, такие как записи, задающие автоматически загружаемые программы, объекты модуля поддержки обозревателя и т. п.

В окне описания также могут быть перечислены файлы, связанные с некоторыми из этих записей. В окне подробных сведений может быть представлена дополнительная информация.

Службы

В окне описания перечислены файлы, зарегистрированные в качестве служб Windows. В окне подробных сведений можно увидеть способ запуска службы, а также просмотреть определенную информацию о файле.

Драйверы

Список драйверов, установленных в системе.

Критические файлы

В окне описания отображается содержимое критически важных файлов операционной системы Microsoft Windows.

Задачи планировщика системы

Содержит список задач, запускаемых планировщиком заданий Windows в указанное время или через заданные интервалы.

Информация о системе

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

Сведения о файле

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

О программе

Информация о версии ESET SysInspector и список модулей программы.

Ниже представлен список сочетаний клавиш, которые можно использовать при работе с ESET SysInspector.

Файл

Ctrl + O	открытие существующего журнала
Ctrl + S	сохранение созданных журналов

Создать

Ctrl + G	создание стандартного снимка состояния компьютера
Ctrl + H	создание снимка состояния компьютера, в котором может быть зарегистрирована конфиденциальная информация

Фильтрация элементов

1, O	безопасные элементы, отображаются элементы с уровнем риска от 1 до 9
2	безопасные элементы, отображаются элементы с уровнем риска от 2 до 9
3	безопасные элементы, отображаются элементы с уровнем риска от 3 до 9
4, U	неизвестные элементы, отображаются элементы с уровнем риска от 4 до 9
5	неизвестные элементы, отображаются элементы с уровнем риска от 5 до 9
6	неизвестные элементы, отображаются элементы с уровнем риска от 6 до 9
7, B	опасные элементы, отображаются элементы с уровнем риска от 7 до 9
8	опасные элементы, отображаются элементы с уровнем риска от 8 до 9
9	опасные элементы, отображаются элементы с уровнем риска 9
-	понижение уровня риска
+	повышение уровня риска
Ctrl + 9	выбор режима фильтрации, равный или более высокий уровень
Ctrl + 0	выбор режима фильтрации, только равный уровень

Представление

Ctrl + 5	просмотр по производителям, все производители
Ctrl + 6	просмотр по производителям, только Microsoft
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	разворачивание дерева
Ctrl + Q	сворачивание дерева

Прочие элементы управления

Ctrl + T	переход к исходному местоположению элемента после его выделения в результатах поиска
Ctrl + P	отображение основных сведений об элементе
Ctrl + A	отображение всех сведений об элементе
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 выделенный 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 службы

Сравнение

Ctrl + Alt + O	открытие исходного или сравниваемого с ним журнала
Ctrl + Alt + R	отмена сравнения
Ctrl + Alt + 1	отображение всех элементов
Ctrl + Alt + 2	отображение только добавленных элементов, в журнале отображаются только элементы из текущего журнала
Ctrl + Alt + 3	отображение только удаленных элементов, в журнале отображаются только элементы из предыдущего журнала
Ctrl + Alt + 4	отображение только замененных элементов (в том числе файлов)
Ctrl + Alt + 5	отображение только различий между журналами
Ctrl + Alt + C	отображение сравнения
Ctrl + Alt + N	отображение текущего журнала
Ctrl + Alt + P	открытие предыдущего журнала

Разное

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

7.6.6.2.2.3 Сравнение

С помощью функции сравнения пользователь может сравнить два существующих журнала. Результатом выполнения 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 в каждый момент времени отображается только один журнал.

Преимущество сравнения двух журналов заключается в том, что можно одновременно просматривать активный в данный момент журнал и сохраненный в файл журнал. Для сравнения журналов в меню **Файл** выберите пункт **Сравнить журналы** и выполните команду **Выбрать файл**. Выбранный журнал будет сравниваться с активным журналом в главном окне программы. В сравнительном журнале отображаются только различия между этими двумя журналами.

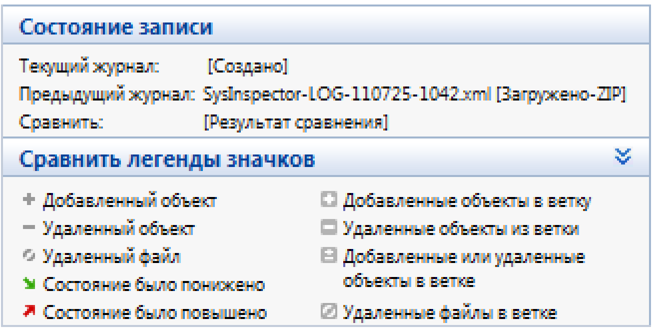
ПРИМЕЧАНИЕ. При сравнении двух файлов журнала в меню **Файл** выберите пункт **Сохранить журнал** и сохраните журнал как файл в формате ZIP. В результате будут сохранены оба файла. Если такой файл впоследствии открыть, содержащиеся в нем журналы сравниваются автоматически.

Напротив отображенных элементов ESET SysInspector выводит символы, обозначающие различия между сравниваемыми журналами.

Описание всех символов, которые могут отображаться напротив элементов

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

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



Любой сравнительный журнал можно сохранить в файл и открыть его позже.

Пример

Создайте и сохраните журнал, содержащий исходную информацию о системе, в файл с названием «предыдущий.xml». После внесения изменений в систему откройте ESET SysInspector и дайте приложению возможность создать 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, содержащий различиями между сравниваемыми.

Тот же результат можно получить с помощью следующих параметров командной строки:

SysIsnpector.exe текущий.xml предыдущий.xml

7.6.6.2.3 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
/privacy	создание журнала без конфиденциальной информации
/zip	сохранение созданного журнала в ZIP-архиве
/silent	скрытие окна 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.

7.6.6.2.4 Сценарий службы

Сценарий службы — это инструмент, который помогает пользователям ESET SysInspector легко удалять нежелательные объекты с компьютера.

Сценарий службы позволяет целиком или частично экспортировать журнал ESET SysInspector. После экспорта пользователь может пометить нежелательные объекты для удаления. Затем можно запустить сценарий с отредактированным журналом для удаления помеченных объектов.

Сценарий службы для пользователей, имеющих опыт в диагностике компьютерных систем. Неквалифицированное внесение изменений может привести к повреждению 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. Выделите первый элемент в разделе слева (в древовидной структуре), нажмите клавишу Shift, а затем выберите последний элемент, чтобы пометить все элементы.
3. Щелкните выделенные объекты правой кнопкой мыши и в контекстном меню выберите пункт **Экспортировать выбранные разделы в сценарий службы**.
4. Выделенные объекты будут экспортированы в новый журнал.
5. Далее следует наиболее важный этап всей процедуры. Откройте созданный журнал и измените атрибут «-» на «+» для всех объектов, которые нужно удалить. Убедитесь, что не помечены никакие важные файлы или объекты операционной системы.
6. Откройте ESET SysInspector, перейдите в раздел **Файл** > **Запустить сценарий службы** и введите путь к своему сценарию.
7. Нажмите кнопку **ОК**, чтобы запустить сценарий.

7.6.6.2.4.1 Создание сценариев службы

Для того чтобы создать сценарий, щелкните правой кнопкой мыши любой объект в древовидном меню (в левой панели) главного окна ESET SysInspector. В контекстном меню выберите команду **Экспортировать все разделы в сценарий службы** или **Экспортировать выбранные разделы в сценарий службы**.

ПРИМЕЧАНИЕ. Сценарий службы нельзя экспортировать во время сравнения двух журналов.

7.6.6.2.4.2 Структура сценария службы

Первая строка заголовка сценария содержит данные о версии модуля (ev), версии графического интерфейса пользователя (gv) и версии журнала (lv). Эти данные позволяют отслеживать изменения в файле в формате XML, используемом для создания сценария. Они предотвращают появление несоответствий на этапе выполнения. Эту часть сценария изменять не следует.

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

01) Running processes (Запущенные процессы)

В этом разделе содержится список процессов, запущенных в системе. Каждый процесс идентифицируется по UNC-пути, а также по хэш-коду 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 выделен (помечен символом «+») процесс module32.exe. При выполнении сценария этот процесс будет завершен.

02) Loaded modules (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 завершаются.

03) TCP connections (Подключения по TCP)

Этот раздел содержит данные о существующих подключениях по TCP.

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 сценария обнаруживается владелец сокета помеченных подключений по TCP, после чего сокет останавливается, высвобождая системные ресурсы.

04) UDP endpoints (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) DNS server entries (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) Important registry entries (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 же будут восстановлены их значения по умолчанию. Действия, применяемые к конкретным записям, зависят от категории и значения записи реестра.

07) Services (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, а также все зависящие от них службы будут остановлены и удалены.

08) Drivers (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 останавливаются выбранные драйверы. Учтите, что некоторые драйверы не позволяют останавливать себя.

09) Critical files (Критические файлы)

Этот раздел содержит информацию о файлах, критически необходимых для 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
[...]
```

Либо выбранные элементы будут удалены, либо будут восстановлены их исходные значения.

7.6.6.2.4.3 Выполнение сценариев службы

Пометьте все нужные объекты, сохраните и закройте сценарий. Запустите измененный сценарий непосредственно из главного окна ESET SysInspector с помощью команды **Запустить сценарий службы** в меню «Файл». При открытии сценария на экран будет выведено следующее сообщение: **«Выполнить сценарий службы "%Scriptname%"?»** После подтверждения может появиться еще одно предупреждение, сообщающее о попытке запуска неподписанного сценария. Для того чтобы запустить сценарий, нажмите кнопку **Запуск**.

В диалоговом окне будет подтверждено успешное выполнение сценария.

Если сценарий удалось обработать только частично, на экран будет выведено диалоговое окно с таким сообщением: **«Сценарий службы частично выполнен. Просмотреть отчет об ошибках?»** Для того чтобы просмотреть полный отчет об ошибках, в котором перечислены операции, нажмите кнопку **Да**.

Если сценарий не был распознан, на экран будет выведено диалоговое окно с таким сообщением: **«Выбранный сценарий службы не подписан. Выполнение неподписанных и неизвестных сценариев может привести к повреждению данных на компьютере. Выполнить сценарий и все действия?»** Это может быть связано с несоответствиями в сценарии (поврежден заголовок, повреждено название раздела, пропущена пустая разделительная строка и т. д.). В этом случае откройте файл сценария и исправьте ошибки или создайте новый сценарий службы.

7.6.6.2.5 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 под учетной записью обычного пользователя или пользователя с ограниченным доступом 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* в файл с именем «SysInpsector-%COMPUTERNAME%-ГГММДД-ЧЧММ.XML». Перед сохранением файла журнала можно изменить его местоположение и название.

Как просмотреть файл журнала ESET SysInspector?

Для просмотра файла журнала, созданного в ESET SysInspector, запустите программу и в главном окне выберите **Файл** > **Открыть журнал**. Файлы журнала также можно перетаскивать в окно приложения ESET SysInspector. Если вы часто просматриваете файлы журнала ESET SysInspector, рекомендуется создать на рабочем столе ярлык для файла SYSINSPECTOR.EXE. После этого просматриваемые файлы можно просто перетаскивать на этот ярлык. Из соображений безопасности в ОС Windows Vista/7 может быть не разрешено перетаскивать элементы между окнами, имеющими разные параметры 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. Возможно, мы выпустим их после выхода конечной версии программы в зависимости от отзывов пользователей и наличия интереса.

Как ESET SysInspector оценивает риск определенного объекта?

В большинстве случаев ESET SysInspector присваивает объектам (файлам, процессам, разделам реестра и т. п.) уровни риска, используя наборы эвристических правил, которые изучают характеристики каждого объекта и затем оценивают вероятность их вредоносного действия. На основе такого эвристического анализа объектам присваивается уровень риска от 1 — безопасно (зеленый) до 9 — опасно (красный). В панели навигации слева разделы окрашиваются в разные цвета в зависимости от самого высокого уровня риска содержащихся в них объектов.

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

Анализ ESET SysInspector не гарантирует, что какой-либо объект является вредоносным. Такая оценка должна выполняться специалистом по безопасности. Приложение ESET SysInspector разработано для того, чтобы специалист по безопасности имел возможность быстро оценить, какие объекты системы следует изучить и проверить их необычное поведение.

Зачем ESET SysInspector в ходе работы подключается к Интернету?

Как и многие приложения, решение ESET SysInspector подписано цифровой подписью («сертификатом»), которая гарантирует, что издателем данного программного обеспечения является компания ESET и оно не было изменено. Для проверки сертификата операционная система связывается с центром сертификации, чтобы подтвердить подлинность издателя программного обеспечения. Это нормальное поведение всех программ с цифровыми подписями в ОС Microsoft Windows.

Что такое технология Anti-Stealth?

Технология Anti-Stealth обеспечивает эффективное обнаружение руткитов.

Если система атакована злонамеренным кодом, который ведет себя как руткит, пользователь подвергается риску потери или хищения данных. Без специального инструмента для борьбы с руткитами обнаружить их практически невозможно.

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

При попытке идентифицировать цифровую подпись исполняемого файла ESET SysInspector сначала проверяет наличие в файле встроенной цифровой подписи. При ее обнаружении файл проверяется с помощью этой информации. В противном случае ESI начинает поиск соответствующего CAT-файла (в каталоге безопасности *%systemroot%\system32\catroot*), в котором содержатся сведения об обрабатываемом исполняемом файле. Если соответствующий CAT-файл найден, его цифровая подпись будет применена в процессе проверки исполняемого файла.

Поэтому иногда в некоторых файлах с пометкой «Подписано MS» имеется другая запись о названии компании.

7.6.6.2.6 ESET SysInspector как часть ESET File Security

Для того чтобы открыть ESET SysInspector в ESET File Security, в меню **Служебные программы** выберите пункт **ESET SysInspector**. В окне ESET SysInspector используется система управления, аналогичная той, которая применяется в окнах журналов сканирования компьютера и запланированных задач. Для выполнения всех операций со снимками системы (создание, просмотр, сравнение, удаление и экспорт) достаточно одного или двух щелчков мыши.

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

Для сравнения, создания и 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 выделенный снимок в файл, щелкните его правой кнопкой и выберите в контекстном меню пункт **Экспорт...**.

Далее приведено подробное описание доступных функций.

- **Сравнить**: позволяет сравнить два журнала. Эта функция удобна, если нужно найти различия между текущим и более старым журналом. Для сравнения необходимо выбрать два снимка состояния.
- **Создать...**: создание записи. Перед созданием записи нужно ввести краткий комментарий к ней. Ход создания формируемого в данный момент снимка отображается в столбце **Состояние**. Все уже созданные снимки имеют состояние **Создано**.
- **Удалить/Удалить все**: удаление записей из списка.
- **Экспорт...**: сохранение выделенной записи в файл в формате XML (также есть возможность создания заархивированной версии).

7.6.7 ESET SysRescue Live

ESET SysRescue Live — это утилита для создания загрузочного диска, содержащего одно из решений ESET Security: ESET NOD32 Antivirus, ESET Smart Security или какой-либо серверный продукт. Главным преимуществом ESET SysRescue Live является то, что решение ESET Security работает независимо от операционной системы компьютера, имея при этом 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.

7.6.8 Планировщик

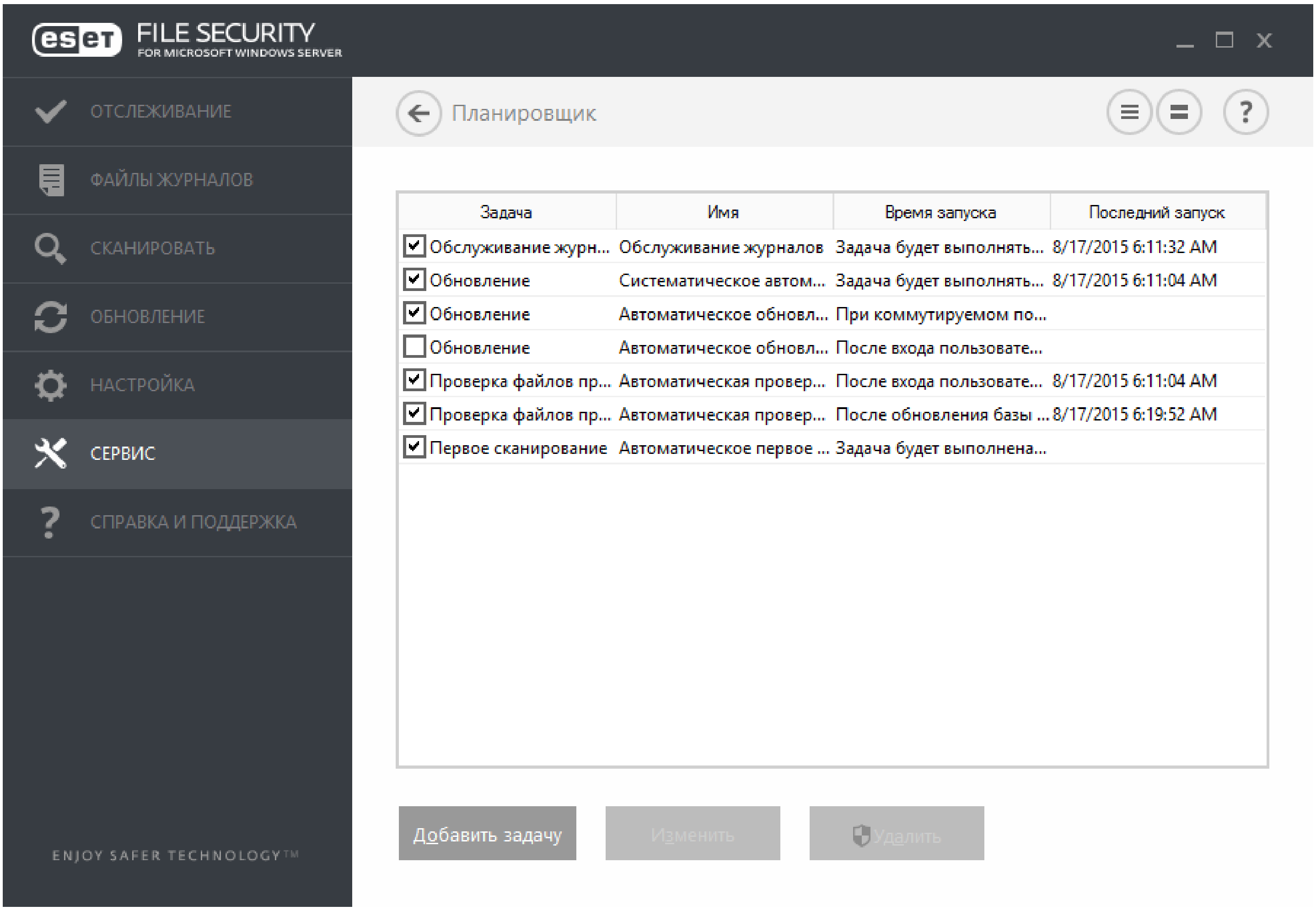
Планировщик доступен в разделе **Служебные программы** главного окна программы. С его помощью можно управлять запланированными задачами и запускать их выполнение согласно заданным параметрам.

Планировщик содержит список всех запланированных задач в форме таблицы, в которой отображаются их параметры, например тип **задачи**, ее **имя**, **время запуска** и **последний запуск**. Чтобы получить дополнительные сведения, щелкните задачу дважды. Отобразится окно Обзор запланированных задач. После установки в этом окне отображаются предварительно заданные задачи. Кроме того, вы можете создавать новые задачи с помощью кнопки Добавить задачу.

Щелкните задачу правой кнопкой мыши и укажите, какое действие нужно выполнить. Доступны такие действия:

- **Показать информацию о задаче**
- **Запустить сейчас**
- **Добавить...**
- **Изменить...**
- **Удалить**

Чтобы включить или отключить задачу, поставьте или снимите флажок напротив нее. Чтобы изменить параметры существующей запланированной задачи, щелкните ее правой кнопкой мыши и выберите команду **Изменить...** или выделите задачу, которую необходимо изменить, и нажмите кнопку **Изменить**.



По умолчанию запланированы такие задачи:

- **Обслуживание журнала**
- **Регулярное автоматическое обновление**
- **Автоматическое обновление после установки коммутируемого соединения**
- **Автоматическое обновление после входа пользователя в систему** (эта задача по умолчанию не активируется)
- **Автоматическая проверка файлов при запуске системы** (после входа пользователя в систему)

- **Автоматическая проверка файлов при запуске системы** (после успешного обновления базы данных сигнатур вирусов)
- **Автоматическое первое сканирование**

7.6.8.1 Добавление задачи в планировщике

Чтобы создать задачу в планировщике, нажмите кнопку **Добавить задачу** или щелкните правой кнопкой мыши и выберите в контекстном меню команду **Добавить**. Откроется мастер, с помощью которого вы можете создать запланированную задачу. Ниже представлены пошаговые инструкции.

1. Введите **имя задачи** и выберите в раскрывающемся меню нужный **тип задачи**.
   - **Запуск внешнего приложения** — планирование выполнения внешнего приложения.
   - **Обслуживание журналов** — в файлах журналов содержатся также 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 системы или входе пользователя в нее.
   - **Создать снимок состояния компьютера** — создание снимка состояния компьютера в решении ESET SysInspector, для которого собираются подробные сведения о компонентах системы (например, о драйверах и приложениях) и оценивается уровень риска для каждого из них.
   - **Сканирование компьютера по требованию** — сканирование файлов и папок на компьютере.
   - **Первое сканирование** — по умолчанию через 20 минут после установки или перезагрузки сканирование компьютера выполняется как задание с низким приоритетом.
   - **Обновление** — планирование задачи обновления, в рамках которой обновляются база данных сигнатур вирусов и программные модули.
   - **Сканирование Hyper-V** — планирование сканирования виртуальных дисков в Hyper-V.
2. Если нужно отключить задачу сразу после ее создания, щелкните переключатель возле элемента **Включено**. Вы можете активировать задачу позже, установив соответствующий флажок в представлении планировщика. Нажмите кнопку **Далее**.
3. Выберите, когда нужно **запускать запланированные задачи**:
   - **Однократно** — задача выполняется один раз в указанные дату и время.
   - **Многократно** — задача выполняется регулярно через указанный промежуток времени (в минутах).
   - **Ежедневно** — задача выполняется каждые сутки в указанное время.
   - **Еженедельно** — задача выполняется один или несколько раз в неделю в указанные дни и время.
   - **При определенных условиях** — задача выполняется при возникновении указанного события.
4. Если нужно, чтобы задача не запускалась тогда, когда устройство работает от аккумулятора (например, от источника бесперебойного питания), щелкните переключатель напротив элемента **Пропускать задачу, если устройство работает от аккумулятора**. Нажмите кнопку **Далее**.
5. Если задачу не удалось запустить в запланированное время, вы можете указать, когда ее нужно запустить.
   - **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**).
6. Нажмите кнопку **Далее**. В зависимости от типа задачи может понадобиться указать **сведения о задаче**. Сделав это, нажмите кнопку **Готово**. Новая запланированная задача отобразится в представлении планировщика.

7.6.9 Отправка образцов на анализ

Диалоговое окно отправки образцов позволяет отправить файл или сайт на анализ в ESET. Чтобы открыть это окно, последовательно выберите элементы **Сервис** > **Отправка образца на анализ**. При обнаружении на компьютере файла, проявляющего подозрительную активность, или подозрительного сайта в Интернете его можно отправить в вирусную лабораторию ESET. Если файл окажется вредоносным приложением или веб-сайтом, сигнатура для его обнаружения будет включена в последующие обновления.

Также можно отправить файл по электронной почте. Для этого заархивируйте файл с помощью программы наподобие WinRAR или WinZip, защитите архив паролем «infected» и отправьте архив на адрес samples@eset.com. Помните, что тема письма должна описывать проблему, а текст должен содержать как можно более полную информацию о файле (например, адрес веб-сайта, с которого он был загружен).

ПРИМЕЧАНИЕ.

Прежде чем отправлять образец в компанию ESET, убедитесь, что он соответствует как минимум одному из следующих критериев:
- файл или веб-сайт совсем не обнаруживается;
- файл или веб-сайт неправильно обнаруживается как угроза.

Ответ на подобное сообщение будет отправлен только в том случае, если для анализа потребуется дополнительная информация.

В раскрывающемся меню **Причина отправки образца** выберите наиболее подходящее описание своего сообщения:
- подозрительный файл;
- подозрительный сайт (веб-сайт, зараженный вредоносной программой);
- ложно обнаруженный файл (файл обнаружен как зараженный, хотя не является таковым);
- ложно обнаруженный сайт;
- другое.

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

Контактный 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 не обязательно. 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.

7.6.9.1 Подозрительный файл

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

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

Примечания и дополнительная информация: здесь можно ввести дополнительную информацию или описание, которые помогут идентифицировать подозрительный файл.

ПРИМЕЧАНИЕ.

Хоть требуется заполнять только первое поле (**Обнаруженные признаки и симптомы заражения вредоносной программой**), дополнительная информация является существенным подспорьем при идентификации образцов в лаборатории.

7.6.9.2 Подозрительный сайт

В раскрывающемся меню **Что не так с этим сайтом** выберите один из следующих пунктов.

- **Зараженный**: веб-сайт содержит вирусы или другие вредоносные программы, которые распространяются различными способами.
- **Фишинг**: часто используется для получения доступа к конфиденциальным сведениям, таким как номера банковских счетов, PIN-коды и т. п. Дополнительную информацию об этом типе атаки см. в глоссарии.
- **Мошеннический**: мошеннический веб-сайт.
- Выберите вариант **Другое**, если вышеуказанные варианты не соответствуют сайту, о котором вы собираетесь сообщить.

Примечания и дополнительная информация: здесь можно ввести дополнительную информацию или описание, которые помогут проанализировать подозрительный сайт.

7.6.9.3 Ложно обнаруженный файл

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

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

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

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

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

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

7.6.9.4 Ложно обнаруженный сайт

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

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

7.6.9.5 Другое

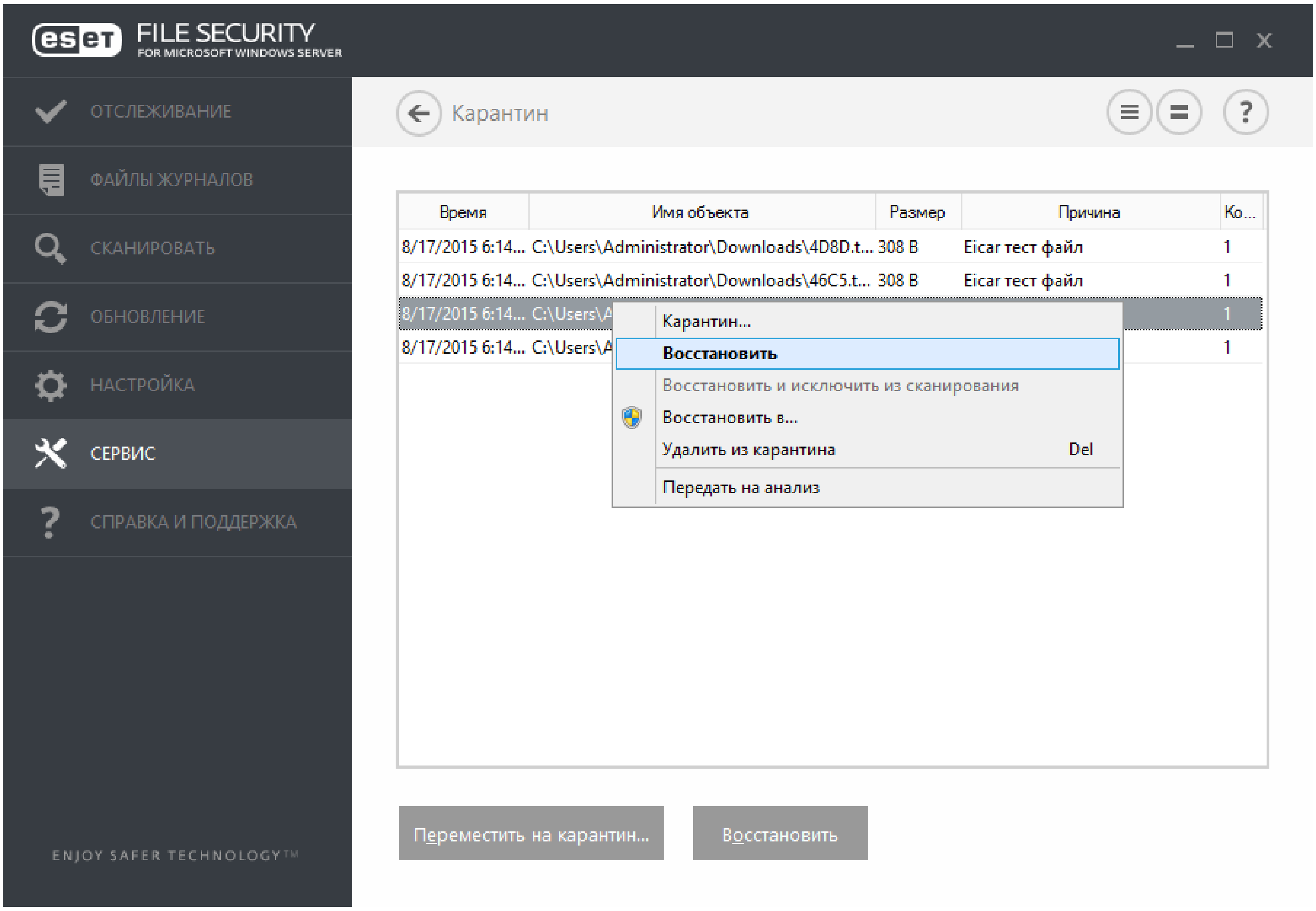
Этот вариант следует использовать, если файл невозможно отнести к категории **Подозрительный файл** или **Ложное срабатывание**.

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

7.6.10 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 File 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 вирусную лабораторию ESET на анализ.



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

Помещение файлов на карантин

Программа ESET File Security автоматически помещает удаленные файлы в 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 помещении на карантин файл удаляется из своего исходного расположения. Для этого также можно воспользоваться контекстным меню, щелкнув правой кнопкой мыши в окне **Карантин** и выбрав пункт **Карантин**.

Восстановление из карантина

Файлы, находящиеся на карантине, можно восстановить в исходном месте. Команда **Восстановить** доступна в контекстном меню, которое открывается правым щелчком мыши нужного файла в окне «Карантин». Если файл помечен как потенциально нежелательное приложение, будет доступен также пункт **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 процесса 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), а затем помещен на карантин, передайте файл в вирусную лабораторию ESET. Чтобы отправить файл из карантина, щелкните его правой кнопкой мыши и выберите пункт **Передать на анализ**.

7.7 Справка и поддержка

В ESET File Security есть средства для устранения проблем и информация по поддержке, которые помогут решить возможные проблемы.

Справка

- **Поиск в базе знаний ESET**: в базе знаний ESET содержатся ответы на наиболее часто задаваемые вопросы, а также рекомендуемые решения различных проблем. База знаний регулярно обновляется техническими специалистами ESET, что делает ее самым полезным инструментом для решения проблем.
- **Открыть справку**: нажмите эту ссылку, чтобы открыть страницы справки ESET File Security.
- **Найти быстрое решение**: выберите эту функцию, чтобы найти решения часто встречающихся проблем. Рекомендуется ознакомиться с этим разделом, прежде чем обращаться в службу технической поддержки.

Служба поддержки клиентов

- **Отправка запроса в службу поддержки**: если не удается найти ответ на вопрос, можно оперативно связаться со службой поддержки с помощью формы на веб-сайте компании ESET.

Средства поддержки

- **Энциклопедия угроз**: ссылка на энциклопедию угроз ESET, которая содержит информацию об опасностях и симптомах разных видов заражений.
- **Сборщик журналов ESET**: ссылка на страницу загрузки сборщика журналов ESET. Это приложение, которое автоматически собирает с сервера данные (например, конфигурацию и журналы) для ускорения решения проблем. Дополнительные сведения о сборщике журналов ESET см. в веб-справке.
- **Журнал базы данных сигнатур вирусов**: связан с вирусным радаром ESET, который содержит информацию о версиях базы данных сигнатур вирусов ESET.
- **Специализированное средство очистки ESET**: это средство очистки автоматически определяет и удаляет распространенные вредоносные заражения. Дополнительную информацию см. в этой статье базы знаний ESET.

Информация о продукте и лицензии

- **О программе ESET File Security**: на экран выводится информация о вашей копии программы ESET File Security.
- Активация продукта/Управление лицензией: щелкните, чтобы открыть окно активации продукта. Выберите доступный метод активации ESET File Security.

7.7.1 Рекомендации

Эта глава содержит ответы и решения для некоторых из наиболее частых вопросов и проблем пользователей. Нажмите ссылку, описывающую вашу проблему:

Обновление ESET File Security

Активация ESET File Security

Планирование задачи сканирования (каждые 24 часа)

Удаление вируса с сервера

Функционирование автоматических исключений

Если проблема отсутствует в перечисленных выше разделах справки, попробуйте выполнить поиск по ключевому слову или фразе, которые описывают эту проблему, или же поищите в справочной системе ESET File Security.

Если решение не удалось найти посредством поиска в справочной системе, обратитесь к регулярно обновляемой базе знаний ESET в Интернете.

При необходимости свяжитесь напрямую со службой технической поддержки, опишите свою проблему или задайте вопрос. Контактная форма находится на вкладке «Справка и поддержка» программы ESET.

7.7.1.1 Выполнение обновления ESET File Security

Обновлять ESET File Security можно вручную или автоматически. Чтобы запустить обновление, щелкните **Обновить сейчас**. Эта кнопка находится в разделе Обновление программы.

При установке программы с параметрами по умолчанию создается задача автоматического обновления. Она запускается каждый час. Изменить интервал обновления можно в служебной программе **Планировщик** (дополнительную информацию о планировщике см. по этой ссылке).

7.7.1.2 Активация ESET File Security

После завершения установки вам будет предложено активировать установленный продукт.

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

Чтобы активировать ESET File Security непосредственно из программы, щелкните в области уведомлений значок и выберите в меню пункт **Продукт не активирован**. Активацию продукта также можно выполнить, последовательно щелкнув в главном меню элементы **Справка и поддержка** > **Активировать продукт** или статус **Мониторинг** > **Продукт не активирован**.

Для активации ESET File Security можно воспользоваться любым из перечисленных ниже способов.

- **Лицензионный ключ** — уникальная строка в формате XXXX-XXXX-XXXX-XXXX-XXXX, которая используется для идентификации владельца и активации лицензии.
- **Администратор безопасности** — учетная запись, созданная на портале ESET License Administrator с использованием учетных данных (адрес электронной почты и пароль). Этот способ позволяет централизовано управлять несколькими лицензиями.
- **Офлайн-лицензия** - автоматически создаваемый файл со сведениями о лицензии, который передается в продукт ESET. Файл офлайн-лицензии создается на портале лицензирования и используется в средах, в которых приложение не может подключиться к центру лицензирования.
- Щелкните элемент **Активировать позже**, если компьютер является участником управляемой сети, и администратор выполнит удаленную активацию через программу ESET Remote Administrator. Этот параметр можно использовать и в тех случаях, когда нужно активировать клиент позже.

Чтобы управлять сведениями о лицензии, в главном окне программы последовательно щелкните элементы **Справка и поддержка** > **Управление лицензией**. Отобразится открытый идентификатор лицензии, используемый компанией ESET для идентификации продукта и лицензии. Имя пользователя, с помощью которого зарегистрирован компьютер, можно найти в разделе **О программе** (в области уведомлений щелкните значок правой кнопкой мыши).

ПРИМЕЧАНИЕ.
Используя предоставленные администратором лицензии, приложение ESET Remote Administrator может активировать клиентские компьютеры в автоматическом режиме.

7.7.1.3 Создание задачи в планировщике

Чтобы создать задачу в планировщике, нажмите кнопку **Добавить задачу** или щелкните правой кнопкой мыши и выберите в контекстном меню команду **Добавить**. Откроется мастер, с помощью которого вы можете создать запланированную задачу. Ниже представлены пошаговые инструкции.

1. Введите **имя задачи** и выберите в раскрывающемся меню нужный **тип задачи**.
   - **Запуск внешнего приложения** — планирование выполнения внешнего приложения.
   - **Обслуживание журналов** — в файлах журналов содержатся также 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 системы или входе пользователя в нее.
   - **Создать снимок состояния компьютера** — создание снимка состояния компьютера в решении ESET SysInspector, для которого собираются подробные сведения о компонентах системы (например, о драйверах и приложениях) и оценивается уровень риска для каждого из них.
   - **Сканирование компьютера по требованию** — сканирование файлов и папок на компьютере.
   - **Первое сканирование** — по умолчанию через 20 минут после установки или перезагрузки сканирование компьютера выполняется как задание с низким приоритетом.
   - **Обновление** — планирование задачи обновления, в рамках которой обновляются база данных сигнатур вирусов и программные модули.
   - **Сканирование Hyper-V** — планирование сканирования виртуальных дисков в Hyper-V.
2. Если нужно отключить задачу сразу после ее создания, щелкните переключатель возле элемента **Включено**. Вы можете активировать задачу позже, установив соответствующий флажок в представлении планировщика. Нажмите кнопку **Далее**.
3. Выберите, когда нужно **запускать запланированные задачи**:
   - **Однократно** — задача выполняется один раз в указанные дату и время.
   - **Многократно** — задача выполняется регулярно через указанный промежуток времени (в минутах).
   - **Ежедневно** — задача выполняется каждые сутки в указанное время.
   - **Еженедельно** — задача выполняется один или несколько раз в неделю в указанные дни и время.
   - **При определенных условиях** — задача выполняется при возникновении указанного события.
4. Если нужно, чтобы задача не запускалась тогда, когда устройство работает от аккумулятора (например, от источника бесперебойного питания), щелкните переключатель напротив элемента **Пропускать задачу, если устройство работает от аккумулятора**. Нажмите кнопку **Далее**.
5. Если задачу не удалось запустить в запланированное время, вы можете указать, когда ее нужно запустить.
   - **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**).
6. Нажмите кнопку **Далее**. В зависимости от типа задачи может понадобиться указать **сведения о задаче**. Сделав это, нажмите кнопку **Готово**. Новая запланированная задача отобразится в представлении планировщика.

7.7.1.4 Удаление вируса с сервера

Если компьютер проявляет признаки заражения вредоносной программой, например работает медленнее или часто зависает, рекомендуется выполнить следующие действия:

1. В главном окне ESET File Security нажмите **Сканирование компьютера**.

2. Нажмите **Сканирование Smart**, чтобы приступить к сканированию системы.

3. После завершения сканирования просмотрите журнал на предмет количества проверенных, зараженных и очищенных файлов.

4. Если необходимо проверить только часть диска, выберите вариант **Выборочное сканирование** и укажите объекты, которые следует просканировать на наличие вирусов.

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

7.7.1.5 Планирование задачи сканирования (каждые 24 часа)

Чтобы запланировать регулярную задачу, перейдите в раздел **ESET File Security** > **Сервис** > **Планировщик**. Описанные ниже действия помогут вам создать задачу для сканирования локальных дисков каждые 24 часа.

Чтобы запланировать задачу сканирования, выполните следующие действия:

1. Щелкните **Добавить задачу** на главном экране **Планировщик** и введите **Имя задачи**.
2. В раскрывающемся меню выберите **Сканирование компьютера по требованию**.
3. Если нужно отключить задачу сразу после ее создания, щелкните переключатель возле элемента **Включено**. Вы можете активировать задачу позже, установив соответствующий флажок в представлении планировщика.
4. Выберите для задачи планировщика режим повторения **Многократно**. Задача будет выполняться регулярно через указанный промежуток времени (1440 минут).
5. Если нужно, чтобы задача не запускалась тогда, когда устройство работает от аккумулятора (например, от источника бесперебойного питания), щелкните переключатель **Пропускать задачу, если устройство работает от аккумулятора**.
6. Нажмите кнопку **Далее**.
7. Выберите действие, которое будет выполняться, если по какой-либо причине не удается выполнить запланированную задачу.
   - **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**).
8. Нажмите кнопку **Далее**.
9. В раскрывающемся меню **Объекты** выберите пункт **Локальные диски**.
10. Для применения задачи нажмите кнопку **Готово**.

7.7.2 Отправка запроса в службу поддержки клиентов

Чтобы оказать помощь максимально быстро и эффективно, компании ESET требуется информация о конфигурации программы ESET File Security, подробные сведения о системе пользователя и выполняющихся процессах (файл журнала ESET SysInspector), а также данные реестра. Компания ESET использует эту информацию только для предоставления клиенту технической поддержки.

При отправке веб-формы будут отправлены и данные о конфигурации системы. Установите флажок **Всегда отправлять эти сведения**, чтобы запомнить это действие для данного процесса. Чтобы отправить форму, не отправляя данные, выберите вариант **Не отправлять данные**, и вы сможете обратиться в службу поддержки клиентов ESET с помощью онлайн-формы.

Этот параметр также можно настроить в окне **Дополнительные настройки** (нажмите клавишу **F5** на клавиатуре). Щелкните **Служебные программы** > **Диагностика** > **Служба поддержки**.

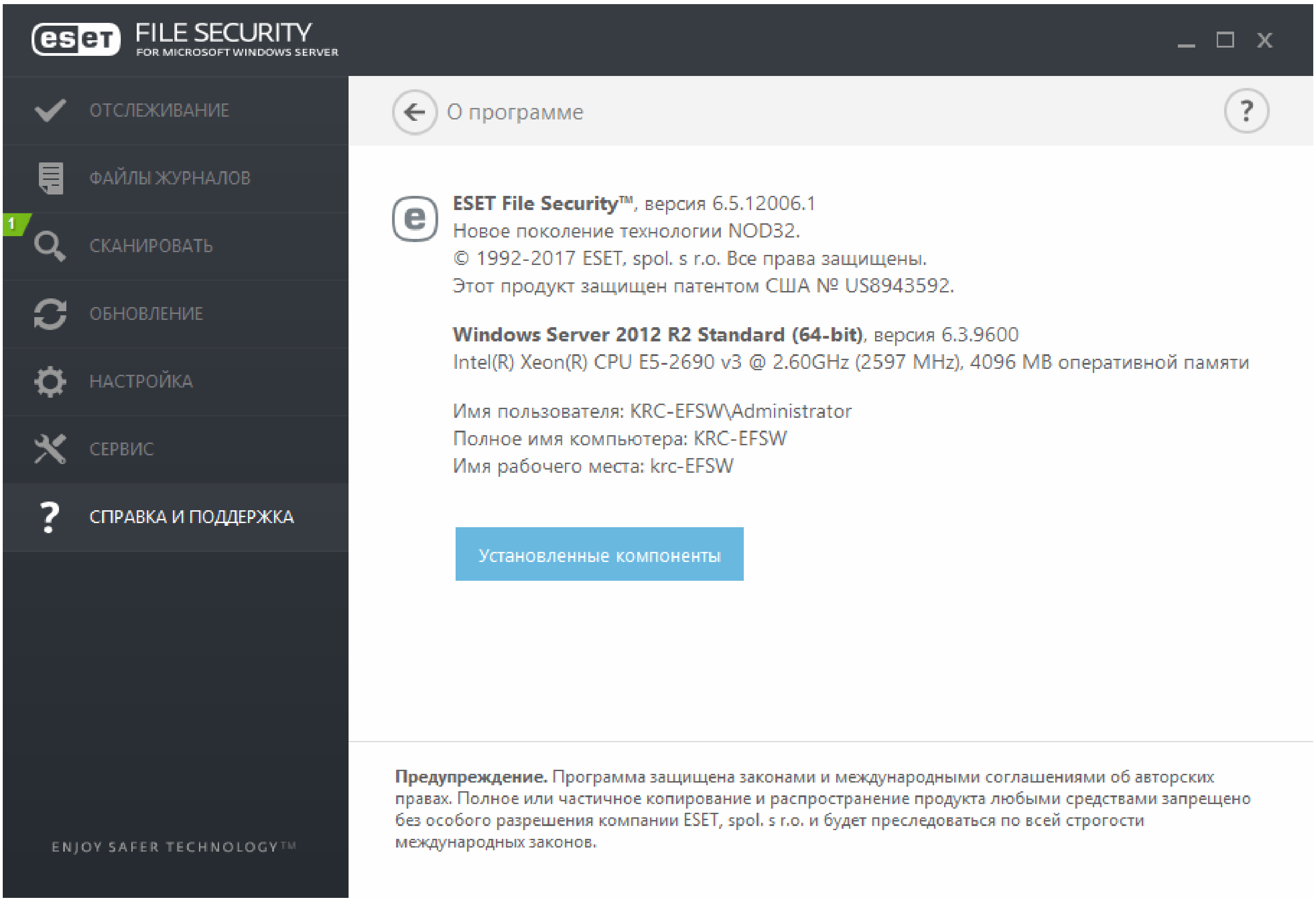
ПРИМЕЧАНИЕ.
Если вы решили отправить данные о системе, нужно заполнить и отправить веб-форму. Иначе запрос не будет создан и данные о системе будут потеряны.

7.7.3 Специализированное средство очистки ESET

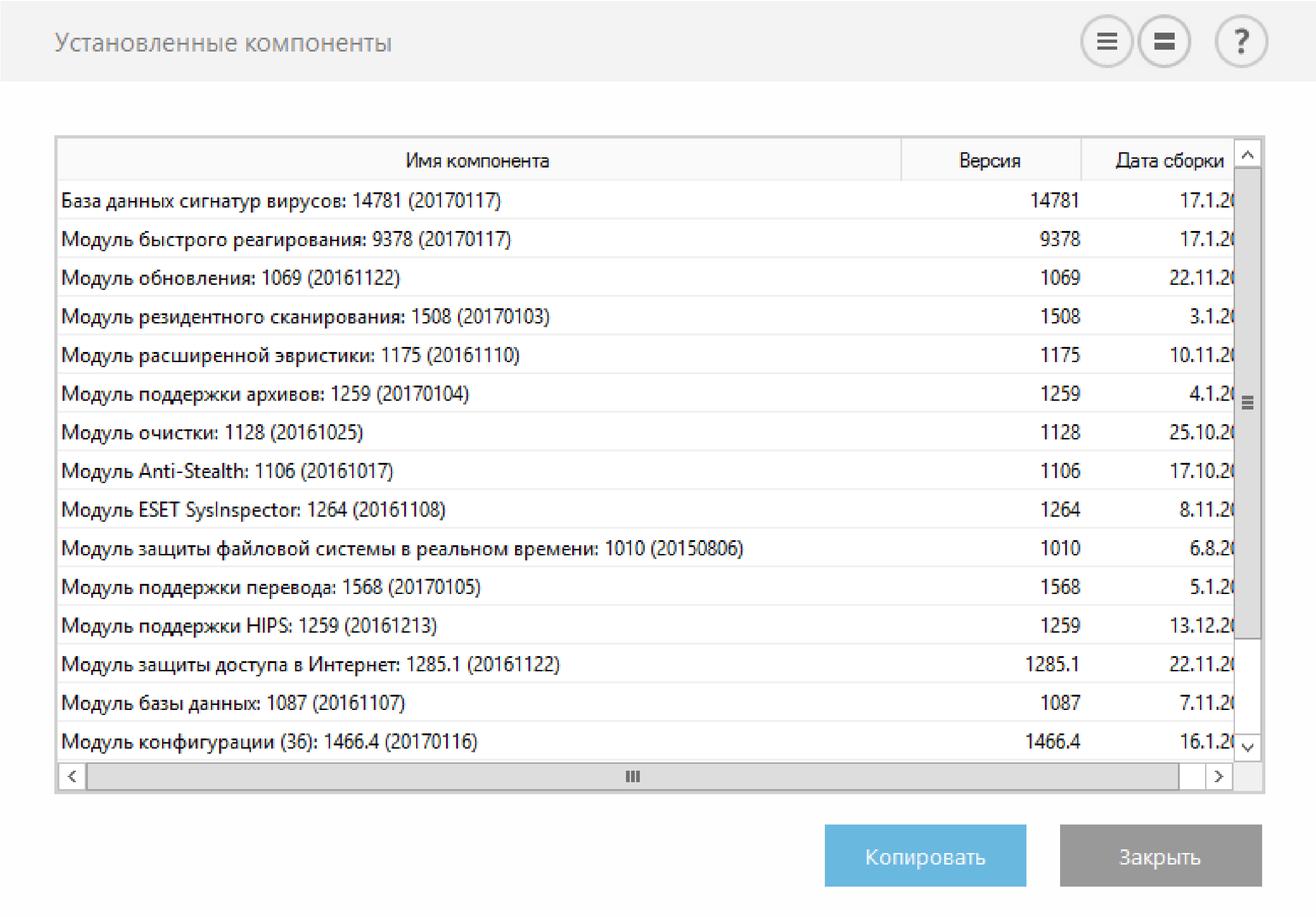
Специализированное средство очистки ESET предназначено для удаления распространенных вредоносных заражений, таких как Conficker, Sirefef или Necurs. Дополнительные сведения можно найти в этой статье базы знаний ESET.

7.7.4 О программе ESET File Security

В этом окне содержатся сведения об установленной версии ESET File Security. В верхней части окна содержится информация об операционной системе и системных ресурсах, а также о текущем пользователе и полном имени компьютера.



В разделе **Установленные компоненты** содержатся сведения о модулях. Щелкните **Установленные компоненты**, чтобы просмотреть список установленных компонентов и сведения о них. Щелкните **Копировать**, чтобы скопировать список в буфер обмена. Это может быть полезно при устранении проблем или обращении в службу технической поддержки.



Имя компонента	Версия	Дата сборки
База данных сигнатур вирусов: 14781 (20170117)	14781	17.1.2
Модуль быстрого реагирования: 9378 (20170117)	9378	17.1.2
Модуль обновления: 1069 (20161122)	1069	22.11.2
Модуль резидентного сканирования: 1508 (20170103)	1508	3.1.2
Модуль расширенной эвристики: 1175 (20161110)	1175	10.11.2
Модуль поддержки архивов: 1259 (20170104)	1259	4.1.2
Модуль очистки: 1128 (20161025)	1128	25.10.2
Модуль Anti-Stealth: 1106 (20161017)	1106	17.10.2
Модуль ESET SysInspector: 1264 (20161108)	1264	8.11.2
Модуль защиты файловой системы в реальном времени: 1010 (20150806)	1010	6.8.2
Модуль поддержки перевода: 1568 (20170105)	1568	5.1.2
Модуль поддержки HIPS: 1259 (20161213)	1259	13.12.2
Модуль защиты доступа в Интернет: 1285.1 (20161122)	1285.1	22.11.2
Модуль базы данных: 1087 (20161107)	1087	7.11.2
Модуль конфигурации (36): 1466.4 (20170116)	1466.4	16.1.2

7.7.5 Активация программы

После завершения установки вам будет предложено активировать установленный продукт.

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

Чтобы активировать ESET File Security непосредственно из программы, щелкните в области уведомлений значок и выберите в меню пункт **Продукт не активирован**. Активацию продукта также можно выполнить, последовательно щелкнув в главном меню элементы **Справка и поддержка** > **Активировать продукт** или статус **Мониторинг** > **Продукт не активирован**.

Для активации ESET File Security можно воспользоваться любым из перечисленных ниже способов.

- **Лицензионный ключ** — уникальная строка в формате XXXX-XXXX-XXXX-XXXX-XXXX, которая используется для идентификации владельца и активации лицензии.
- **Администратор безопасности** — учетная запись, созданная на портале ESET License Administrator с использованием учетных данных (адрес электронной почты и пароль). Этот способ позволяет централизовано управлять несколькими лицензиями.
- **Офлайн-лицензия** - автоматически создаваемый файл со сведениями о лицензии, который передается в продукт ESET. Файл офлайн-лицензии создается на портале лицензирования и используется в средах, в которых приложение не может подключиться к центру лицензирования.

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

Чтобы управлять сведениями о лицензии, в главном окне программы последовательно щелкните элементы **Справка и поддержка** > **Управление лицензией**. Отобразится открытый идентификатор лицензии, используемый компанией ESET для идентификации продукта и лицензии. Имя пользователя, с помощью которого зарегистрирован компьютер, можно найти в разделе **О программе** (в области уведомлений щелкните значок правой кнопкой мыши).

ПРИМЕЧАНИЕ.
Используя предоставленные администратором лицензии, приложение ESET Remote Administrator может активировать клиентские компьютеры в автоматическом режиме.

7.7.5.1 Регистрация

Зарегистрируйте лицензию, заполнив поля регистрационной формы и нажав кнопку **Продолжить**. Обязательны к заполнению поля, возле которых в скобках дано соответствующее указание. Данная информация будет использоваться только в целях, связанных с вашей лицензией ESET.

7.7.5.2 Активация администратора безопасности

Учетная запись администратора безопасности создается на портале лицензирования с указанием **адреса электронной почты** и **пароля**, и в этой учетной записи отображены все компьютеры с лицензией.

С помощью учетной записи **администратора безопасности** можно управлять несколькими лицензиями. Если у вас нет такой учетной записи, щелкните **Создать учетную запись**, и вы окажетесь на веб-странице администраторов лицензии ESET, на которой можно зарегистрироваться со своими учетными данными.

Если вы забыли пароль, нажмите **Восстановление пароля**, и система перенаправит вас на бизнес-портал ESET. Введите адрес электронной почты и щелкните **Передать** для подтверждения. Вам будет отправлено сообщение с указаниями по сбросу пароля.

ПРИМЕЧАНИЕ.
Чтобы узнать подробнее об использовании ESET License Administrator, см. руководство пользователяESET License Administrator.

7.7.5.3 Сбой активации

Не удалось выполнить активацию ESET File Security. Убедитесь, что введен правильный **лицензионный ключ** или вложена **офлайн-лицензия**. Если у вас есть другая **офлайн-лицензия**, введите ее снова. Чтобы проверить введенный лицензионный ключ, щелкните элемент **Перепроверить лицензионный ключ**. Чтобы перейти на нашу веб-страницу, на которой можно купить лицензию, щелкните элемент **Приобрести лицензию**.

7.7.5.4 Лицензия

При активации администратора безопасности отобразится запрос, и нужно будет выбрать лицензию, связанную с учетной записью, которая будет использоваться для ESET File Security. Щелкните **Активировать**, чтобы продолжить.

7.7.5.5 Ход выполнения активации

Продукт ESET File Security активируется. Подождите. Эта процедура может занять некоторое время.

7.7.5.6 Активация выполнена

Продукт ESET File Security успешно активирован. Теперь ESET File Security будет регулярно загружать обновления, следить за безопасностью компьютера и устранять все известные угрозы. Чтобы завершить активацию продукта, нажмите кнопку **Готово**.

8. Работа с ESET File Security

В окне **Дополнительные настройки** можно настраивать параметры в соответствии со своими потребностями. В меню слева можно выбрать следующие категории:

- Защита от вирусов: включение и выключение обнаружения потенциально нежелательных, небезопасных и подозрительных приложений, указание исключений, защита файловой системы в режиме реального времени, сканирование компьютера по требованию, сканирование Hyper-V и т. д.
- Обновление: настройка списка профилей, создание снимков файла обновления, информация об источниках обновления, например сведения о серверах обновления и данные аутентификации для них.
- Интернет и электронная почта: настройка защиты почтового клиента, фильтрации протоколов, защиты доступа в Интернет и т. д.
- Контроль устройств: настройка правил и групп для функции контроля устройств.
- Служебные программы: настройка служебных программ, например ESET LiveGrid, файлов журнала, прокси-сервера, кластера и т. д.
- Интерфейс: настройка поведения графического интерфейса программы, состояний, сведений о лицензии и т. д.

Если щелкнуть элемент (категорию или подкатегорию) в меню слева, параметры, соответствующие этому элементу, отображаются на правой вкладке.

8.1 Защита от вирусов

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

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

- **Потенциально нежелательные приложения** не всегда являются вредоносными, однако могут негативно повлиять на производительность компьютера. Дополнительную информацию о приложениях этого типа см. в глоссарии.
- **Потенциально опасные приложения**: это определение относится к законному коммерческому программному обеспечению, которое может быть использовано для причинения вреда. К потенциально опасным приложениям относятся средства удаленного доступа, приложения для взлома паролей и клавиатурные шпионы (программы, регистрирующие каждое нажатие пользователем клавиш на клавиатуре). По умолчанию этот параметр отключен. Дополнительную информацию о приложениях этого типа см. в глоссарии.
- **Потенциально подозрительные приложения** — к ним относятся программы, сжатые при помощи упаковщиков или средств защиты. Злоумышленники часто используют такие средства защиты, чтобы избежать обнаружения.

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

Исключения для процессов — эта функция позволяет исключить конкретные процессы. Например, если исключить процессы в решении резервного копирования, то все те операции с файлами, которые касаются исключенных процессов, игнорируются и считаются безопасными. Таким образом факторы, мешающие резервному копированию, сводятся к минимуму.

Исключения позволяют исключить из сканирования файлы и папки. Чтобы на наличие угроз сканировались все объекты, исключения рекомендуется создавать 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.

8.1.1 Действия при обнаружении заражения

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

Стандартное поведение

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

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

Каждый модуль использует стандартный уровень очистки и пытается очистить файл, поместить его в карантин или прервать подключение. Окно уведомлений отображается в области уведомлений в правом нижнем углу экрана. 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 программа сначала пытается очистить зараженный файл, чтобы восстановить его первоначальное состояние до очистки. Если файл содержит только вредоносный код, он будет удален.

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

Множественные угрозы

Если какие-либо зараженные файлы при сканировании компьютера не были очищены (или был выбран уровень очистки **Без очистки**), на экран будет выведено окно предупреждения, в котором пользователю предлагается выбрать действие для таких файлов. Выберите для каждой угрозы, приведенной в списке, отдельное действие или с помощью параметра **Выберите, что нужно сделать с каждой из приведенных угроз** выберите одно действие для всех угроз, приведенных в списке, и щелкните **Выполнить**.

Удаление файлов из архивов

В режиме очистки по умолчанию архив удаляется целиком, только если он содержит лишь 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 File Security и выберите команду «Сканирование компьютера».
- Выберите вариант **Сканирование Smart** (дополнительную информацию см. в разделе Сканирование компьютера).
- После окончания сканирования проверьте в журнале количество просканированных, зараженных и очищенных файлов.

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

8.1.2 Исключения для процессов

Эта функция позволяет исключить процессы приложений только из сканирования на наличие вирусов при доступе. Исключения помогают свести к минимуму риск возможных конфликтов и улучшить производительность исключенных приложений, что, в свою очередь, повышает общую производительность операционной системы.

Когда процесс исключен, мониторинг его исполняемого файла не выполняется. Программа ESET File Security не контролирует активность исключенного процесса. Не сканируются также и операции с файлами, которые выполняет процесс.

Используйте кнопки **Добавить, Изменить** и **Удалить**, чтобы управлять исключениями для процессов.

ПРИМЕР

Защита доступа в Интернет не учитывает эти исключения. Поэтому если исключить исполняемый файл веб-браузера, загружаемые файлы все равно будут сканироваться. То есть заражения все же можно обнаружить. Этот сценарий — всего лишь пример. Не рекомендуется создавать исключения для веб-браузеров.

ПРИМЕЧАНИЕ.

Система HIPS используется для оценки исключенных процессов, поэтому недавно исключенные процессы рекомендуется проверять, когда система HIPS включена (или, если возникли проблемы, отключена). Отключение системы HIPS не затрагивает исключения для процессов. Если система HIPS отключена, то исключенные процессы идентифицируются только по пути.

8.1.3 Автоматические исключения

Разработчики серверных приложений и операционных систем рекомендуют исключать наборы критических рабочих файлов и папок из антивирусного сканирования для большинства таких программных продуктов. Антивирусное сканирование может отрицательно повлиять на производительность сервера, что может привести к конфликтам и даже не дать некоторым приложениям работать на сервере. Исключения помогают свести к минимуму риск возможных конфликтов и улучшить общую производительность сервера при работе программного обеспечения защиты от вирусов.

Программа ESET File Security выявляет критические файлы серверных приложений и серверных операционных систем и автоматически добавляет их в список Исключения. Список обнаруженных серверных приложений, для которых были созданы исключения, отображается под заголовком **Автоматические исключения, которые необходимо создать**. По умолчанию все автоматические исключения активированы. Чтобы активировать или деактивировать исключение для любого серверного приложения, щелкните переключатель. Последствия каждого действия приведены ниже.

- Если исключение для приложения или операционной системы остается активированным, все соответствующие критические файлы и папки будут добавлены в список файлов, исключенных из сканирования (**Дополнительные настройки** > **Защита от вирусов** > **Основное** > **Исключения** > **Изменить**). При каждом перезапуске сервера система автоматически проверяет исключения и восстанавливает все исключения, которые могли быть удалены из списка. Это рекомендуемая настройка, которая позволяет обеспечить постоянное применение рекомендуемых автоматических исключений.

- Если деактивировать исключение для приложения или операционной системы, соответствующие критические файлы и папки остаются в списке файлов, исключенных из сканирования (**Дополнительные настройки** > **Защита от вирусов** > **Основное** > **Исключения** > **Изменить**). Однако они не будут автоматически проверяться и восстанавливаться в списке **Исключения** при каждом перезапуске сервера (см. пункт 1 выше). Эту настройку рекомендуется применять только опытным пользователям, которым нужно удалить или изменить какие-либо из стандартных исключений. Если нужно удалить исключения из списка без перезапуска сервера, их следует удалить вручную (**Дополнительные настройки** > **Защита от вирусов** > **Основное** > **Исключения** > **Изменить**).

Описанные выше настройки никак не влияют на пользовательские исключения, введенные вручную (**Дополнительные настройки** > **Защита от вирусов** > **Основное** > **Исключения** > **Изменить**).

8.1.4 Общий локальный кэш

Общий локальный кэш ESET повышает производительность в виртуализированных средах, запрещая повторяющееся сканирование в сети. Благодаря этому каждый файл сканируется только один раз, а затем сохраняется в общем кэше.

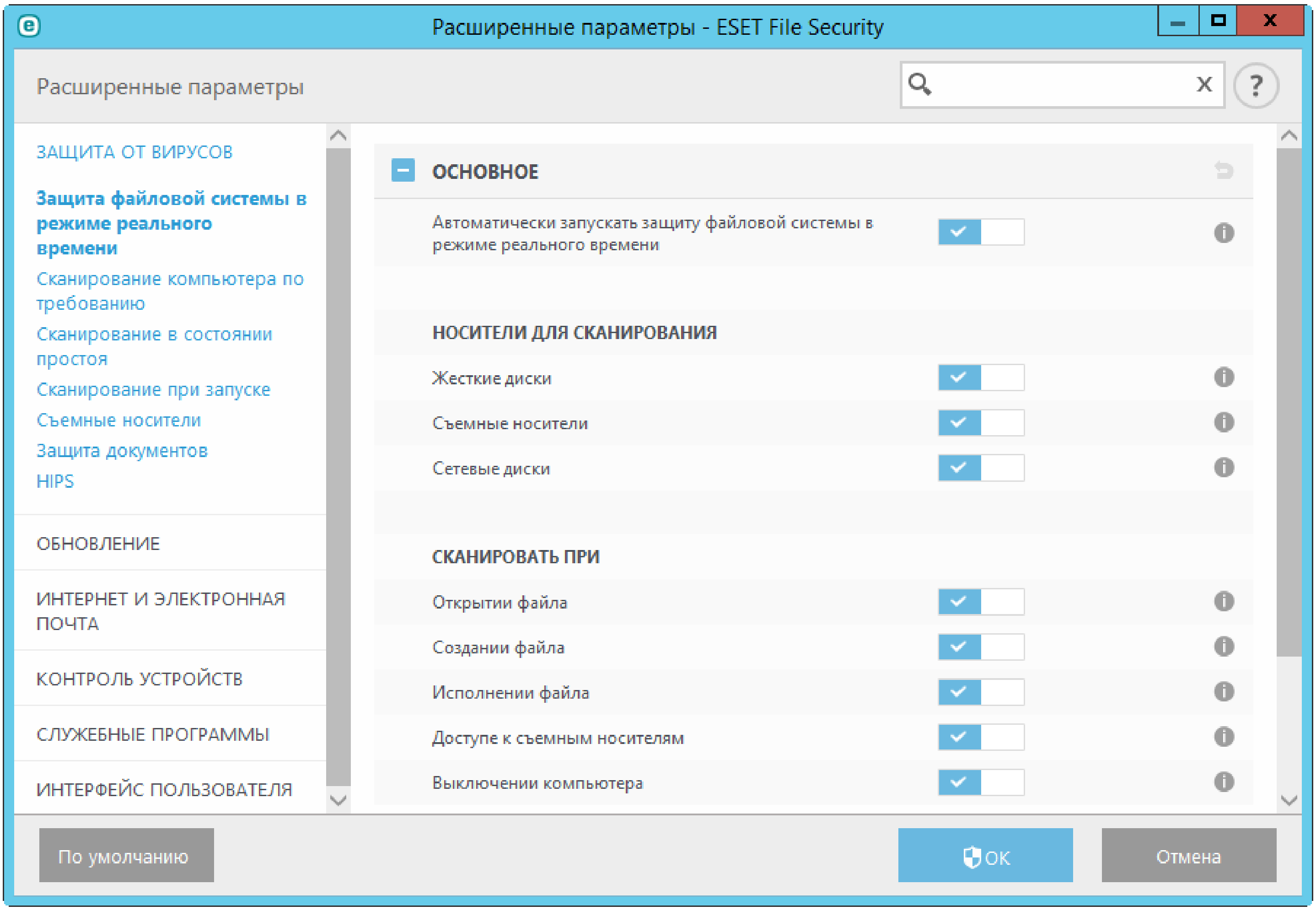
Чтобы сохранять данные о сканировании файлов и папок в сети в локальный кэш, включите переключатель **Параметры кэширования**. При следующем сканировании продукт ESET File Security будет искать сканируемые файлы в кэше Если файлы совпадают, они будут исключены из сканирования.

При настройке **сервера кэширования** нужно работать с указанными ниже параметрами:

- **Имя хоста** — имя или IP-адрес компьютера, на котором расположен кэш.
- **Порт** — номер порта, используемого для передачи данных (такой же, какой указан для общего локального кэша).
- **Пароль** — пароль общего локального кэша (если понадобится).

8.1.5 Защита файловой системы в режиме реального времени

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



По умолчанию функция защиты файловой системы в реальном 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 дополнительных настроек 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 на наличие возможных угроз сканируются все типы носителей.

- **Жесткие диски** — контролируются все жесткие диски системы.
- **Съемные носители** — контролируются компакт-/DVD-диски, USB-накопители, 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 реальном времени проверяет все типы носителей, и ее могут запустить различные системные события, например получение доступа к файлу. За счет использования способов 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 реальном времени так, чтобы она более тщательно отслеживала вновь созданные файлы.

Чтобы уменьшить влияние на производительность компьютера при использовании защиты в реальном времени, файлы, которые уже сканировались, не сканируются повторно (если с момента последнего сканирования они не были изменены). Файлы сканируются повторно сразу после каждого обновления базы данных сигнатур вирусов. Такое поведение контролируется с помощью **оптимизации Smart**. Если оптимизация Smart отключена, все файлы сканируются при каждом получении доступа к ним. Чтобы изменить этот параметр, нажмите клавишу **F5**. Откроется раздел дополнительных настроек и будут развернуты элементы **Защита от вирусов** > **Защита файловой системы в реальном времени**. Последовательно щелкните элементы **Параметры ThreatSense** > **Другое** и снимите или установите флажок **Включить интеллектуальную оптимизацию**.

8.1.5.1 Исключения

Исключения позволяют исключить из сканирования файлы и папки. Чтобы на наличие угроз сканировались все объекты, исключения рекомендуется создавать только в случае крайней необходимости. Ситуации, в которых может понадобиться создать исключение, — это, например, сканирование больших баз данных, которые замедляют работу, или программ, конфликтующих с процессом сканирования (например, программное обеспечение для резервного копирования).

ВНИМАНИЕ!
Не следует путать с разделом Исключенные расширения**.**

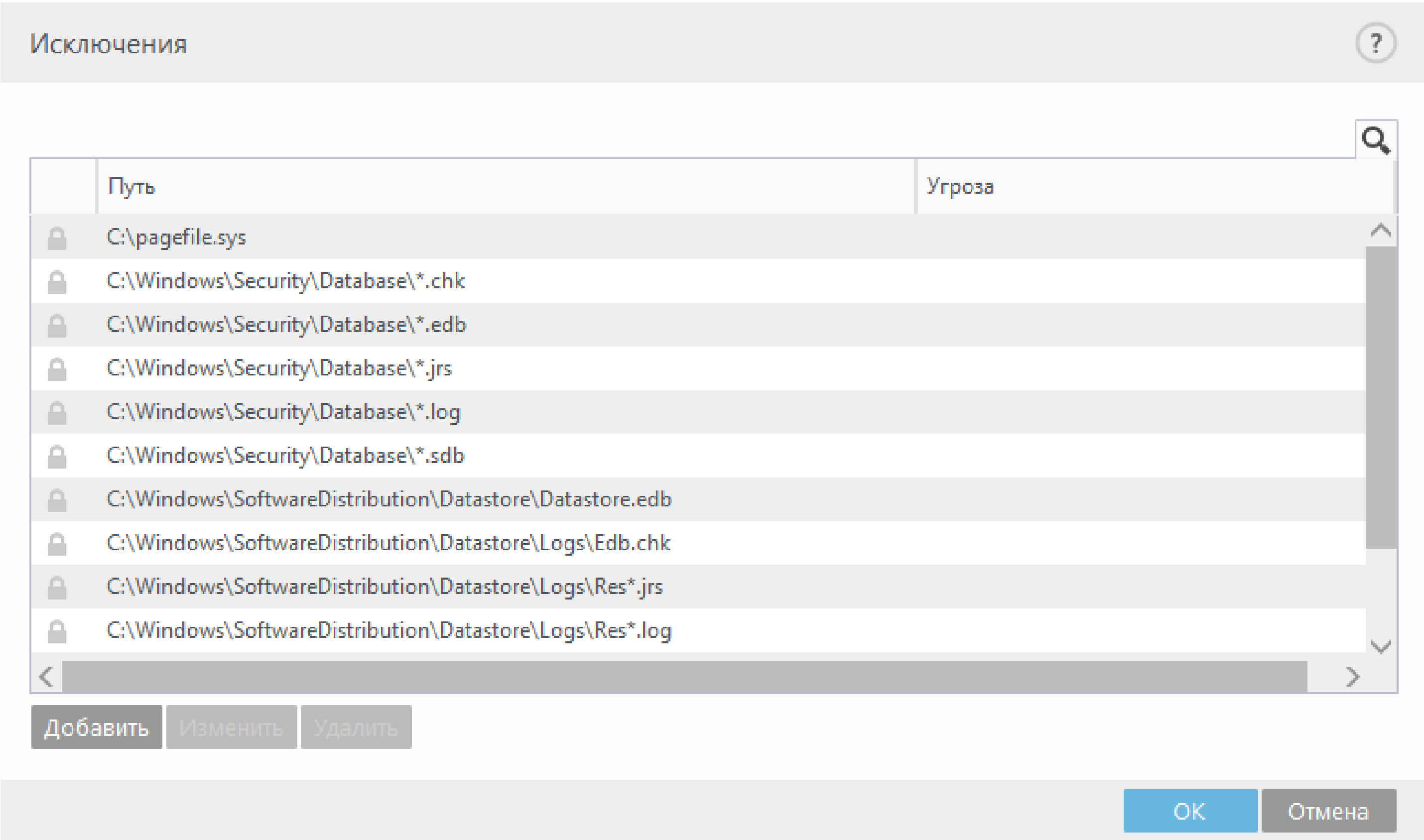
Для исключения объекта из сканирования выполните следующие действия.

Щелкните элемент Добавить и введите путь к объекту или выберите его в древовидной структуре.

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

ПРИМЕР

- Если нужно исключить все файлы в папке, следует ввести путь к папке и использовать маску «*.*».
- 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 наверняка известна только первая буква имени (например, «D»), следует использовать следующий формат: «D????.*exe*». Вопросительные знаки замещают отсутствующие (неизвестные) символы.



ПРИМЕЧАНИЕ.
Модуль защиты файловой системы в режиме реального времени и модуль сканирования компьютера не обнаружат угрозу в файле, если он соответствует критериям исключения из сканирования.

Столбцы

Путь — путь к файлам и папкам, исключенным из сканирования.
Угроза — если рядом с исключаемым файлом указано имя угрозы, это значит, что файл сканируется на наличие всех угроз, кроме этой. Если впоследствии этот файл заразит другая вредоносная программа, модуль защиты от вирусов ее обнаружит. Этот тип исключений можно использовать только для определенных типов заражений. Создать такое исключение можно либо в окне предупреждения об угрозе, в котором сообщается о заражении (последовательно щелкните элементы **Показать параметры** > **Исключить из проверки**), либо в разделе **Служебные программы** > **Карантин**, щелкнув правой кнопкой мыши файл на карантине и выбрав в контекстном меню пункт **Восстановить и исключить из сканирования**.

Элементы управления

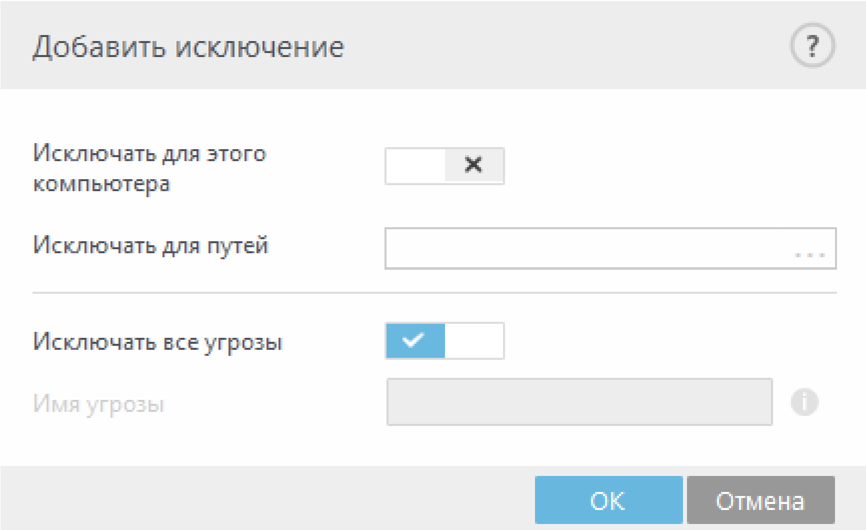
Добавить — исключение объектов из обнаружения.
Изменить — изменение выделенных записей.
Удалить — удаление выделенных записей.

8.1.5.1.1 Добавление или изменение исключений

В этом диалоговом окне можно добавить или изменить исключения. Это может быть выполнено двумя способами:

- посредством указания пути к объекту, который необходимо исключить;
- выбором объекта в древовидной структуре (щелкните элемент **...** в конце текстового поля, чтобы открыть функцию обзора).

В первом случае можно использовать подстановочные знаки, описанные в разделе Формат исключений.



Исключать для этого компьютера/Исключать для путей: исключение конкретных угроз или конкретного пути для этого компьютера. Если включены оба параметра, вы не сможете создать исключение.

Исключать все угрозы/Имя угрозы: исключения применяются к потенциально нежелательным, потенциально небезопасным и подозрительным приложениям.

8.1.5.1.2 Формат исключений

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

ПРИМЕР

- Если нужно исключить все файлы в папке, следует ввести путь к папке и использовать маску «*.*».
- 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 наверняка известна только первая буква имени (например, «D»), следует использовать следующий формат: «D????.*exe*». Вопросительные знаки замещают отсутствующие (неизвестные) символы.

8.1.5.2 Параметры ThreatSense

ThreatSense — это технология, состоящая из множества сложных способов обнаружения угроз. Это упреждающая технология, т. е. она защищает от новой угрозы уже в начале ее распространения. При этом используются: анализ и эмуляция кода, универсальные сигнатуры и сигнатуры вирусов. Вместе все эти средства значительно повышают уровень безопасности компьютера. Модуль сканирования может контролировать несколько потоков данных одновременно, что делает количество обнаруживаемых угроз и эффективность максимальными. Кроме того, технология ThreatSense успешно уничтожает руткиты.

ПРИМЕЧАНИЕ.
Сведения об автоматической проверке файлов при запуске см. в разделе Сканирование при запуске.

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 элемент **Настройка параметров модуля ThreatSense** в окне **Дополнительные настройки** любого модуля, использующего технологию ThreatSense (см. ниже). Для разных сценариев обеспечения безопасности могут требоваться различные конфигурации. Поэтому технологию ThreatSense можно настроить отдельно для каждого из перечисленных далее модулей защиты.

- Сканирование с помощью Hyper-V
- Защита файловой системы в режиме реального времени
- Сканирование в состоянии простоя
- Сканирование файлов, исполняемых при запуске системы
- Защита документов
- Защита почтового клиента
- Защита доступа в Интернет

Параметры ThreatSense хорошо оптимизированы для каждого из модулей, а их изменение значительно влияет на поведение системы. Например, если настроить сканирование программ сжатия исполняемых файлов или включить расширенную эвристику в модуле защиты файловой системы в реальном времени, работа системы может замедлиться (обычно только новые файлы сканируются с применением этих способов). Рекомендуется не изменять параметры ThreatSense по умолчанию ни для каких модулей, кроме модуля «Сканирование компьютера».

Сканируемые объекты

В этом разделе можно указать компоненты и файлы компьютера, которые будут сканироваться на наличие заражений.

- **Оперативная память** — выполняется сканирование на наличие угроз, которые атакуют оперативную память системы.
- **Загрузочные секторы**: загрузочные секторы сканируются на наличие вирусов в основной загрузочной записи. Основная загрузочная запись диска виртуальной машины Hyper-V сканируется в режиме только для чтения.
- **Почтовые файлы** — программа поддерживает расширения DBX (Outlook Express) и EML.
- **Архивы** — программа поддерживает расширения ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE и многие другие.
- **Самораспаковывающиеся архивы** — самораспаковывающиеся архивы (файлы с расширением SFX) — это архивы, которым для распаковки не нужны специальные программы.
- **Программы сжатия исполняемых файлов** — в отличие от стандартных типов архивов, программы сжатия, будучи выполненными, распаковываются в память. Благодаря эмуляции кода модуль сканирования распознает не только стандартные статические программы сжатия (UPX, yoda, ASPack, FGS и т. д.), но и множество других типов таких программ.

Параметры сканирования

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

- **Эвристический анализ** — анализ вредоносной активности программ с помощью специального алгоритма. Главным достоинством этого метода является способность идентифицировать вредоносные программы, сведения о которых отсутствуют в существующей базе данных сигнатур вирусов.

- **Расширенный эвристический анализ/сигнатуры распределенных сетевых атак**: для расширенного эвристического анализа используется уникальный эвристический алгоритм компании ESET, который оптимизирован для обнаружения компьютерных червей и троянских программ и написан на высокоуровневых языках программирования. Использование расширенной эвристики значительным образом увеличивает возможности продуктов ESET по обнаружению угроз. С помощью сигнатур осуществляется точное обнаружение и идентификация вирусов. Система автоматического обновления обеспечивает наличие новых сигнатур через несколько часов после обнаружения угрозы. Недостатком же сигнатур является то, что они позволяют обнаруживать только известные вирусы (или их незначительно модифицированные версии).

Очистка

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

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

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

Тщательная очистка: программа очищает или удаляет все зараженные файлы. Исключение составляют только системные файлы. Если очистить файл невозможно, программа предложит пользователю выбрать, какое действие следует выполнить.

ВНИМАНИЕ!
Если в архиве содержатся зараженные файлы, существует два варианта его обработки. В режиме по умолчанию (**Обычная очистка**) архив удаляется целиком, если все файлы в нем заражены. В режиме **Тщательная очистка** архив удаляется, если он содержит по крайней мере один зараженный файл, независимо от состояния остальных файлов.

ВАЖНО!
Если узел Hyper-V работает под управлением Windows Server 2008 R2, не поддерживаются варианты **Обычная очистка** и **Тщательная очистка**. Сканирование дисков виртуальной машины выполняется в режиме только для чтения, очистка не производится. Какой бы уровень очистки ни был выбран, сканирование всегда выполняется в режиме только для чтения.

Исключения

Расширением называется часть имени файла, отделенная от основной части точкой. Оно определяет тип файла и его содержимое. Этот раздел параметров модуля ThreatSense позволяет определить типы файлов, которые не нужно сканировать.

Другое

При настройке модуля ThreatSense также доступны представленные ниже параметры раздела **Другое**.

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

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

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

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

- **Сохранить отметку о времени последнего доступа**: установите этот флажок, чтобы сохранить исходное значение времени доступа к сканируемым файлам, а не обновлять их (например, для использования с системами резервного копирования данных).

Ограничения

В разделе «Ограничения» можно указать максимальный размер объектов и уровни вложенности архивов для сканирования.

Параметры объектов

Параметры объектов по умолчанию — включите для использования настроек по умолчанию (без ограничений). ESET File Security будет игнорировать пользовательские настройки.

- **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 больших объектов из сканирования. Значение по умолчанию: *не ограничено*.

- **Максимальное время сканирования, в секундах** — определяет максимальное значение времени сканирования объекта. Если значение здесь укажет пользователь, модуль защиты от вирусов прекратит сканирование объекта по истечении указанного времени вне зависимости от того, было ли сканирование завершено. Значение по умолчанию: *не ограничено*.

Настройки сканирования архивов

Уровень вложенности архивов: определяет максимальную глубину проверки архивов. Значение по умолчанию: *10*. Для объектов, обнаруженных защитой почтового транспорта, фактическая глубина вложенности составляет +1 уровень, поскольку архив, вложенный в почтовое сообщение, считается первым уровнем. Например, если указан уровень вложенности 3, файл архива с уровнем вложенности 3 будет сканироваться на транспортном уровне только до фактического уровня 2. Поэтому, если необходимо сканировать архивы защитой почтового транспорта до уровня 3, установите для параметра **Уровень вложенности архивов** значение 4.

Максимальный размер файла в архиве — этот параметр позволяет задать максимальный размер файлов в архиве (при их извлечении), которые должны сканироваться. Значение по умолчанию: *не ограничено*.

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

8.1.5.2.1 Исключенные из сканирования расширения файлов

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

По умолчанию сканируются все файлы. Любое расширение можно добавить в список файлов, исключенных из сканирования.

Может быть необходимо исключить определенное файловое расширение, если сканирование файлов, принадлежащих к определенным типам, препятствует нормальной работе программы, которая использует соответствующие расширения. Например, может быть целесообразно исключить расширения `.edb`, `.eml` и `.tmp` при использовании серверов Microsoft Exchange.

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

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

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

8.1.5.2.2 Дополнительные параметры ThreatSense

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

Дополнительную информацию о **программах сжатия исполняемых файлов**, **самораспаковывающихся архивах** и **расширенном эвристическом анализе** см. в разделе о настройках параметров модуля ThreatSense.

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

8.1.5.2.3 Уровни очистки

Защита в реальном времени предусматривает три уровня очистки. Для доступа к ним в разделе **Защита файловой системы в реальном времени** выберите элемент **Параметры ThreatSense**. Выберите в раскрывающемся списке требуемый уровень очистки.

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

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

Тщательная очистка: программа очищает или удаляет все зараженные файлы. Исключение составляют только системные файлы. Если очистить файл невозможно, программа предложит пользователю выбрать, какое действие следует выполнить.

ВНИМАНИЕ!
Если в архиве содержатся зараженные файлы, существует два варианта его обработки. В режиме по умолчанию (**Обычная очистка**) архив удаляется целиком, если все файлы в нем заражены. В режиме **Тщательная очистка** архив удаляется, если он содержит по крайней мере один зараженный файл, независимо от состояния остальных файлов.

ВАЖНО!
Если узел Hyper-V работает под управлением Windows Server 2008 R2, не поддерживаются варианты **Обычная очистка** и **Тщательная очистка**. Сканирование дисков виртуальной машины выполняется в режиме только для чтения, очистка не производится. Какой бы уровень очистки ни был выбран, сканирование всегда выполняется в режиме только для чтения.

8.1.5.2.4 Момент изменения конфигурации защиты в режиме реального времени

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

После установки ESET File Security все параметры оптимизированы для максимальной защиты системы. Чтобы восстановить параметры по умолчанию, щелкните возле каждой вкладки в окне (**Дополнительные настройки** > **Защита от вирусов** > **Защита файловой системы в режиме реального времени**).

8.1.5.2.5 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.

8.1.5.2.6 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 была непреднамеренно отключена пользователем, ее нужно включить. Для повторной активации защиты в режиме реального времени перейдите в раздел **Настройки** и в главном окне программы щелкните элемент **Защита файловой системы в реальном времени**.

Если защита файловой системы в режиме реального времени не запускается при загрузке операционной системы, обычно это связано с тем, что отключен параметр **Автоматически запускать защиту файловой системы в режиме реального времени**. Чтобы включить этот параметр, перейдите к разделу **Дополнительные настройки** (**F5**) и последовательно щелкните элементы **Компьютер** > **Защита в режиме реального времени**> **Основные сведения**. Обязательно установите флажок **Автоматически запускать защиту файловой системы в режиме реального времени**.

Защита в режиме реального времени не обнаруживает и не очищает заражения

Убедитесь в том, что на компьютере не установлены другие программы защиты от вирусов. При одновременной работе двух систем защиты от вирусов могут возникнуть конфликты. Перед установкой ESET рекомендуется удалить с компьютера все прочие программы защиты от вирусов.

Защита файловой системы в режиме реального времени не запускается

Если защита не запускается при загрузке системы, но функция **Автоматически запускать защиту 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.

8.1.5.2.7 Отправка

Можно выбрать, как именно файлы и статистическая информация будут отправляться в компанию ESET. Выберите вариант **Средствами удаленного администрирования или непосредственно в ESET** для отправки файлов и статистической информации любым доступным способом. Выберите вариант **Средствами удаленного администрирования**, чтобы отправлять файлы и статистику на сервер удаленного администрирования, который обеспечивает последующую отправку в лабораторию ESET. При выборе варианта **Непосредственно в ESET** все подозрительные файлы и статистическая информация отправляются в вирусную лабораторию ESET непосредственно из программы.

Если есть ожидающие отправки файлы, будет доступна кнопка **Передать сейчас**. Нажмите эту кнопку, чтобы немедленно отправить файлы и статистическую информацию.

Установите флажок **Включить ведение журналов**, чтобы создать журнал для регистрации фактов отправки файлов и статистической информации.

8.1.5.2.8 Статистика

Система своевременного обнаружения ThreatSense.Net собирает анонимную информацию о компьютерах пользователей, связанную со вновь обнаруженными угрозами. Это может быть имя заражения, дата и время обнаружения, версия программного продукта обеспечения безопасности ESET, версия операционной системы и информация о расположении. Обычно статистика передается на сервер ESET один или два раза в день.

Пример отправляемого пакета со статистикой представлен ниже.

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C14J8
```

Когда отправлять: можно указать, когда будет отправляться статистическая информация. Если выбрать вариант **Как можно скорее**, статистическая информация будет отправляться сразу же после создания. Этот вариант уместен при наличии постоянного подключения к Интернету. Если выбран вариант **В процессе обновления**, статистическая информация будет отправляться одним пакетом во время следующего обновления.

8.1.5.2.9 Подозрительные файлы

На вкладке **Подозрительные файлы** можно сконфигурировать способ отправки угроз в лабораторию ESET на анализ.

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

Отправку файлов можно сделать автоматической или же выбрать вариант **Спросить перед передачей**, если пользователю нужно знать, какие файлы будут отправлены на анализ, и подтверждать отправку.

Если вы не хотите отправлять какие-либо файлы на анализ, установите флажок **Не передавать на анализ**. Отказ от отправки файлов на анализ не влияет на отправку статистической информации, для конфигурирования которой существуют собственные параметры (см. раздел Статистика).

Время отправки: по умолчанию для отправки подозрительных файлов в лабораторию ESET выбран вариант **Как можно скорее**. Этот вариант рекомендуется использовать, если существует постоянное подключение к Интернету, а подозрительные файлы могут доставляться без задержек. Установите флажок **В процессе обновления**, чтобы подозрительные файлы загружались в ThreatSense.Net при следующем обновлении.

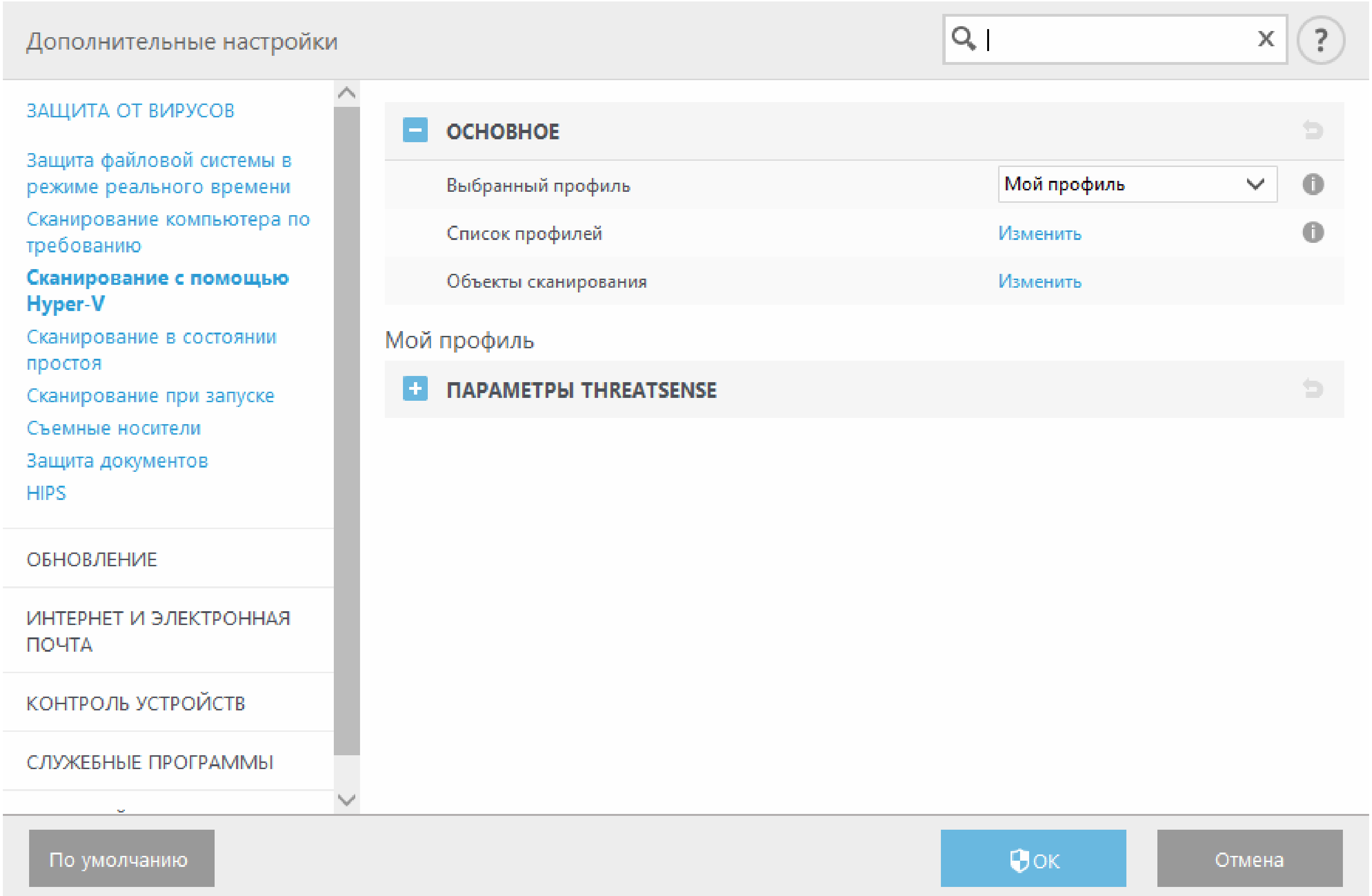
Фильтр исключения: этот вариант позволяет исключить из отправки определенные файлы или папки. Например, может быть полезно исключить файлы, в которых может присутствовать конфиденциальная информация, такие как документы и электронные таблицы. Файлы наиболее распространенных типов (*.doc* и т. п.) исключаются по умолчанию. При желании список исключенных файлов можно дополнять.

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

8.1.6 Сканирование компьютера по требованию и сканирование Hyper-V

В этом разделе можно выбрать параметры сканирования. **Выбранный профиль** — определенный набор параметров, который используется модулем сканирования по требованию. Чтобы создать новый профиль, нажмите кнопку **Изменить** возле элемента **Список профилей**.

> **ПРИМЕЧАНИЕ.**
> Этот переключатель профилей сканирования применяется к сканированию компьютера по требованию и к сканированию Hyper-V.



Если нужно просканировать определенный целевой объект, нажмите кнопку **Изменить** возле элемента **Объекты сканирования** и выберите один из вариантов в раскрывающемся меню или определенные целевые объекты в дереве папок.

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

- **По параметрам профиля** — выбираются объекты, указанные в выделенном профиле сканирования.
- **Сменные носители** — выбираются дискеты, USB-устройства хранения, компакт- и DVD-диски.
- **Жесткие диски** — выбираются все жесткие диски системы.
- **Сетевые диски** — выбираются все подключенные сетевые диски.

- **Общие папки** — выбираются все общие папки на локальном сервере.
- **Ничего не выбирать** — выбор объектов отменяется.

В раскрывающемся меню **Объекты сканирования**для Hyper -V можно выбрать предварительно определенные объекты сканирования.

- **По параметрам профиля** — выбираются объекты, указанные в выбранном профиле сканирования.
- **Все виртуальные машины** — выбираются все виртуальные машины.
- **Включенные виртуальные машины** — выбираются все активные виртуальные машины.
- **Выключенные виртуальные машины** — выбираются все неактивные виртуальные машины.
- **Ничего не выбирать** — выбор объектов отменяется.

Для изменения параметров сканирования в состоянии простоя (например, способов обнаружения) выберите элемент Параметры ThreatSense.

8.1.6.1 Средство запуска выборочного сканирования и сканирования Hyper-V

Если нужно просканировать только определенный объект, можно использовать **выборочное сканирование**. Для этого выберите один из вариантов в раскрывающемся меню **Объекты сканирования** или выберите определенные объекты в дереве папок.

ПРИМЕЧАНИЕ.
Этот переключатель объектов сканирования применяется к выборочному сканированию и к сканированию Hyper-V.

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

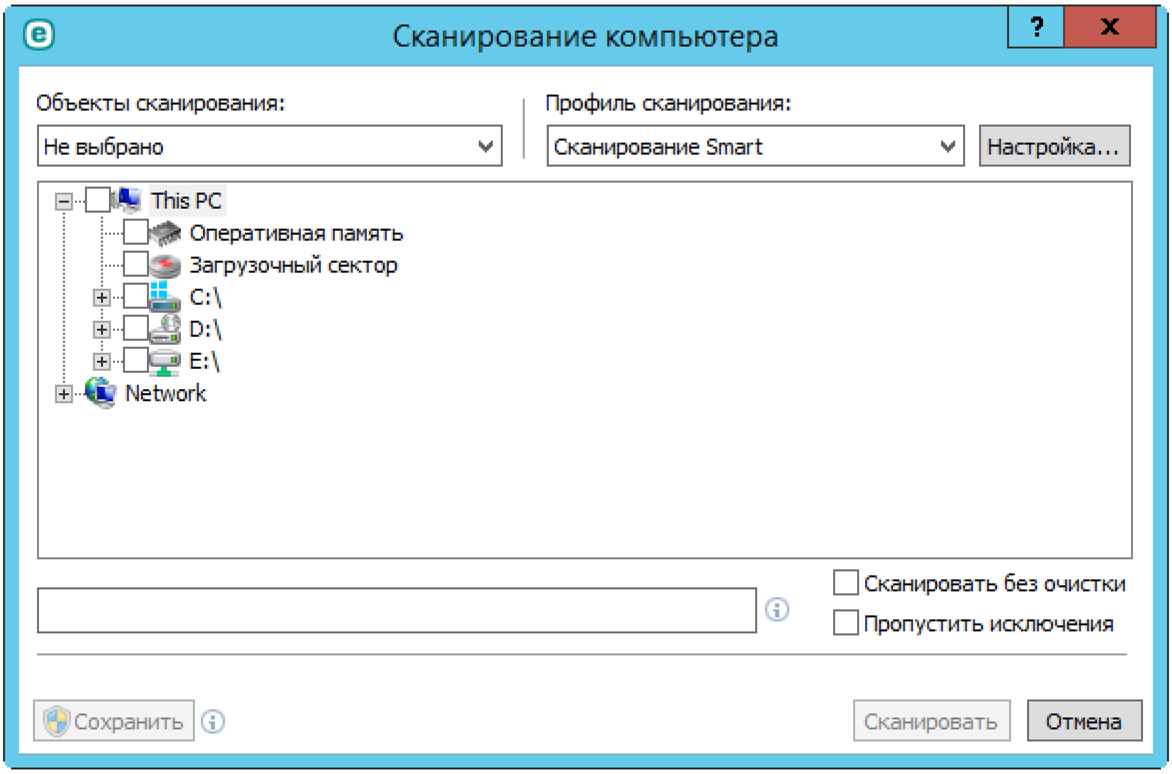
- **По параметрам профиля** — выбираются объекты, указанные в выделенном профиле сканирования.
- **Сменные носители** — выбираются дискеты, USB-устройства хранения, компакт- и DVD-диски.
- **Жесткие диски** — выбираются все жесткие диски системы.
- **Сетевые диски** — выбираются все подключенные сетевые диски.
- **Общие папки** — выбираются все общие папки на локальном сервере.
- **Ничего не выбирать** — выбор объектов отменяется.

В раскрывающемся меню **Объекты сканирования**для Hyper -V можно выбрать предварительно определенные объекты сканирования.

- **По параметрам профиля** — выбираются объекты, указанные в выбранном профиле сканирования.
- **Все виртуальные машины** — выбираются все виртуальные машины.
- **Включенные виртуальные машины** — выбираются все активные виртуальные машины.
- **Выключенные виртуальные машины** — выбираются все неактивные виртуальные машины.
- **Ничего не выбирать** — выбор объектов отменяется.

Для быстрого перехода к какому-либо объекту сканирования или для добавления нового объекта (файла или папки) укажите нужный объект в пустом поле под списком папок. Это возможно только в том случае, если в древовидной структуре не выбраны никакие объекты, а в меню **Объекты сканирования** выбран пункт **Ничего не выбирать**.

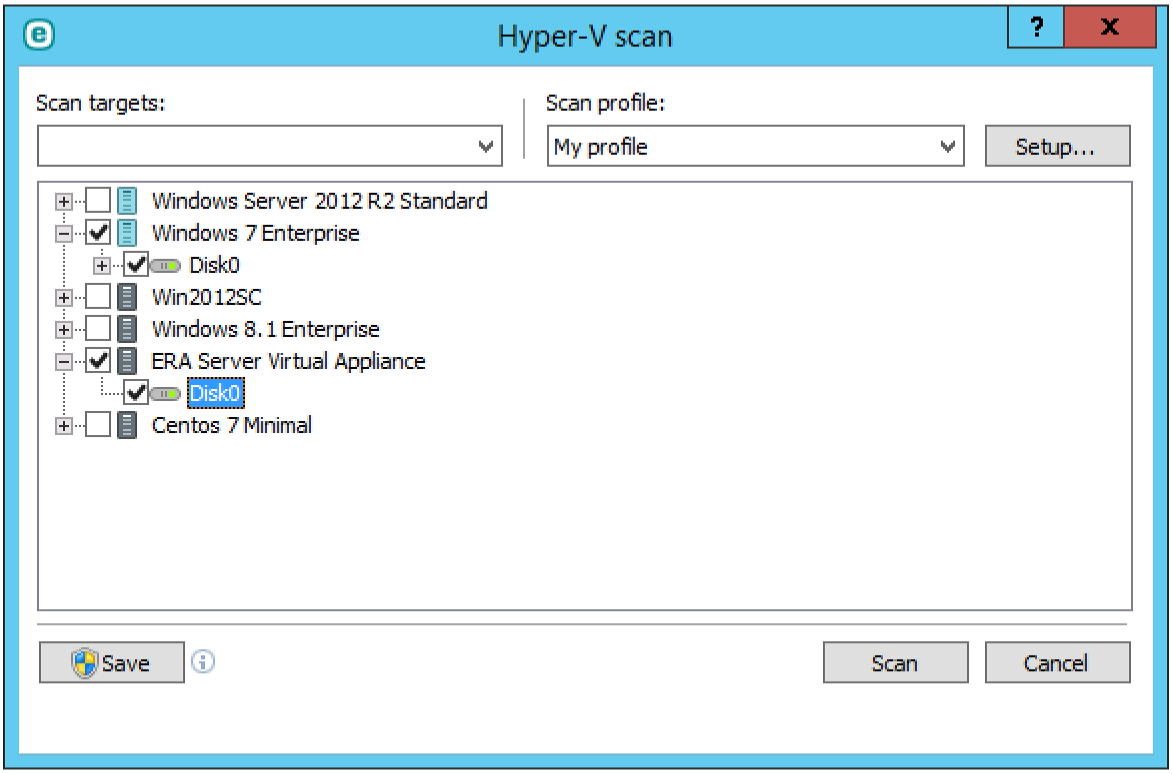
Всплывающее окно **Выборочное сканирование**:



Если нужно выполнить сканирование системы без дополнительных действий по очистке, выберите параметр **Сканировать без очистки**. Этот параметр полезен, если нужен только обзор зараженных файлов и сведения об этих заражениях (если они вообще есть). Можно выбрать один из трех уровней очистки, последовательно щелкнув элементы **Настройки** > **Параметры ThreatSense** > **Очистка**. Информация о сканировании сохраняется в журнале сканирования.

Если выбрать **Пропустить исключения**, при сканировании игнорируются исключения, которые в противном случае применяются.

Всплывающее окно **Сканирование Hyper-V** (дополнительные сведения см. в разделе Сканирование Hyper-V):



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

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

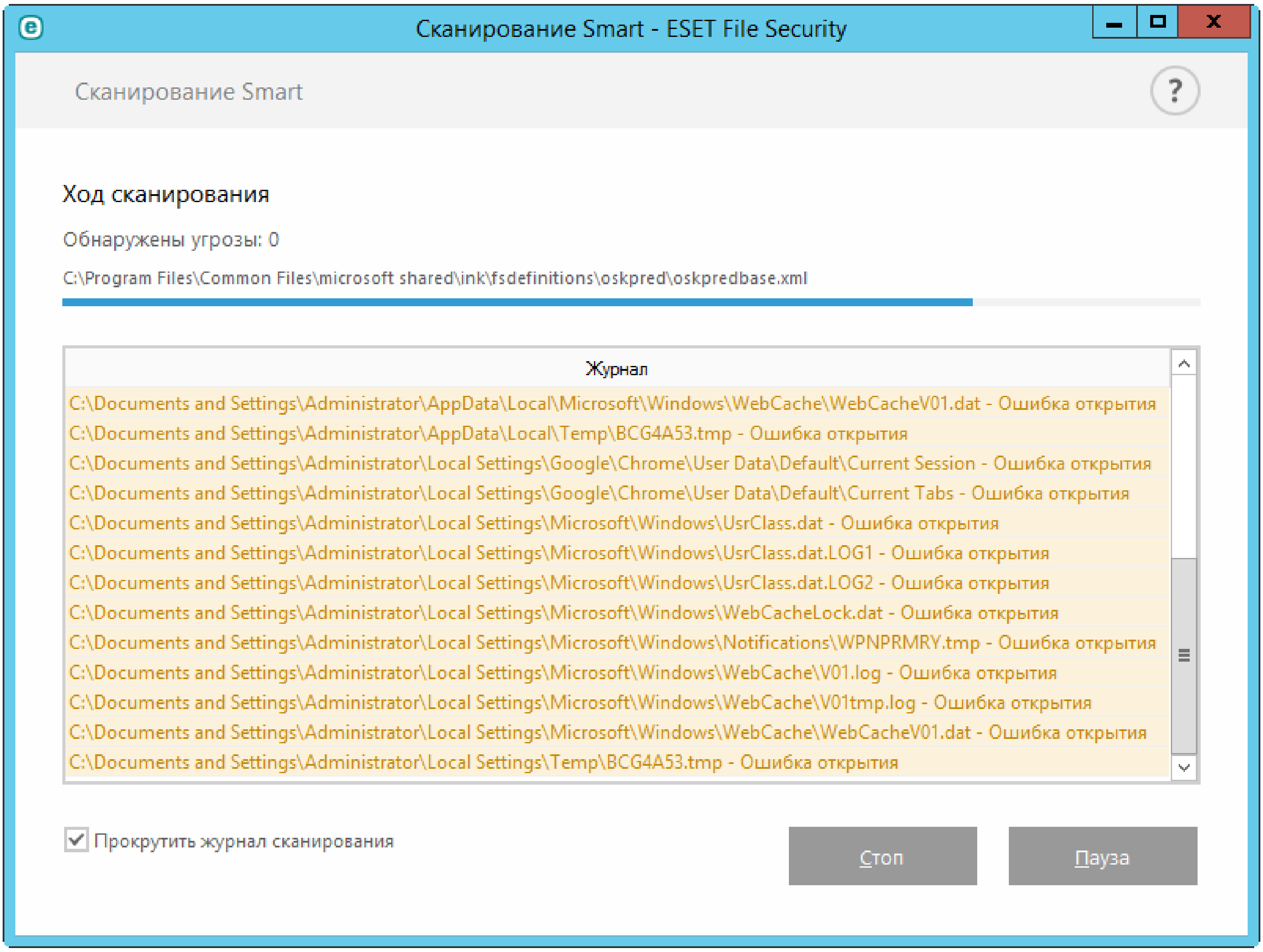
Нажмите кнопку **Сканировать**, чтобы выполнить сканирование с выбранными параметрами.

Кнопка **Сканировать с правами администратора** позволяет выполнять сканирование под учетной записью администратора. Воспользуйтесь этой функцией, если текущая учетная запись пользователя не имеет достаточных прав на доступ к файлам, которые следует сканировать. Обратите внимание, что данная кнопка недоступна, если текущий пользователь не может вызывать операции контроля учетных записей в качестве администратора.

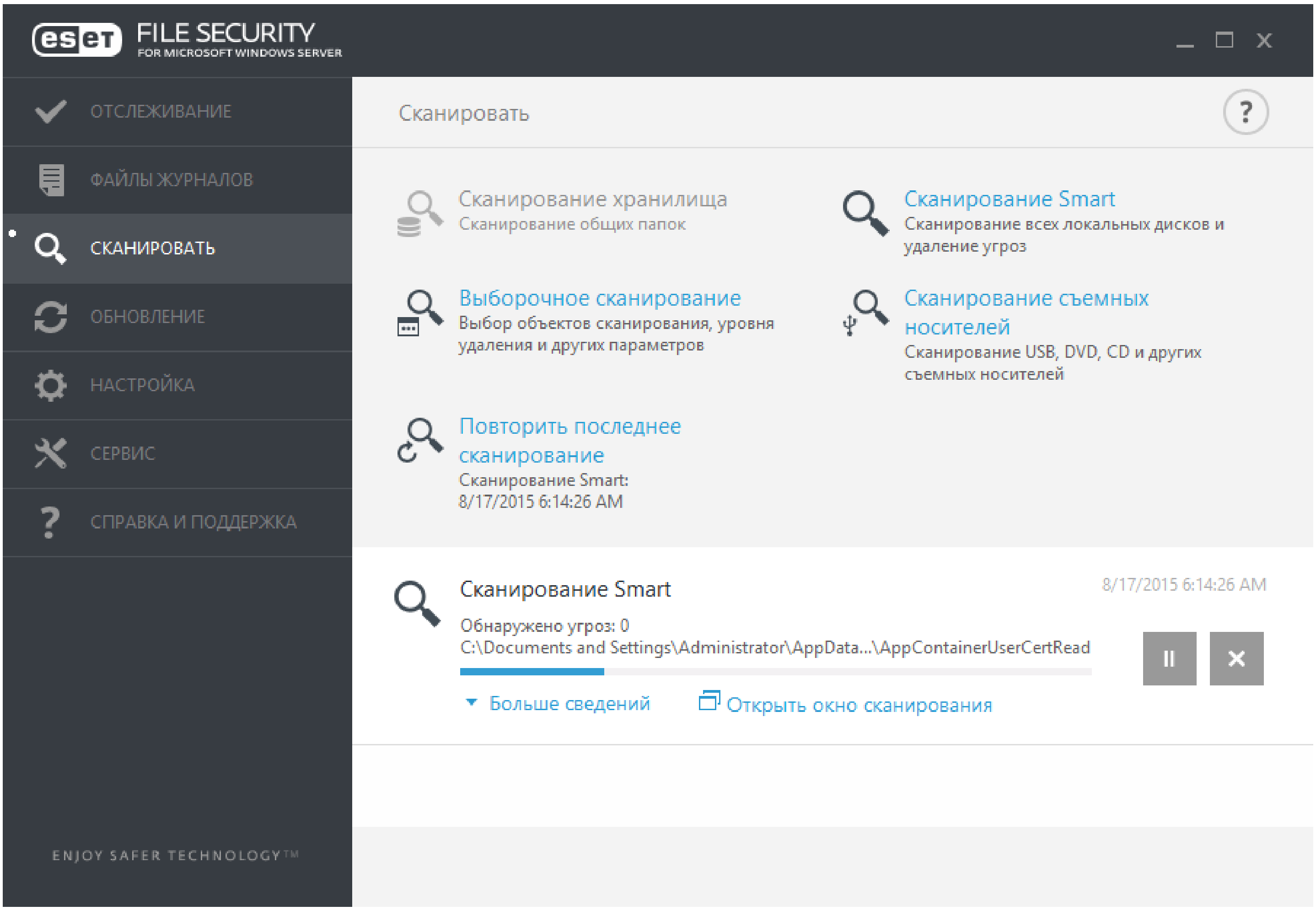
8.1.6.2 Ход сканирования

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

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



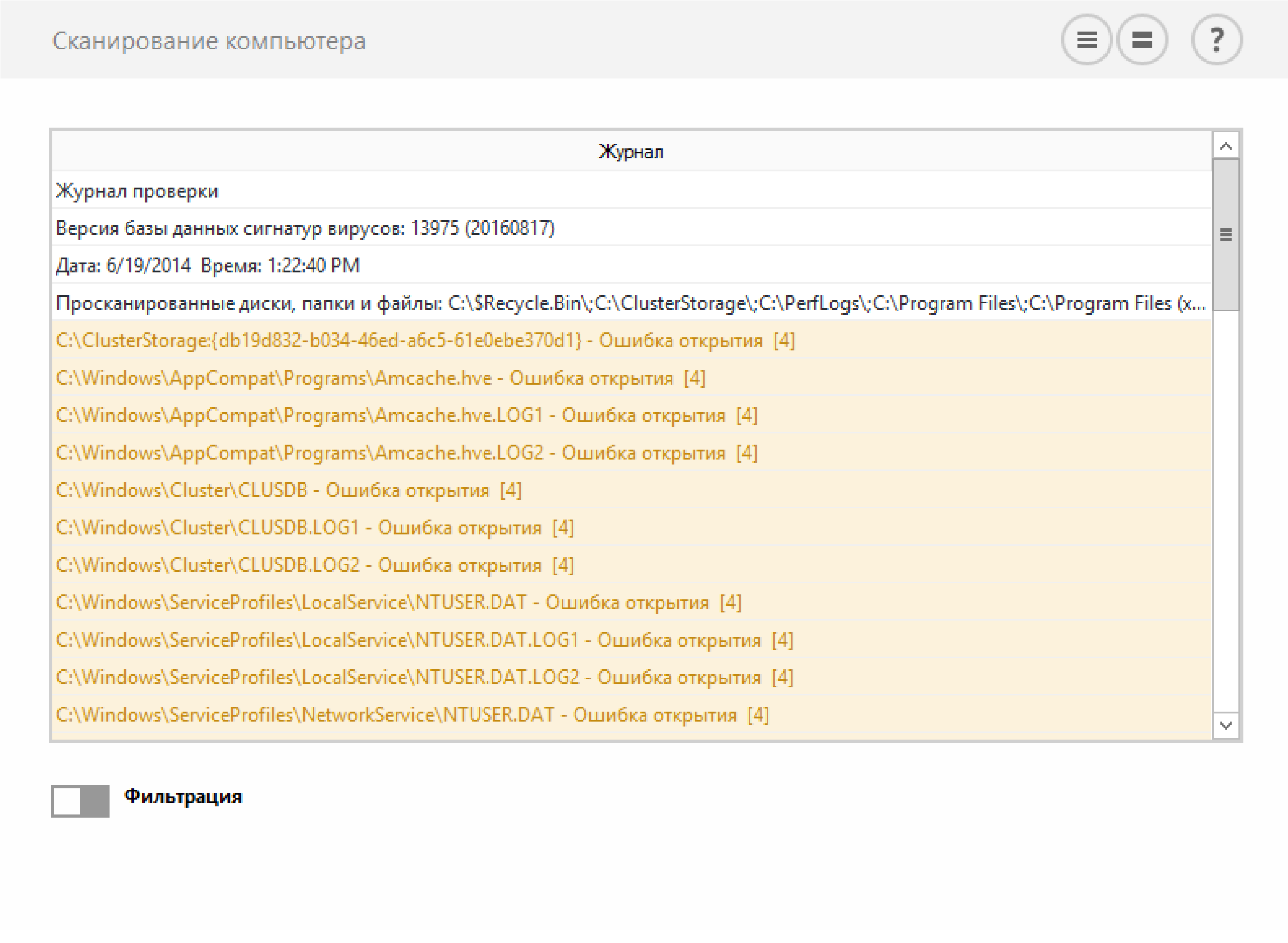
Ход сканирования — индикатор выполнения показывает состояние уже просканированных объектов по сравнению с оставшимися. Состояние выполнения сканирования формируется на основе общего количества объектов, включенных в сканирование.
Объект — имя объекта, который сканируется в настоящий момент, и его расположение.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



Щелкнув **Дополнительные сведения** в ходе сканирования, можно просмотреть, например, информацию о **пользователе**, который запустил сканирование, о количестве **просканированных объектов**, а также о **продолжительности** сканирования.

8.1.6.2.1 Журнал сканирования

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



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

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

Для просмотра приведенных ниже элементов контекстного меню щелкните правой кнопкой мыши определенную запись.

- **Показать**: просмотр в новом окне более подробной информации о выбранном журнале (как и при двойном щелчке).
- **Фильтрация одинаковых записей**: активация фильтра журнала, который показывает только записи одного выбранного типа.
- **Фильтр...**: при выборе этого параметра в окне Фильтрация журнала будет можно задать критерии фильтрации для определенных записей журнала.
- **Включить фильтр**: активация настроек фильтра. При первой активации фильтрации необходимо задать настройки.
- **Отключить фильтр**: отключение фильтрации (такое же действие, как и при использовании переключателя внизу).
- **Копировать**: копирование выделенных записей в буфер обмена.
- **Копировать все**: копируется информация из всех записей в окне.
- **Удалить**: удаление выбранных записей (для этого необходимы права администратора).

- **Удалить все**: удаление всех записей в окне (для этого необходимы права администратора).
- **Экспорт...**: экспорт информации выбранных записей в XML-файл.
- **Экспорт всего...**: экспорт всей информации в окне в XML-файл.
- **Найти...**: этот параметр открывает окно Поиск в журнале и позволяет определить критерии поиска. С помощью функции поиска можно найти определенную запись даже при включенной фильтрации.
- **Найти далее**: поиск следующего вхождения, соответствующего заданным критериям поиска.
- **Найти ранее**: поиск предыдущих вхождений.
- **Прокрутить журнал**: установите этот флажок, чтобы выполнялась автоматическая прокрутка старых журналов, а на экран в окне **Файлы журнала** выводились активные журналы.

8.1.6.3 Диспетчер профилей

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

Сканирование компьютера по требованию

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

Для создания нового профиля откройте окно **Дополнительные настройки** (**F5**) и щелкните **Защита от вирусов** > **Сканирование компьютера по требованию**, а затем выберите команду **Изменить** напротив**списка профилей**. В раскрывающемся меню **Выбранный профиль** отображаются существующие профили сканирования. Для создания профиля сканирования в соответствии с конкретными потребностями см. раздел Настройка параметров модуля ThreatSense, где описывается каждый параметр, используемый для настройки сканирования.

Пример. Предположим, пользователю требуется создать собственный профиль сканирования, причем конфигурация сканирования Smart частично устраивает его, однако не требуется 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. Пользовательские профили обновлений нужны только в том случае, если компьютер подключается к серверам обновлений с помощью разных средств.

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 **Сервис** > **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.

Список профилей: создание или редактирование профилей обновления.

8.1.6.4 Объекты сканирования

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

- **По параметрам профиля** — выбираются объекты, указанные в выделенном профиле сканирования.
- **Сменные носители** — выбираются дискеты, USB-устройства хранения, компакт- и DVD-диски.
- **Жесткие диски** — выбираются все жесткие диски системы.
- **Сетевые диски** — выбираются все подключенные сетевые диски.
- **Общие папки** — выбираются все общие папки на локальном сервере.
- **Ничего не выбирать** — выбор объектов отменяется.

В раскрывающемся меню **Объекты сканирования**для Hyper -V можно выбрать предварительно определенные объекты сканирования.

- **По параметрам профиля** — выбираются объекты, указанные в выбранном профиле сканирования.
- **Все виртуальные машины** — выбираются все виртуальные машины.
- **Включенные виртуальные машины** — выбираются все активные виртуальные машины.
- **Выключенные виртуальные машины** — выбираются все неактивные виртуальные машины.
- **Ничего не выбирать** — выбор объектов отменяется.

8.1.6.5 Приостановка запланированного процесса сканирования

Запланированный процесс сканирования можно отложить. Чтобы сделать это, задайте значение для параметра **Останавливать запланированное сканирование через (мин.)**.

8.1.7 Сканирование в состоянии простоя

Можно разрешить сканирование в состоянии простоя, войдя в раздел **Дополнительные настройки** или нажав клавишу **F5**, затем перейдя в меню **Антивирус** > **Сканирование в состоянии простоя** > **Основное**. Чтобы разрешить использование этой функции, установите переключатель возле элемента **Включить сканирование в состоянии простоя**. Когда компьютер находится в состоянии простоя, автоматически выполняется сканирование всех жестких дисков.

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

В разделе **Дополнительные настройки** выберите параметр **Включить ведение журналов** или нажмите клавишу **F5**, чтобы результаты сканирования компьютера регистрировались в разделе Файлы журнала (в главном окне программы щелкните **Файлы журнала** и выберите тип журнала **Сканирование компьютера** из раскрывающегося меню).

Сканирование в состоянии простоя запускается в случае пребывания компьютера в одном из следующих режимов:

- **Выключенный экран или заставка**
- **блокировка компьютера;**
- **выход пользователя.**

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

8.1.8 Сканирование файлов, исполняемых при запуске системы

При загрузке компьютера и обновлении базы данных сигнатур вирусов автоматически проверяются файлы, исполняемые при запуске системы. Параметры этого сканирования определяются конфигурацией и задачами планировщика.

Сканирование файлов, исполняемых при запуске, входит в принадлежащую планировщику задачу **Проверка файлов, исполняемых при запуске системы**. Чтобы изменить параметры такого сканирования, последовательно выберите элементы **Сервис** > **Планировщик** > **Автоматическая проверка файлов при запуске системы** > **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 новых задач.

8.1.8.1 Автоматическая проверка файлов при запуске системы

При создании запланированной задачи «Проверка файлов, исполняемых при запуске системы» предоставляется несколько вариантов настройки следующих параметров.

Раскрывающееся меню **Объект сканирования** задает глубину сканирования файлов, исполняемых при запуске системы. Файлы упорядочены по возрастанию в соответствии с указанными ниже критериями.

- **Только наиболее часто используемые файлы** (сканируется меньше всего файлов)
- **Часто используемые файлы**
- **Обычно используемые файлы**
- **Редко используемые файлы**
- **Все зарегистрированные файлы** (сканируется больше всего файлов)

Кроме того, существуют две особые группы **объектов сканирования**.

- **Файлы, которые запускаются перед входом пользователя** — содержит файлы из таких папок, которые можно открыть без входа пользователя в систему (в том числе большинство элементов, исполняемых при запуске системы: службы, объекты модуля поддержки браузера, уведомления Winlogon, задания в планировщике Windows, известные библиотеки DLL и т. д.).
- **Файлы, которые запускаются после входа пользователя** — содержит файлы из таких папок, которые можно открыть только после входа пользователя в систему (в том числе файлы, запускаемые под определенными учетными записями, обычно это 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.

- **Обычный** — средняя нагрузка на систему.
- **Более низкий** — низкая нагрузка на систему.
- **Самый низкий** — минимальная нагрузка на систему.
- **При простое** — задача будет выполняться только при бездействии системы.

8.1.9 Съемные носители

Программа ESET File Security обеспечивает автоматическое сканирование съемных носителей (компакт- и DVD-дисков, USB-устройств). Данный модуль позволяет сканировать вставленный носитель. Это может быть удобно, если администратору компьютера нужно, чтобы пользователи не подключали съемные носители с нежелательным содержимым.

Действие, которое следует предпринять после подключения съемного носителя — выбор действия по умолчанию, которое выполняется при подключении съемного носителя (компакт-диска, DVD-диска, USB-устройства) к компьютеру. 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 указанное ниже диалоговое окно.

- **Сканировать сейчас** — начнется сканирование съемного носителя.
- **Сканировать позже** — сканирование съемного носителя будет отложено.
- **Настройки** — вызов дополнительных настроек.
- **Всегда использовать выбранный вариант** — если установить этот флажок, выбранное действие будет выполняться каждый раз, когда вставляется съемный носитель.

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

8.1.10 Защита документов

Функция защиты документов сканирует документы Microsoft Office перед их открытием, а также проверяет файлы, автоматически загружаемые браузером Internet Explorer, такие как элементы Microsoft ActiveX. Функция защиты документов обеспечивает безопасность в дополнение к функции защиты файловой системы в реальном времени. Ее можно отключить, чтобы улучшить производительность систем, которые не содержат большого количества документов Microsoft Office.

- Параметр **Интеграция с системой** активирует систему защиты. Для настройки этого параметра нажмите клавишу F5, чтобы открыть окно **Дополнительные настройки**, и щелкните **Защита от вирусов** > **Защита документов** в дереве дополнительных настроек.

- Дополнительные сведения о параметрах защиты документов см. в разделе Параметры Threatsense.

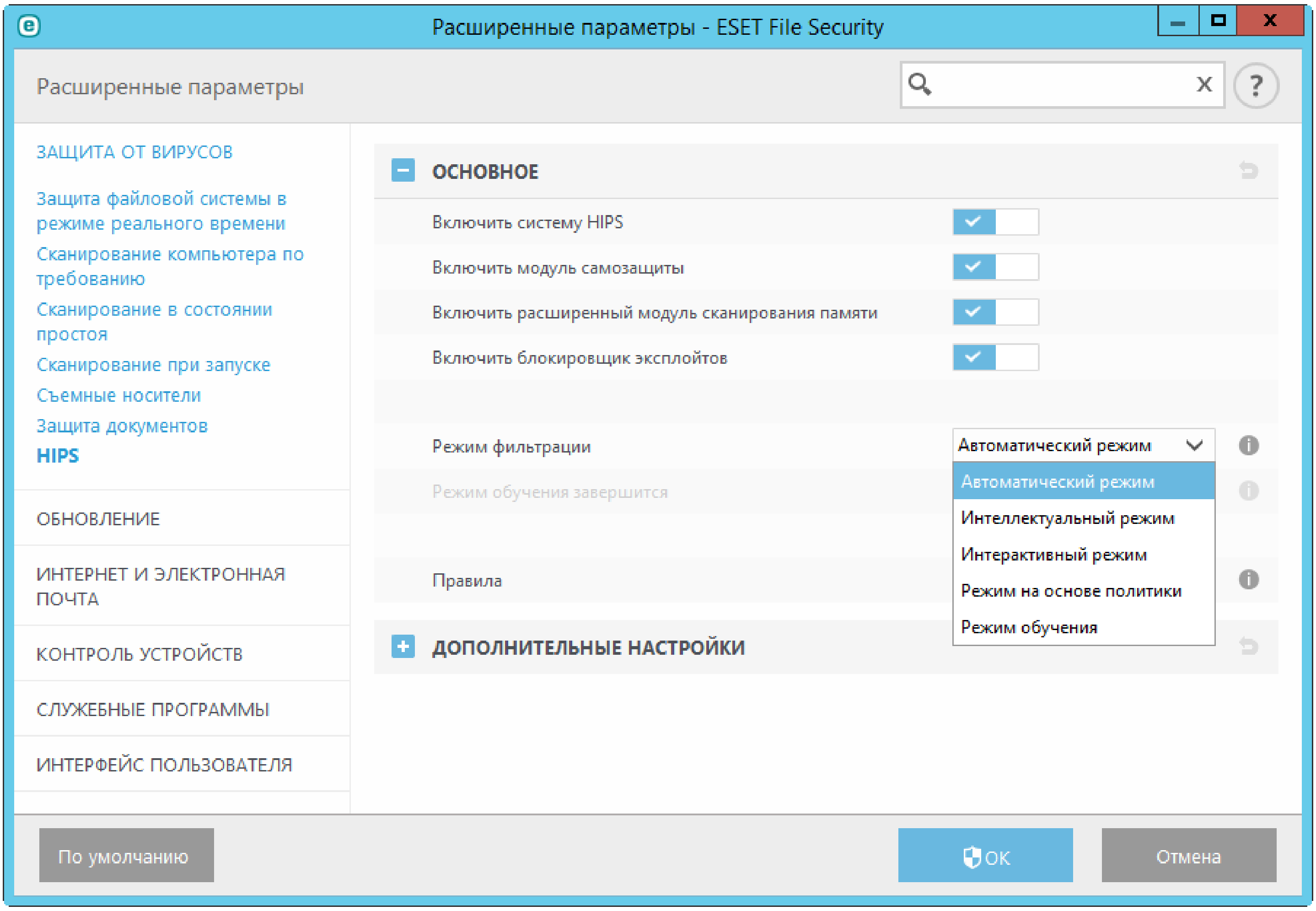
Эта функция активируется приложениями, в которых используется Microsoft Antivirus API (например, Microsoft Office 2000 и более поздние версии или Microsoft Internet Explorer 5.0 и более поздние версии).

8.1.11 HIPS

Система предотвращения вторжений на узел защищает от вредоносных программ и нежелательных процессов, которые пытаются отрицательно повлиять на безопасность компьютера. В системе HIPS используется расширенный анализ поведения в сочетании с возможностями сетевой фильтрации по обнаружению, благодаря чему отслеживаются запущенные процессы, файлы и разделы реестра. Система HIPS отличается от защиты файловой системы в режиме реального времени и не является файерволом — она отслеживает только процессы, запущенные в операционной системе.

ВНИМАНИЕ!
Изменения в параметры системы HIPS должны вносить только опытные пользователи. Неправильная настройка этих параметров может привести к нестабильной работе системы.

Настройки HIPS доступны в дереве **Дополнительные настройки** (F5) > **Защита от вирусов** > **HIPS**. Состояние системы HIPS (включена или отключена) отображается в главном окне ESET File Security, на вкладке **Настройки**, в правой части раздела **Компьютер**.



В программе ESET File Security есть встроенная технология *самозащиты*, которая не позволяет вредоносным программам повредить или отключить защиту от вирусов и шпионских программ, благодаря чему пользователь всегда уверен в защите компьютера. Изменения параметров **Включить систему HIPS** и **Включить модуль самозащиты** вступают в силу после перезапуска операционной системы Windows. Перезагрузить компьютер нужно и для полного отключения **системы предотвращения вторжений на узел**.

Расширенный модуль сканирования памяти работает в сочетании с блокировщиком эксплойтов для усиления защиты от вредоносных программ, которые могут избегать обнаружения продуктами для защиты от вредоносных программ за счет использования умышленного запутывания или шифрования. По умолчанию расширенный модуль сканирования памяти 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. По умолчанию блокировщик эксплойтов включен. Дополнительную информацию об этом типе защиты см. в глоссарии.

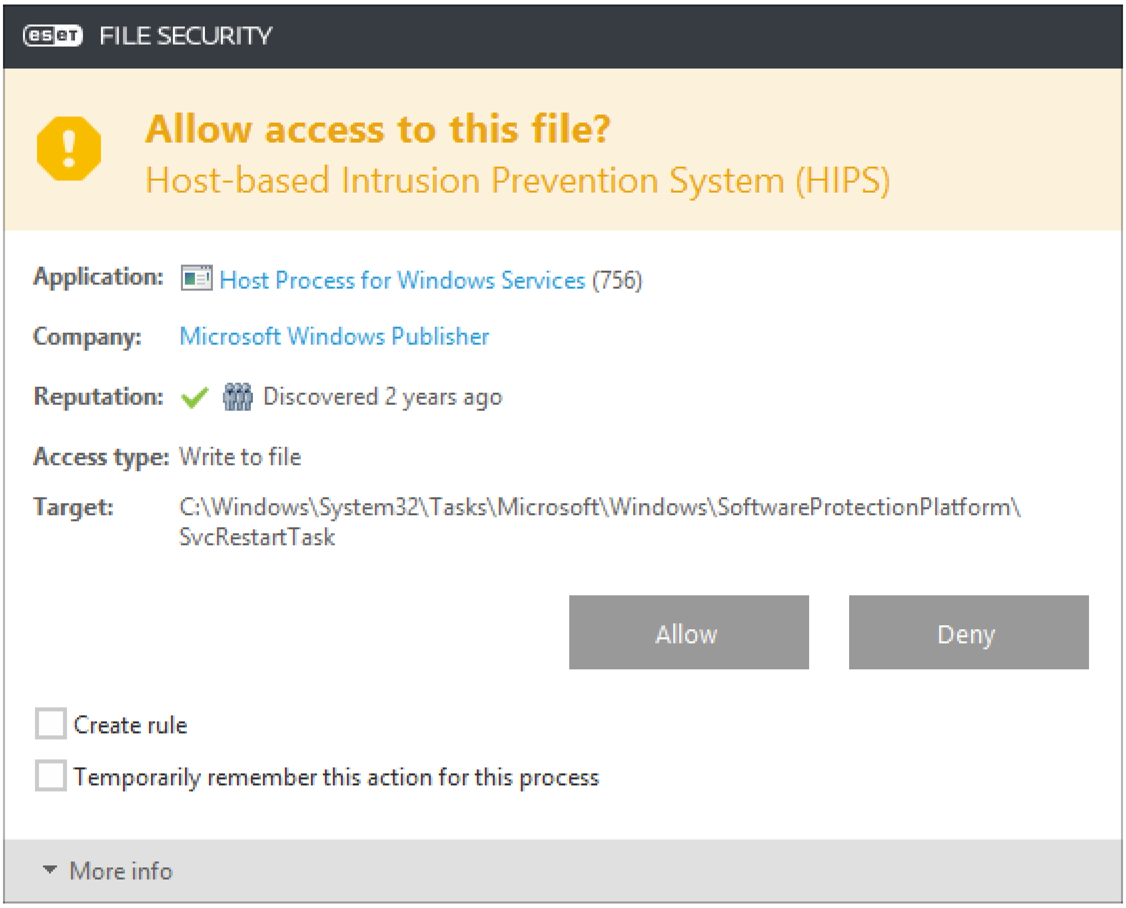
Доступны четыре режима фильтрации.

- **Автоматический режим** — включены все операции за исключением тех, которые заблокированы предварительно заданными правилами, защищающими компьютер.
- **Интеллектуальный режим** — пользователь будет получать уведомления только об очень подозрительных событиях.
- **Интерактивный режим** — будут отображаться запросы на подтверждение операций.
- **Режим на основе политики** — операции блокируются.

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

Система HIPS отслеживает события в операционной системе и реагирует на них соответствующим образом на основе правил, которые аналогичны правилам персонального файервола. Нажмите кнопку **Изменить**, чтобы открыть окно управления правилами системы HIPS. Здесь вы можете выбирать, создавать, изменять и удалять правила. Дополнительные сведения о создании правил и операциях системы HIPS приводятся в главе Изменение правил.

Если для правила по умолчанию установлено действие «Запросить», то при каждом запуске правила будет отображаться диалоговое окно. Для операции можно выбрать и другие действия: **Блокировать** или **Разрешить**. Если пользователь не выбирает действие в течение определенного времени, на основе правил выбирается новое действие.



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

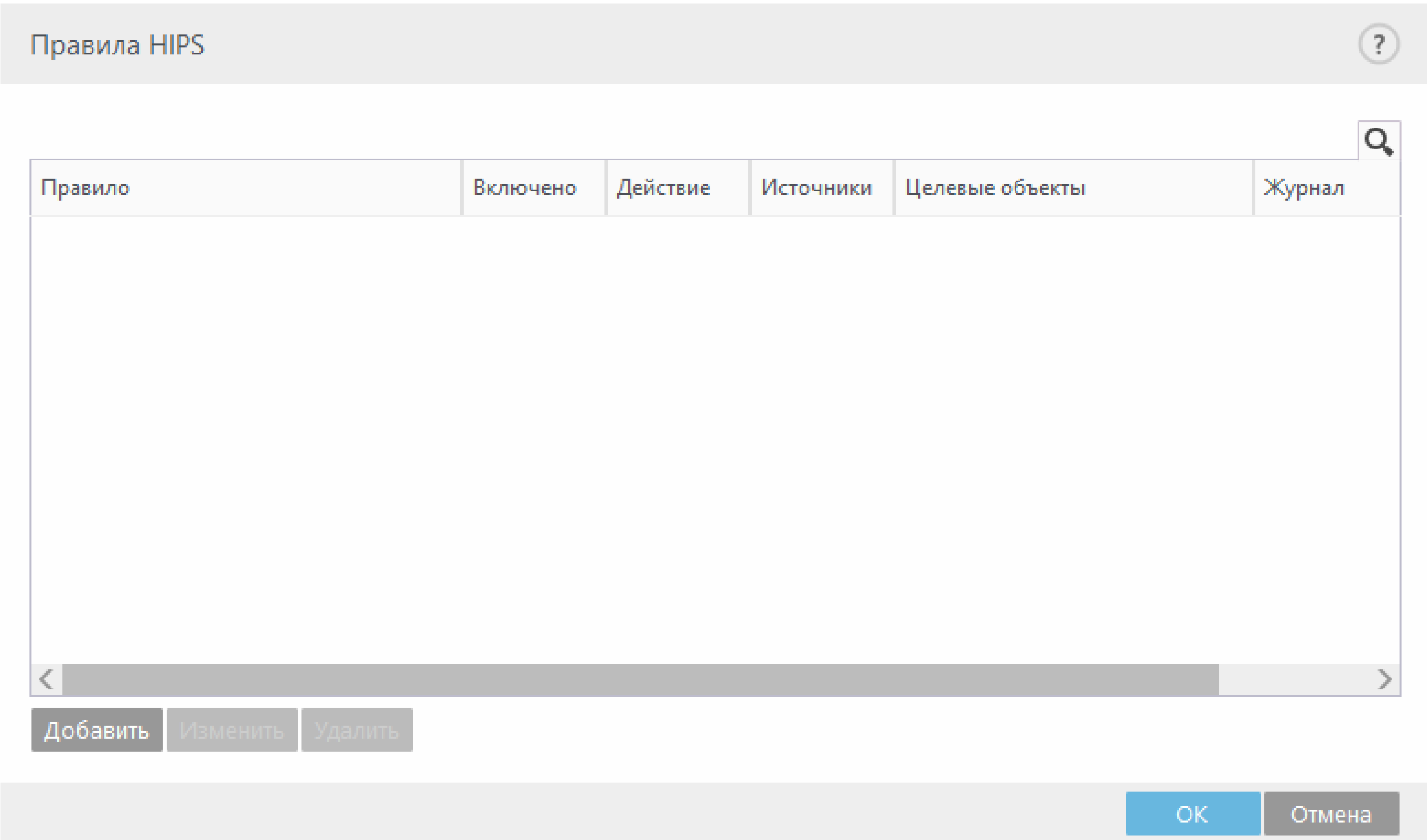
Выбор параметра **Временно запомнить это действие для данного процесса** приводит к использованию действия (**Разрешить/Блокировать**) до тех пор, пока не будут изменены правила или режимы фильтрации, не будет обновлен модуль системы HIPS или не будет выполнена перезагрузка компьютера. После выполнения любого из этих трех действий временные правила удаляются.

8.1.11.1 Правила HIPS

В этом окне отображаются общие сведения об имеющихся правилах HIPS.

Столбцы

Имя — указанное пользователем или автоматически выбранное имя правила.
Включено — отключите этот параметр, если следует оставить правило в списке, но при этом не использовать его.
Действие: правило задает действие (**Разрешить**, **Блокировать** или **Запросить**), которое должно быть выполнено при соблюдении условий.
Источники — правило будет использоваться только в том случае, если событие вызывается этими приложениями.
Объекты — правило будет использоваться только в том случае, если операция связана с тем или иным файлом, приложением или записью реестра.
Журнал — если включить этот параметр, информация о данном правиле будет записываться в журнал HIPS.
Уведомить — если запускается событие, в правом нижнем углу экрана выводится маленькое всплывающее окно.



Элементы управления

Добавить — создание правила.
Изменить — изменение выделенных записей.
Удалить — удаление выделенных записей.

ПРИМЕР

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 продукта, которую можно открыть, нажав клавишу F1)..
5. Выберите в раскрывающемся списке вариант **Определенные приложения** и **добавьте** одно или несколько приложений, которые нужно защитить.
6. Нажмите кнопку **Готово**, чтобы сохранить новое правило.

8.1.11.1.1 Параметры правил HIPS

- **Имя правила** — указанное пользователем или автоматически выбранное имя правила.
- **Действие**: правило задает действие (**Разрешить**, **Блокировать** или **Запросить**), которое должно быть выполнено при соблюдении условий.

Операции влияния — выберите тип операции, к которому будет применяться правило. Правило будет использоваться только для этого типа операции и для выбранного объекта.

- **Файлы** — это правило будет использоваться, только если операция относится к данному объекту. Выберите файлы из раскрывающегося меню и нажмите **Добавить**, чтобы добавить новые файлы или папки. Вы можете также выбрать в раскрывающемся меню пункт **Все файлы**, чтобы добавить все приложения.
- **Приложения** — правило будет использоваться только в том случае, если событие вызывается указанными приложениями. Выберите определенные приложения в раскрывающемся меню и нажмите кнопку **Добавить**, чтобы добавить новые файлы или папки, или выберите пункт «Все приложения», чтобы добавить все приложения.
- **Записи реестра** — это правило будет использоваться, только если операция относится к данному объекту. В раскрывающемся меню выберите определенные записи и нажмите кнопку **Добавить**, чтобы добавить новые файлы или папки, или выберите пункт «Все записи», чтобы добавить все приложения.
- **Включено** — отключите этот параметр, если следует оставить правило в списке, но при этом не использовать его.
- **Журнал** — если включить этот параметр, информация о данном правиле будет записываться в журнал HIPS.
- **Уведомить пользователя** — если запускается событие, в правом нижнем углу экрана выводится небольшое всплывающее окно.

Правило состоит из частей, в которых описываются условия выполнения правила.

Исходные приложения: правило будет использовано только в том случае, если событие запускают выбранные приложения.Выберите **Определенные приложения** в раскрывающемся меню и щелкните **Добавить**, чтобы добавить новые файлы или папки, или выберите в этом меню пункт **Все приложения**, чтобы добавить все приложения.

Файлы — это правило будет использоваться, только если операция относится к данному объекту. Выберите **Определенные файлы** из раскрывающегося меню и нажмите **Добавить**, чтобы добавить новые файлы или папки. Вы можете также выбрать в раскрывающемся меню пункт **Все файлы**, чтобы добавить все приложения.

Приложения — это правило будет использоваться, только если операция относится к данному объекту. Выберите **Определенные приложения** из раскрывающегося меню и нажмите **Добавить**, чтобы добавить новые файлы или папки. Вы можете также выбрать в раскрывающемся меню пункт **Все приложения**, чтобы добавить все приложения.

Записи реестра — это правило будет использоваться, только если операция относится к данному объекту. Выберите **Определенные записи** из раскрывающегося меню и нажмите **Добавить**, чтобы добавить новые файлы или папки. Можно также выбрать в раскрывающемся списке пункт **Все записи**, чтобы добавить все приложения.

ПРИМЕЧАНИЕ.
Некоторые операции определенных правил, предварительно заданных системой HIPS, невозможно заблокировать, и они разрешены по умолчанию. Кроме того, не все системные операции отслеживаются системой HIPS. Система HIPS отслеживает операции, которые могут считаться небезопасными.

Описание важных операций

Операции с файлами

- **Удалить файл** — приложение запрашивает разрешение на удаление целевого файла.
- **Выполнить запись в файл** — приложение запрашивает разрешение на запись в целевой файл.
- **Непосредственный доступ к диску** — приложение пытается выполнить чтение с диска или запись на диск нестандартным образом, в обход стандартных алгоритмов Windows. Это может привести к изменению файлов без применения соответствующих правил. Эта операция может быть вызвана вредоносной программой, пытающейся избежать обнаружения, программным обеспечением резервного копирования, которое пытается создать точную копию диска, или диспетчером разделов, пытающимся реорганизовать тома диска.
- **Установить глобальную ловушку**: вызов функции SetWindowsHookEx из библиотеки MSDN.
- **Загрузить драйвер** — установка и загрузка драйверов в системе.

Операции с приложениями

- **Выполнить отладку другого приложения** — прикрепление отладчика к процессу. При отладке приложения можно просмотреть и изменить многие сведения о его поведении и получить доступ к его данным.
- **Перехватывать события другого приложения** — исходное приложение пытается записать события, направленные на другое приложение (например, клавиатурный шпион, пытающийся записать события браузера).
- **Завершить/приостановить работу другого приложения** — приостановка, возобновление или завершение процесса (можно получить доступ непосредственно из обозревателя процессов или окна «Процессы»).
- **Запустить новое приложение** — запуск новых приложений или процессов.
- **Изменить состояние другого приложения** — исходное приложение пытается осуществить запись в память целевого приложения или выполнить код от его имени. Эта функциональность может быть полезна, если нужно защитить важное приложение путем конфигурирования его в качестве целевого приложения в правиле, которое блокирует использование этой операции.

Операции с реестром

- **Изменить параметры запуска** — любые изменения параметров, которые определяют, какие приложения будут выполнены при запуске ОС Windows. Их можно найти, например, выполнив поиск раздела Run в реестре Windows.
- **Удалить из реестра** — удаление раздела реестра или его значения.
- **Переименовать раздел реестра** — переименование разделов реестра.
- **Изменить реестр** — создание новых значений разделов реестра, изменение существующих значений, перемещение данных в древовидной структуре базы данных или настройка прав пользователя или группы для разделов реестра.

ПРИМЕЧАНИЕ.
При вводе объекта можно использовать подстановочные знаки с определенными ограничениями. Вместо конкретного раздела в пути реестра можно использовать символ звездочки («*»). Например, *HKEY_USERS*\software* может означать *HKEY_USER\.default\software*, но не *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*. Путь *HKEY_LOCAL_MACHINE\system\ControlSet** не является допустимым путем раздела реестра. Путь, в котором содержится сочетание символов *, означает «этот путь или любой путь на любом уровне после этого символа». Это единственный способ использования подстановочных знаков для обозначения целевых файлов. Сначала оценивается точный путь, а затем путь после подстановочного знака (*).

ВНИМАНИЕ!
Если созданное правило будет слишком общим, появится соответствующее уведомление.

8.1.11.2 Дополнительные настройки

Перечисленные далее параметры полезны для отладки и анализа поведения приложения.

- Драйверы, загрузка которых разрешена всегда: загрузка выбранных драйверов разрешена всегда, вне зависимости от настроенного режима фильтрации, если они не заблокированы в явном виде правилом пользователя.
- **Регистрировать все заблокированные операции**: все заблокированные операции будут записываться в журнал HIPS.
- **Сообщать об изменениях приложений, загружаемых при запуске системы**: при добавлении или удалении приложения, загружаемого при запуске системы, на рабочем столе отображается уведомление.

8.1.11.2.1 Драйверы, загрузка которых разрешена всегда

Загрузка драйверов, отображенных в этом списке, разрешена всегда вне зависимости от режима фильтрации HIPS. Это не касается случаев, когда загрузка драйвера явным образом заблокирована правилом пользователя.

Добавить — добавление нового драйвера.
Изменить — изменение пути к выбранному драйверу.
Удалить — удаление драйвера из списка.
Сброс — перезагрузка набора системных драйверов.

ПРИМЕЧАНИЕ.
Если щелкнуть элемент **Сброс**, драйверы, добавленные вручную, будут удалены из списка. Это может пригодиться, если вы добавили несколько драйверов и не можете удалить их из списка вручную.

8.2 Обновление

Параметры обновления доступны в окне **Дополнительные настройки** (нажмите клавишу **F5**) в разделе **Обновление** > **Общие**. В этом разделе указывается информация об источниках обновлений, например сведения о серверах обновлений и данные аутентификации для них.

ПРИМЕЧАНИЕ.
Для обеспечения правильной загрузки обновлений необходимо корректно задать все параметры обновлений. Если используется файервол, программе должно быть разрешено обмениваться данными через Интернет (например, через HTTP-соединение).

Общие сведения

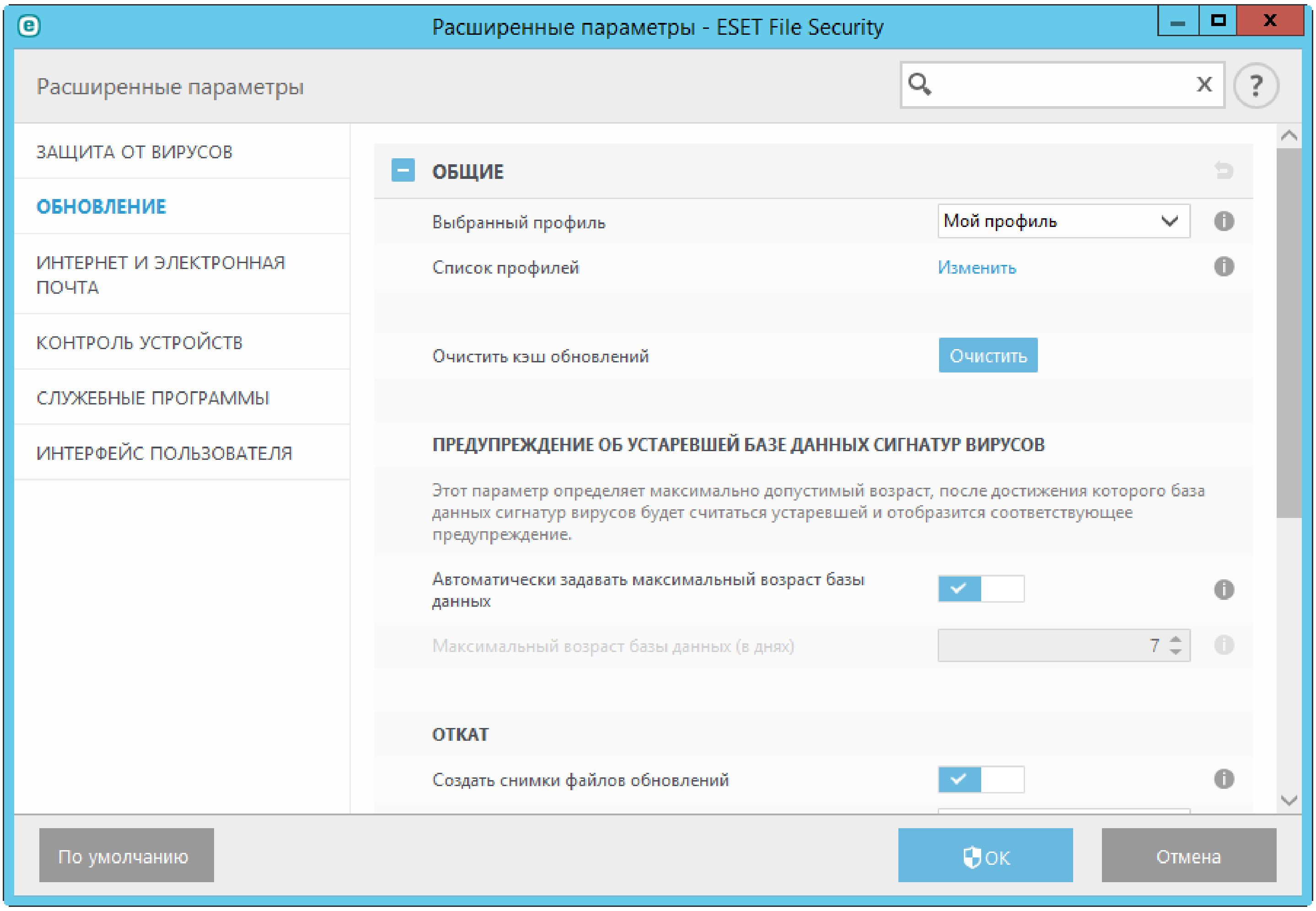
- Текущий **профиль обновления** отображается в раскрывающемся меню выбранного профиля. При возникновении проблем с обновлением нажмите кнопку **Очистить**, чтобы удалить из кэша временные файлы обновления.

Предупреждения об устаревшей базе данных сигнатур вирусов

- **Автоматически задавать максимальный возраст базы данных**/**Максимальный возраст базы данных (в днях)**: этот параметр позволяет задать максимальное время в днях, по истечении которого база данных сигнатур вирусов будет считаться устаревшей. По умолчанию установлено значение 7 дней.

Откат

Если вы подозреваете, что последнее обновление базы данных сигнатур вирусов и/или модулей программы повреждено или работает нестабильно, вы можете выполнить откат к предыдущей версии и отключить обновления на определенный период времени. Или же можно включить ранее отключенные обновления, если они отложены на неопределенный период времени. ESET File Security записывает моментальные снимки базы данных сигнатур вирусов и программных модулей для использования с функцией **Откат**. Если нужно, чтобы снимки базы данных вирусов создавались, оставьте установленным флажок **Создать снимки файлов обновлений**. В поле **Количество локально хранимых снимков** указывается количество хранящихся снимков предыдущих баз данных сигнатур вирусов.

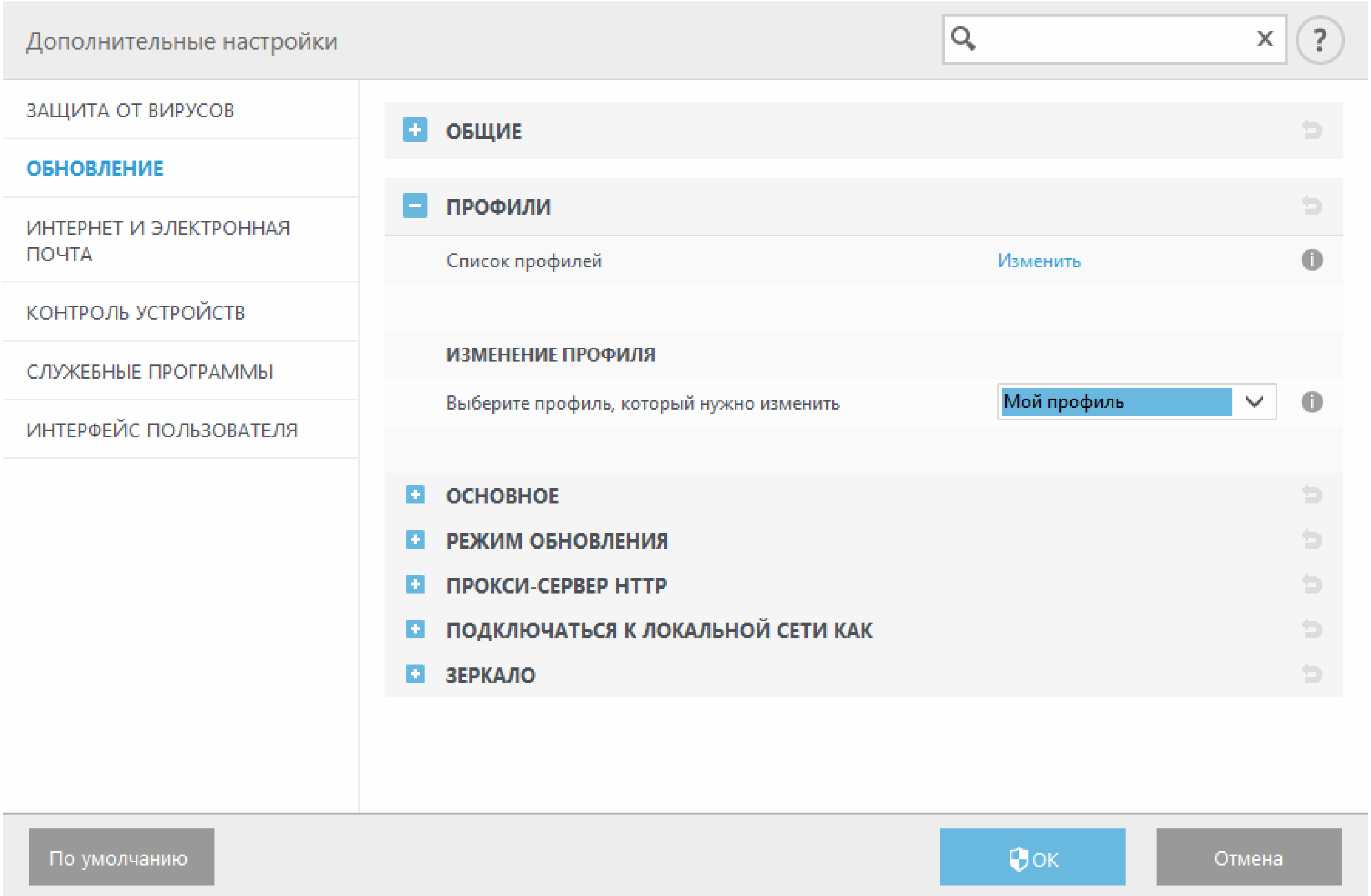


ПРИМЕР

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

Профили

Чтобы создать профиль, рядом с элементом **Список профилей** нажмите кнопку **Изменить**, введите **имя профиля** и нажмите кнопку **Добавить**. **Изменить профиль** можно с помощью следующих параметров:



⊟ Основная информация

Тип обновления — выберите в раскрывающемся меню тип обновления, который нужно использовать.

- **Регулярное обновление** — задаваемый по умолчанию, такой тип обновления обеспечивает автоматическую загрузку файлов обновлений с сервера ESET с минимальным расходом сетевого трафика.
- **Тестовое обновление** — 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 рабочих серверах и рабочих станциях, где необходимы максимальные работоспособность и стабильность.
- **Отложенное обновление** — позволяет загружать обновления со специальных серверов с задержкой в несколько часов (т. е. после того, как обновления будут протестированы в реальных средах и признаны стабильными).

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

Обновлять со съемных носителей — позволяет выполнить обновление со съемного носителя, если он содержит созданное зеркало. Если установлен флажок **Автоматически**, обновления будут выполняться в фоновом режиме. Если диалоговые окна обновления должны отображаться, выберите **Всегда спрашивать**.

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

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

Если используется локальный HTTP-сервер с поддержкой SSL, сервер обновлений должен быть указан следующим образом:
https://имя_компьютера_или_его_IP-адрес:2221.

Если используется локальная общая папка, сервер обновлений должен быть указан следующим образом:
\\имя компьютера или его IP-адрес\общая папка

- **Обновление с зеркала**

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

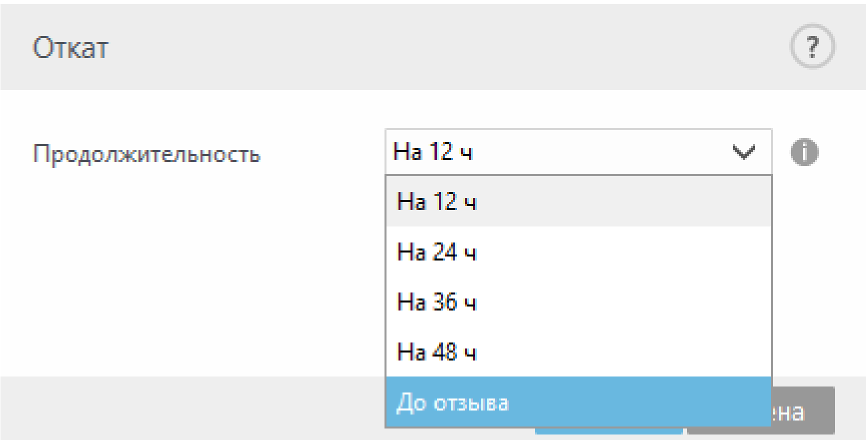
- Режим обновления
- Прокси-сервер HTTP
- Подключаться к локальной сети как
- Зеркало

8.2.1 Откат обновления

Нажав кнопку **Откатить**, в раскрывающемся меню нужно выбрать промежуток времени, на который будет приостановлено обновление базы данных сигнатур вирусов и модулей программы.

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

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



8.2.2 Режим обновления

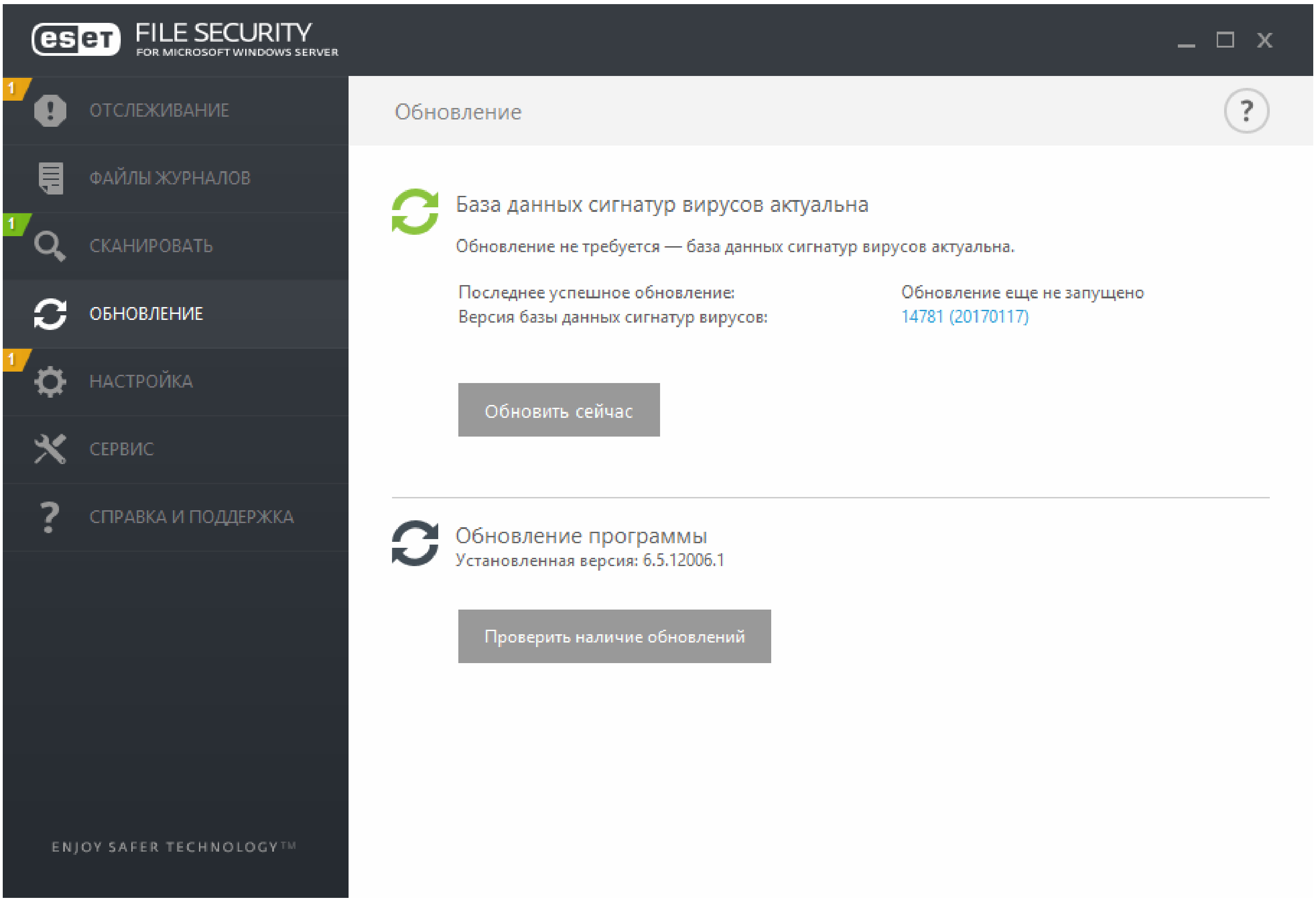
Вкладка **Режим обновления** содержит параметры, относящиеся к обновлениям компонентов программы. Программа позволяет заранее задать ее поведение в тех случаях, когда становятся доступны обновления компонентов.

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

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

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

Если нужно обновить версию ESET File Security **Включить ручное обновление компонентов программы**. По умолчанию этот параметр отключен. Когда он включен и доступна новая версия программы ESET File Security, на вкладке **Обновление** появляется элемент **Проверить наличие обновлений**.



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

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

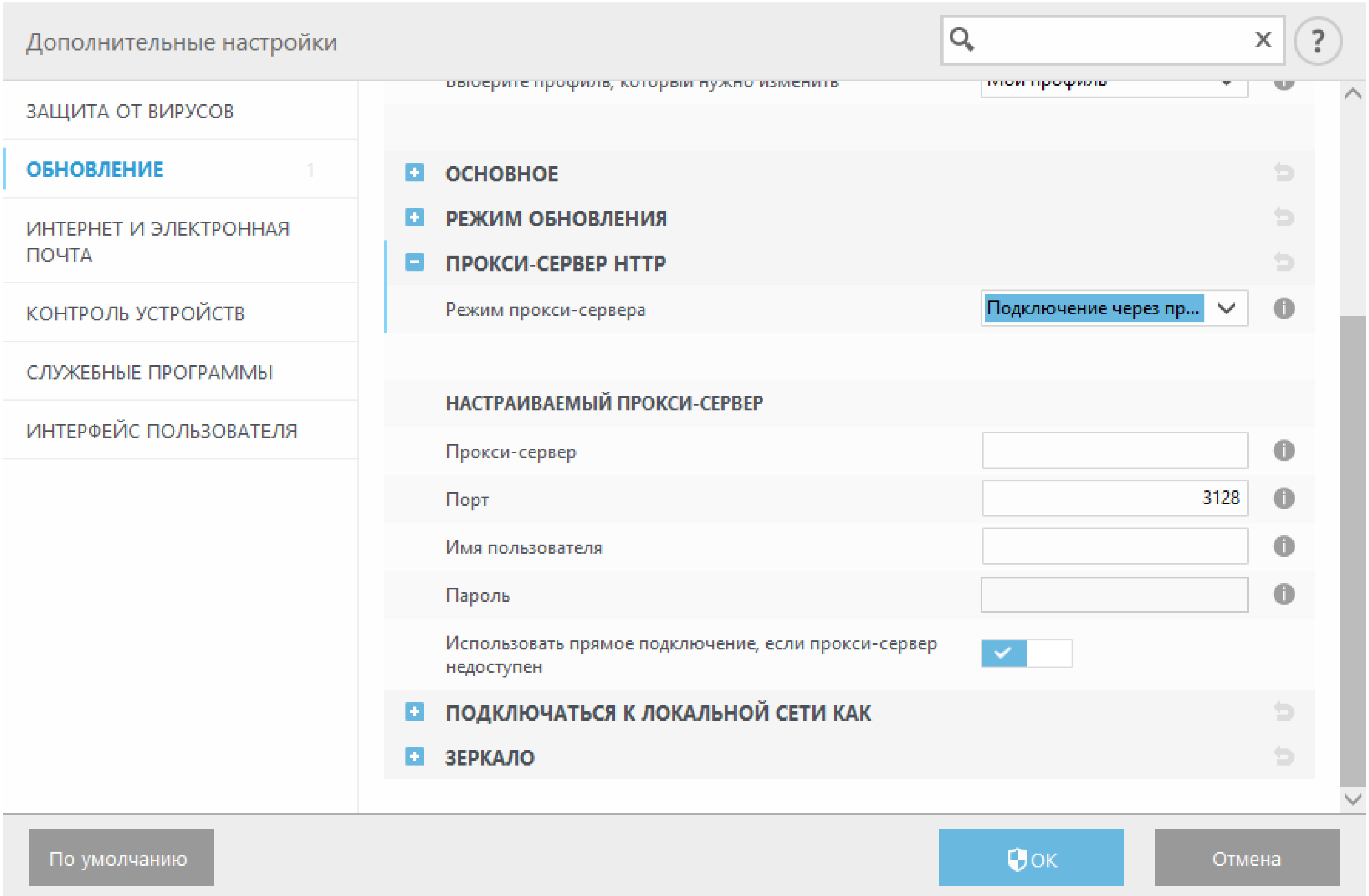
8.2.3 Прокси-сервер HTTP

Для доступа к параметрам настройки прокси-сервера для конкретного профиля обновлений щелкните **Режим прокси-сервера** и выберите один из трех перечисленных далее вариантов.

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

> **ПРИМЕЧАНИЕ.**
> По умолчанию установлен вариант **Использовать глобальные параметры прокси-сервера**.

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



- **Подключение через прокси-сервер**: этот флажок должен быть установлен в следующих случаях.
  - Для обновления ESET File Security должен использоваться прокси-сервер, отличный от указанного в глобальных параметрах (**Служебные программы** > Прокси-сервер). В этом случае нужно указать следующие параметры: адрес **прокси-сервера**, **порт** передачи данных (3128 по умолчанию), а также **имя пользователя** и **пароль** для прокси-сервера (если необходимо).
  - Не были заданы общие параметры прокси-сервера, однако ESET File Security будет подключаться к прокси-серверу для получения обновлений.
  - Компьютер подключается к Интернету через прокси-сервер. Параметры берутся из браузера Internet Explorer в процессе установки программы, но если впоследствии они будут изменены (например, при смене поставщика услуг Интернета), нужно будет убедиться в том, что указанные в этом окне параметры

прокси-сервера HTTP верны. Если этого не сделать, программа не сможет подключаться к серверам обновлений.

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

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.

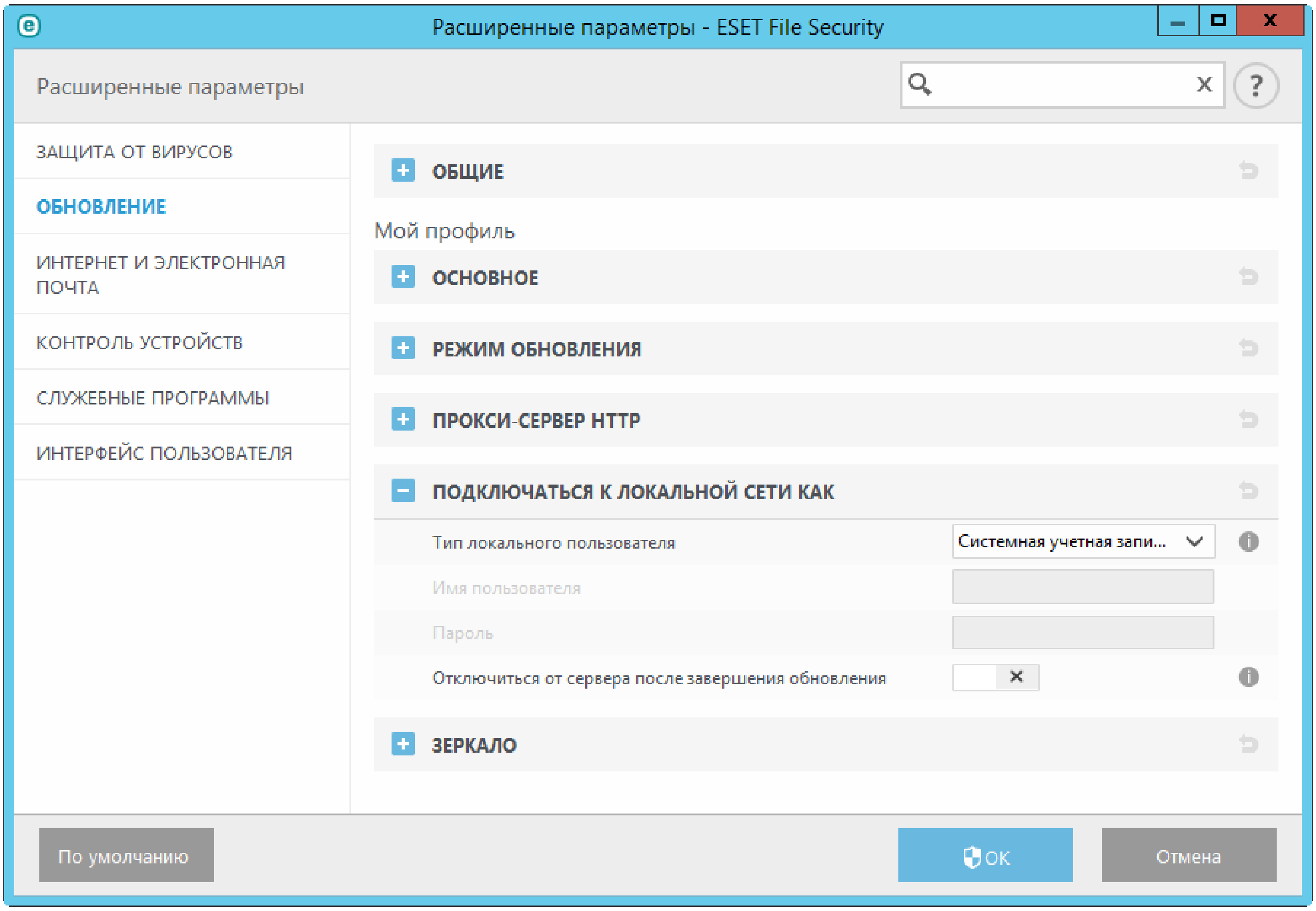
8.2.4 Подключение к локальной сети

При обновлении с локального сервера под управлением ОС Windows по умолчанию требуется аутентификация всех сетевых подключений. Параметры конфигурации находятся в дереве **Дополнительные настройки** (F5) в разделе **Обновление** > **Профили** > **Подключаться к локальной сети как**. Чтобы настроить учетную запись, в раскрывающемся меню **Тип локального пользователя** выберите один из следующих параметров.

- Чтобы использовать для аутентификации системную учетную запись, выберите вариант **Системная учетная запись (по умолчанию)**. Если данные аутентификации в главном разделе параметров обновлений не указаны, то процесс аутентификации, как правило, не происходит.
- Чтобы программа использовала для аутентификации учетную запись, под которой в данный момент выполнен вход в систему, выберите вариант **Текущий пользователь**. Недостаток этого варианта заключается в том, что программа не может подключиться к серверу обновлений, если в данный момент ни один пользователь не выполнил вход в систему.
- Если нужно указать учетную запись определенного пользователя для аутентификации, выберите элемент **Указанный пользователь**. Этот метод следует использовать, когда невозможно установить соединение с помощью учетной записи системы. Обратите внимание на то, что указанная учетная запись должна обладать правами на доступ к каталогу на локальном сервере, в котором хранятся файлы обновлений. В противном случае программа не сможет установить соединение и загрузить обновления.

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

- Если подключение к серверу остается активным после загрузки обновлений, то для принудительного отключения выберите параметр **Отключиться от сервера после завершения обновления**.



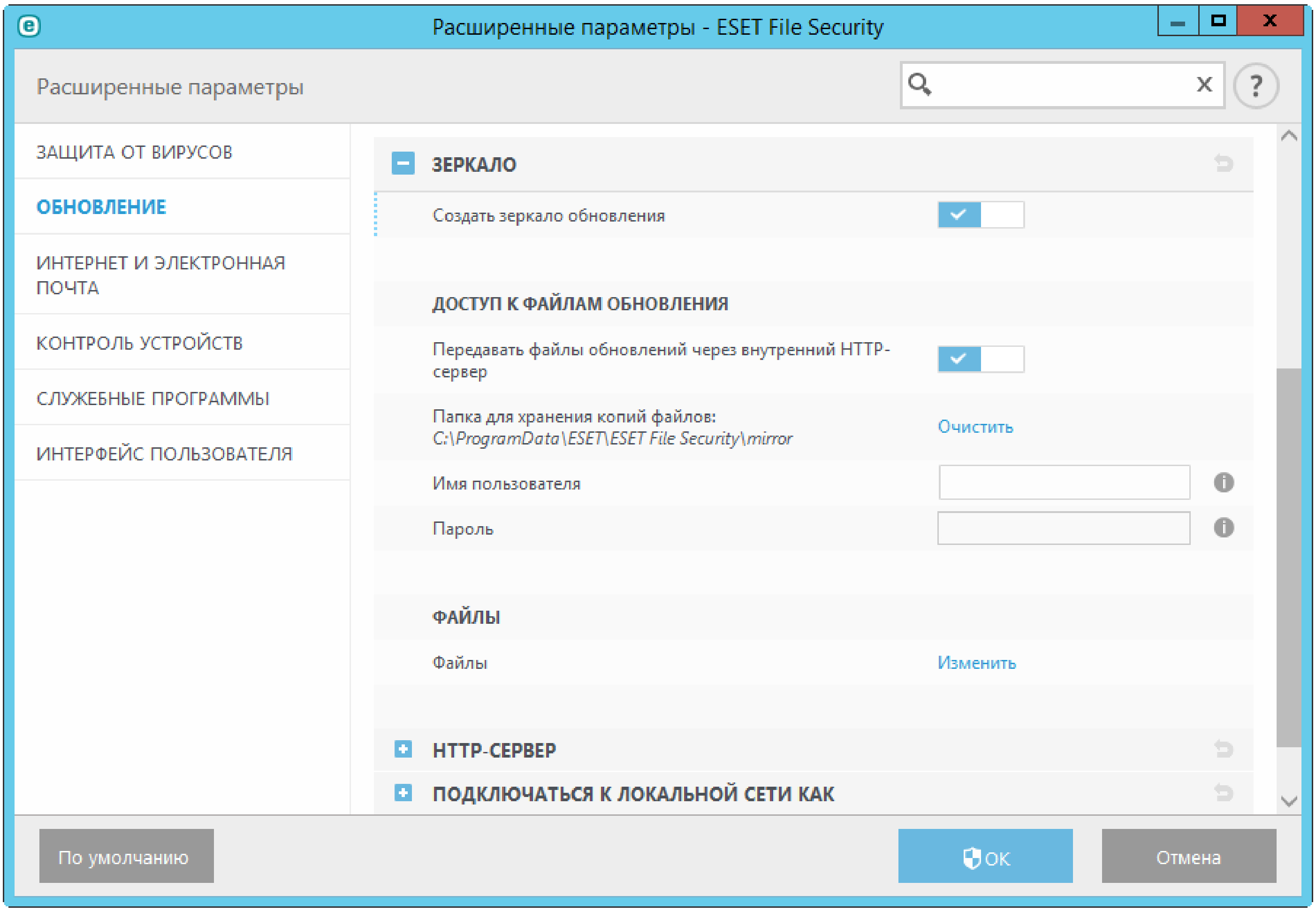
8.2.5 Зеркало

ESET File Security дает возможность создавать копии файлов обновлений, которые могут использоваться для обновления других рабочих станций в сети. Использование *зеркала* (копии файлов обновлений в локальной сети) позволяет избежать загрузки одних и тех же обновлений с сервера производителя всеми рабочими станциями. Обновления загружаются на локальный сервер зеркала, а затем распространяются на рабочие станции. Это позволяет избежать перегрузки трафика. Обновление клиентских рабочих станций с зеркала оптимизирует балансировку сетевой нагрузки и уменьшает процент используемой пропускной способности подключения к Интернету.

Параметры конфигурации локального сервера зеркала расположены в дереве **Дополнительные настройки** (F5) на вкладке **Обновление** > **Профили** > **Зеркало**.

Создание зеркала обновления

Создать зеркало обновления — включение этого параметра активирует другие параметры конфигурации зеркала, такие как способ доступа к файлам обновлений и путь для обновления файлов зеркала.



Доступ к файлам обновления

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

> **ПРИМЕЧАНИЕ.**
> Для использования HTTP-сервера в Windows XP необходимо установить пакет обновления 2 или более позднюю версию.

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

- **Папка для хранения копий файлов** — нажмите **Очистить**, если нужно изменить заданную по умолчанию папку для хранения зеркальных копий файлов *C:\ProgramData\ESET\ESET File Security\mirror.* Нажмите **Изменить**, чтобы выбрать папку на локальном компьютере или общую сетевую папку. Если для указанной папки нужна авторизация, данные аутентификации должны быть указаны в полях **Имя пользователя** и **Пароль**. Если выбранная папка назначения расположена на сетевом диске компьютера под управлением ОС Windows NT/2000/XP, указанные имя пользователя и пароль должны принадлежать пользователю с правами на запись в указанную папку. Имя пользователя и пароль следует вводить в формате *Домен/Пользователь* или *Рабочая_группа/Пользователь*. Не забудьте ввести соответствующие пароли.

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

HTTP-сервер

- **Порт сервера** — по умолчанию порт сервера имеет значение 2221.

- Параметром **Аутентификация** определяется способ аутентификации, используемый для доступа к файлам обновлений. Доступны указанные ниже варианты. **Нет**, **Обычная** и **NTLM**.

Выберите вариант **Обычная**, чтобы использовать кодировку base64 и упрощенную аутентификацию по имени пользователя и паролю.
Вариант **NTLM** обеспечивает шифрование с использованием безопасного способа шифрования. Для аутентификации используется учетная запись пользователя, созданная на рабочей станции, которая предоставляет общий доступ к файлам обновлений. Значение по умолчанию — **Нет**. Этот вариант обеспечивает доступ к файлам обновлений без аутентификации.

SSL для HTTP-сервера

- Чтобы использовать HTTP-сервер с поддержкой протокола HTTPS (SSL), прикрепите свой **файл цепочки сертификатов** или создайте самозаверяющий сертификат. Доступны следующие типы сертификатов: PEM, PFX и ASN. Из соображений дополнительной безопасности для загрузки файлов обновления можно использовать протокол HTTPS. При его использовании практически невозможно отследить передаваемые сведения и учетные данные.

- Для параметра **Тип закрытого ключа** по умолчанию задается значение **Интегрированный** (поэтому параметр **Файл закрытого ключа** по умолчанию неактивен). Это означает, что закрытый ключ является частью выбранного файла цепочки сертификатов.

Подключение к локальной сети

- **Тип локального пользователя** — варианты **Системная учетная запись (по умолчанию)**, **Текущий пользователь** и **Указанный пользователь** отображаются в соответствующих раскрывающихся меню. **Имя пользователя** и **пароль** указывать необязательно. См.статью Подключение к локальной сети.
- Если подключение к серверу остается активным после загрузки обновлений, то для принудительного отключения выберите элемент **Отключиться от сервера после завершения обновления**.

Обновление компонентов программы

- **Автоматически обновлять компоненты** — разрешает установку новых компонентов и обновление существующих. Обновление может выполняться как в автоматическом режиме без вмешательства пользователя, так и с уведомлением. После установки обновления компонентов программы может потребоваться перезагрузка компьютера.
- **Обновить компоненты сейчас** — обновляет компоненты программы до последней версии.

8.2.5.1 Обновление с зеркала

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

Доступ к файлам зеркала с помощью внутреннего HTTP-сервера

Это вариант по умолчанию, выбранный в предварительно заданной конфигурации программы. Для обеспечения доступа к зеркалу с помощью HTTP-сервера перейдите на вкладку **Дополнительные настройки** (F5) > **Обновление** > **Профили** > **Зеркало** и выберите элемент **Создать зеркало обновления**.

В разделе **HTTP-сервер** вкладки **Зеркало** можно указать **порт сервера**, на котором HTTP-сервер будет принимать запросы, а также тип **аутентификации**, используемой HTTP-сервером. По умолчанию порт сервера имеет значение **2221**. С помощью параметра **Аутентификация** определяется способ аутентификации, используемый для доступа к файлам обновлений. Доступны указанные ниже варианты. **Нет**, **Обычная** и **NTLM**.

- Выберите вариант **Обычная**, чтобы использовать кодировку base64 и упрощенную аутентификацию по имени пользователя и паролю.

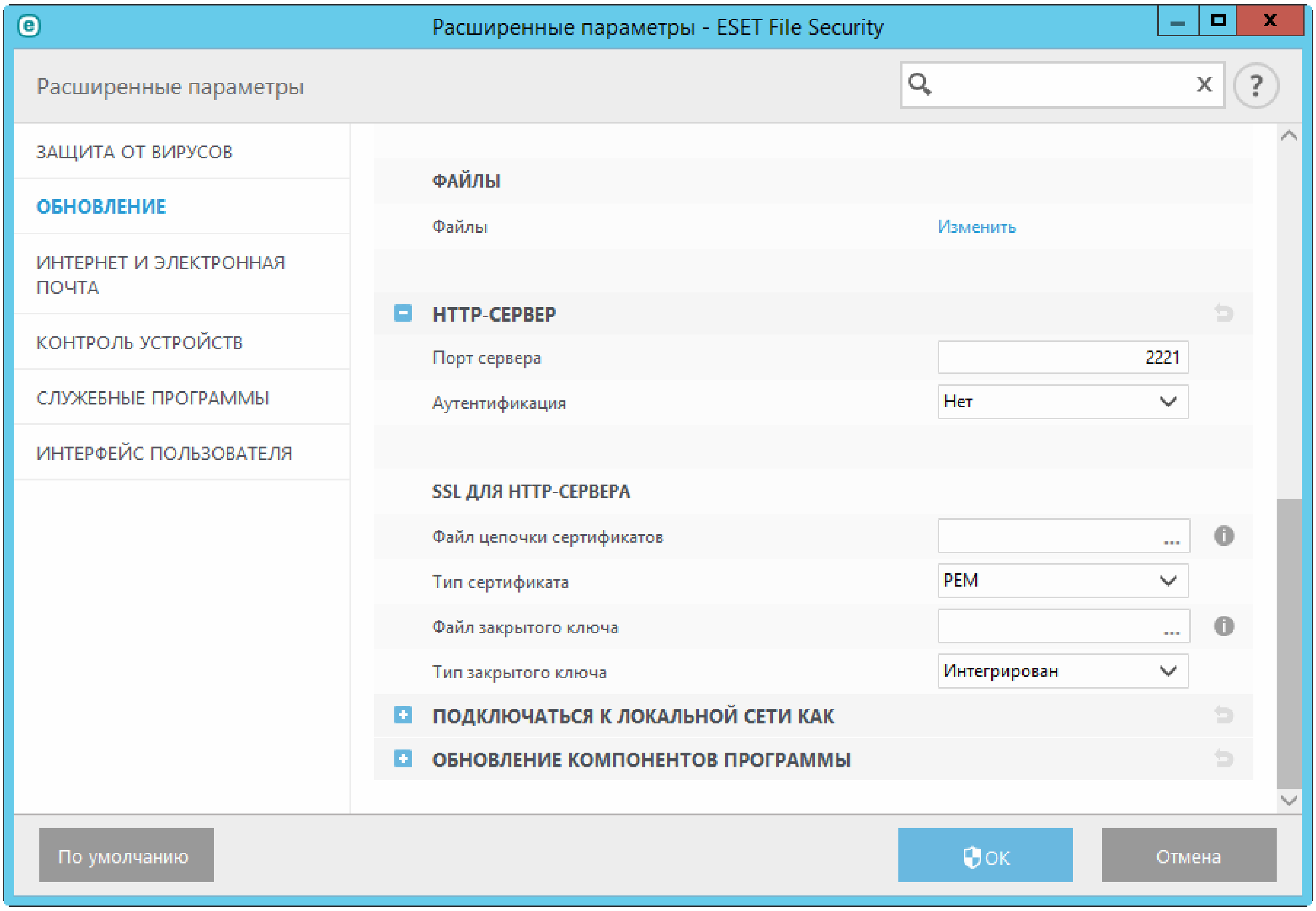
- Вариант **NTLM** обеспечивает шифрование с использованием безопасного способа шифрования. Для аутентификации используется учетная запись пользователя, созданная на рабочей станции, которая предоставляет общий доступ к файлам обновлений.
- Значение по умолчанию — **Нет**. Этот вариант обеспечивает доступ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

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

SSL для HTTP-сервера

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

ПРИМЕЧАНИЕ.
После нескольких неудачных попыток обновить базу данных сигнатур вирусов с зеркала в главном меню на вкладке «Обновление» появится ошибка **Неверные имя пользователя и (или) пароль**. Рекомендуем перейти в меню **Дополнительные настройки** (F5) > **Обновление** > **Профили** > **Зеркало** и проверить указанные имя пользователя и пароль. Обычно эта ошибка вызвана неправильными аутентификационными данными.



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

1. Откройте меню **Дополнительные настройки** (F5) и последовательно щелкните элементы **Обновление** > **Профили** > **Обычная**.
2. Снимите флажок **Выбирать автоматически** и добавьте в поле **Сервер обновлений** новый сервер в одном из таких форматов:

http://IP_адрес_нового_сервера:2221
https://IP_адрес_нового_сервера:2221 (если используется SSL)

Доступ к зеркалу через общие системные папки

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

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

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

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

1. Откройте меню ESET File Security **Дополнительные настройки** (F5) и последовательно щелкните элементы **Обновление** > **Профили** > **Обычная**.
2. Щелкните элемент **Сервер обновлений** и добавьте новый сервер, используя формат *\\UNC\ПУТЬ*.

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

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

8.2.5.2 Файлы с зеркала

Список доступных и локализованных файлов компонентов программы.

8.2.5.3 Устранение проблем при обновлении с зеркала

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

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

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

- **Ошибка при подключении ESET File Security к серверу зеркала**: подключение к порту, указанному для доступа к HTTP-версии зеркала, блокируется.

8.3 Интернет и электронная почта

В разделе **Интернет и электронная почта** можно настроить защиту почтового клиента, обеспечить защиту обмена данными через Интернет с помощью модуля защиты доступа в Интернет и контролировать интернет-протоколы, настроив фильтрацию протоколов. Эти функции имеют принципиально важно значение для защиты компьютера при обмене данными через Интернет.

Защита почтового клиента контролирует весь обмен данными по электронной почте, защищает от вредоносного кода и позволяет выбрать действие, которое следует выполнять при обнаружении заражения.

Защита доступа в Интернет отслеживает обмен данными между веб-браузерами и удаленными серверами и соответствует правилам для протоколов HTTP и HTTPS. Эта функция также позволяет блокировать, разрешать и исключать определенные URL-адреса.

Фильтрация протоколов — это расширенная защита протоколов приложений, которую предоставляет модуль сканирования ThreatSense. Эта функция работает автоматически вне зависимости от того, используется или нет веб-браузер или почтовый клиент. Кроме того, она работает для зашифрованных соединений (SSL/TLS).

> **ПРИМЕЧАНИЕ.**
> В ОС Windows Server 2008, Windows Server 2008 R2, Small Business Server 2008 и Small Business Server 2011 установка компонента **Интернет и электронная почта** по умолчанию отключена. Если нужно установить этот компонент, выберите тип установки **Выборочная**. Если решение ESET File Security уже установлено, вы можете запустить средство установки еще раз, чтобы изменить уже установленный продукт, добавив к нему компонент Интернет и электронная почта.

8.3.1 Фильтрация протоколов

Защиту протоколов приложений от вирусов обеспечивает модуль сканирования ThreatSense, в котором объединено множество современных методов сканирования для выявления вредоносных программ. Функция фильтрации протоколов работает автоматически вне зависимости от используемого веб-браузера и почтового клиента. Если фильтрация протоколов включена, ESET File Security будет проверять соединения, использующие протокол SSL или TLS. Выберите **Интернет и электронная почта** > SSL/TLS.

- «Включить фильтрацию содержимого протоколов приложений» — может использоваться для отключения фильтрации протоколов. Многие компоненты ESET File Security (защита доступа в Интернет, защита протоколов электронной почты, защита от фишинга) зависят от этого параметра и не смогут работать в случае его отключения.
- Исключенные приложения: позволяет исключить указанные приложения из фильтрации протоколов. Нажмите **Изменить** и выберите их из списка приложений.
- Исключенные IP-адреса: позволяет исключить указанные удаленные адреса из фильтрации протоколов.

> **ПРИМЕЧАНИЕ.**
> Исключения полезны, если фильтрация протоколов вызывает проблемы совместимости.

8.3.1.1 Исключенные приложения

Для исключения соединений определенных сетевых приложений из фильтрации содержимого выделите их в списке. Соединения выделенных приложений по протоколам HTTP/POP3 не будут проверяться на наличие угроз.

ВАЖНО!
Рекомендуется использовать эту возможность только для тех приложений, которые работают некорректно, если их соединения проверяются.

Доступны указанные ниже функции.

- Добавить — отображение приложений и служб, затронутых фильтрацией протоколов.
- **Изменить** — изменение приложения, выбранного в списке.
- **Удалить** — удаление приложения, выбранного в списке.

8.3.1.2 Исключенные IP-адреса

IP-адреса в этом списке будут исключены из фильтрации содержимого протоколов. Соединения по протоколам HTTP/POP3/IMAP, в которых участвуют выбранные адреса, не будут проверяться на наличие угроз.

ВАЖНО!
Этот параметр рекомендуется использовать только для заслуживающих доверия адресов.

Доступны указанные ниже функции.

- **Добавить** — добавление IP-адреса, диапазона адресов или подсети удаленной конечной точки, к которой применяется правило.

Выбрав элемент **Добавить несколько значений**, вы можете добавить несколько IP-адресов, разделенных переводом строки, запятыми или точками с запятой. Если разрешен ввод нескольких значений, адреса отображаются в виде списка исключенных IP-адресов.

- **Изменить** — изменение выбранного IP-адреса.
- **Удалить** — удаление выбранного IP-адреса из списка.

8.3.1.3 Клиенты Интернета и электронной почты

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 File Security основное внимание уделяется обеспечению безопасности веб-браузеров. Каждое приложение, обращающееся к сети, может быть помечено как веб-браузер. Приложения, которые уже использовали протоколы для передачи данных, и приложения, находящиеся по выбранному адресу, можно внести в список веб-клиентов и почтовых клиентов.

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 как технология платформы фильтрации Windows использует особые методы отслеживания, раздел **Веб-клиенты и почтовые клиенты** недоступен.

8.3.2 SSL/TLS

Программа ESET File Security может проверять на наличие угроз соединения, в которых используется протокол SSL/TLS. Вы можете 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/TLS: если фильтрация протоколов отключена, программа не сканирует соединения по протоколам SSL/TLS.

Режим фильтрации протокола SSL/TLS доступен в следующих вариантах:

- **Автоматический режим**: выберите этот вариант, чтобы сканировать все защищенные SSL/TLS-соединения, за исключением тех, которые защищены сертификатами, исключенными из проверки. Если устанавливается новое соединение, использующее неизвестный заверенный сертификат, пользователь не получит уведомления, а само соединение автоматически будет фильтроваться. При доступе к серверу с ненадежным сертификатом, который помечен пользователем как доверенный (добавлен в список доверенных сертификатов), соединение с этим сервером разрешается, а содержимое канала связи фильтруется.
- **Интерактивный режим**: при выполнении входа на новый защищенный протоколами SSL/TLS сайт (с неизвестным сертификатом) на экран выводится диалоговое окно выбора действий. Этот режим позволяет создавать список сертификатов SSL/TLS, которые будут исключены из сканирования.

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

Блокировать шифрованные подключения, использующие устаревший протокол SSL версии 2: соединения, использующие эту более раннюю версию протокола SSL, автоматически блокируются.

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

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

Срок действия сертификата

В некоторых случаях сертификат невозможно проверить с помощью хранилища доверенных корневых центров сертификации. Это значит, что сертификат уже подписан (например, администратором 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 хранилищем доверенных корневых центров сертификации. Если установлен флажок **Запрашивать срок действия сертификата** (по умолчанию), пользователю будет предложено выбрать действие, которое следует предпринять во время установки зашифрованного соединения. Можно выбрать вариант **Блокировать подключения, использующие данный сертификат**, чтобы всегда разрывать зашифрованные соединения с сайтами, использующими непроверенные сертификаты.

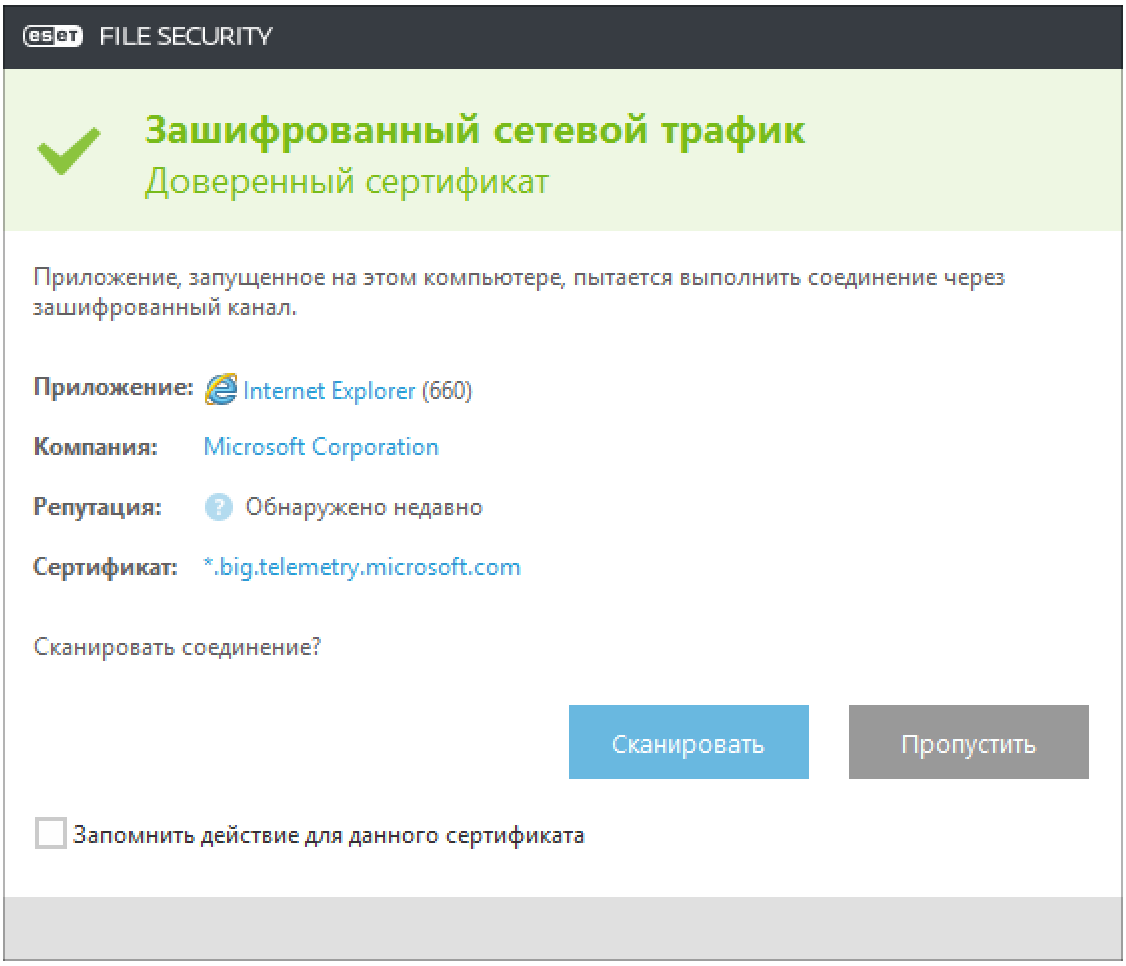
Если сертификат недействителен или поврежден, это значит, что истек срок действия сертификата или же используется недопустимая подпись. В этом случае рекомендуется выбрать элемент **Блокировать подключения, использующие данный сертификат**.

8.3.2.1 Шифрованное соединение SSL

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

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

Во-вторых, если в качестве **режима фильтрации протокола SSL** выбран **интерактивный режим**, то при подключении к любому веб-сайту будет отображаться запрос на **сканирование** или **игнорирование**. Некоторые приложения проверяют SSL-трафик на предмет изменений и мониторинга. В таких случаях для сохранения работоспособности приложения программа ESET File Security должна SSL-трафик **игнорировать**.



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

8.3.2.2 Список известных сертификатов

Список известных сертификатов позволяет настроить поведение ESET File Security в отношении конкретных сертификатов SSL/TLS, а также настроить запоминание действий пользователя в интерактивном режиме фильтрации протокола SSL/TLS. Для просмотра и управления списком нажмите кнопку **Изменить** возле элемента **Список известных сертификатов**.

Доступны следующие действия:

- **Добавить** — добавление сертификата из URL-адреса или файла.
- **Изменить** — выберите сертификат, который нужно настроить, и нажмите кнопку **Изменить**.
- **Удалить** — выберите сертификат, который нужно удалить, и нажмите кнопку **Удалить**.

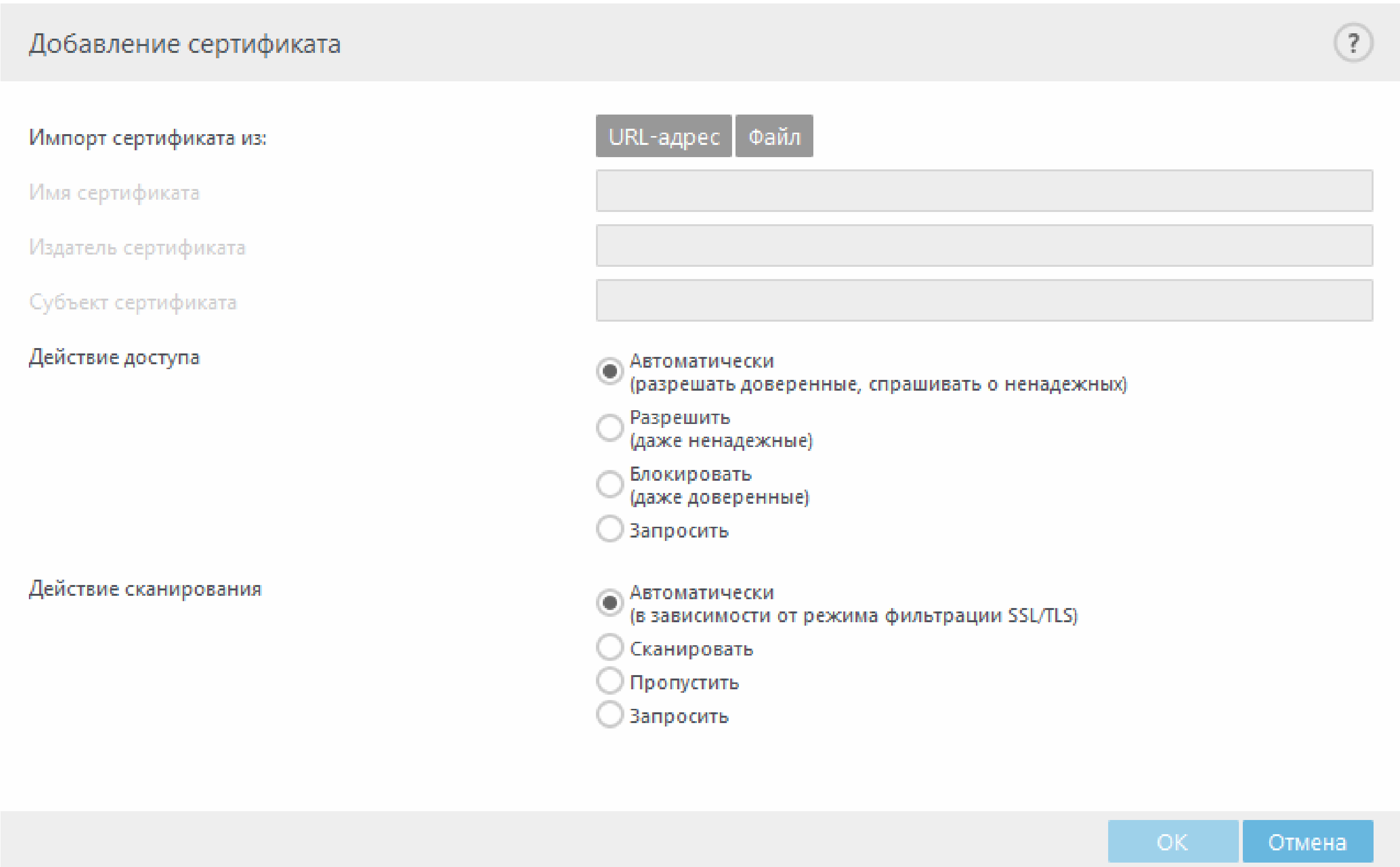
После открытия окна **Добавление сертификата** нажмите кнопку **URL-адрес** или **Файл** и укажите URL-адрес сертификата либо найдите файл сертификата. На основе данных этого сертификата автоматически заполняются следующие поля:

- **Имя сертификата** — собственно имя сертификата.
- **Издатель сертификата** — имя создателя сертификата.
- **Субъект сертификата** — в этом поле можно указать сущность, которой принадлежит открытый ключ, содержащийся в поле открытого ключа субъекта.

Можно настроить следующие параметры.

- Выберите **Разрешить** или **Заблокировать** в качестве значения параметра **Действие доступа**, чтобы разрешить или заблокировать обмен данными, защищенный этим сертификатом, вне зависимости от его надежности. Чтобы разрешать доверенные сертификаты и предлагать варианты действий для ненадежных, выберите значение **Автоматически**. Выберите вариант **Запросить**, чтобы получать запрос при обнаружении определенного сертификата.

- Выберите значение **Сканировать** или **Пропустить** для параметра **Действие сканирования**, чтобы сканировать или игнорировать соединение, защищенное сертификатом. Чтобы сканировать в автоматическом режиме и запрашивать действия в интерактивном, выберите элемент **Автоматически**. Выберите вариант **Запросить**, чтобы получать запрос при обнаружении определенного сертификата.



Нажмите кнопку **OK**, чтобы сохранить внесенные изменения, или кнопку **Отмена**, чтобы выйти без сохранения.

8.3.3 Защита почтового клиента

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

Интеграция с почтовым клиентом

В настоящий момент поддерживаются следующие почтовые клиенты: Microsoft Outlook, Outlook Express, почта Windows и почта Windows Live. Защита электронной почты реализована в этих программах в виде подключаемого модуля. Главное преимущество подключаемого модуля заключается в том, что он не зависит от используемого протокола. При получении почтовым клиентом зашифрованного сообщения оно расшифровывается и передается модулю сканирования. Полный список поддерживаемых почтовых клиентов и их версий см. в следующей статье базы знаний.

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

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

Сканируемая электронная почта

Полученные сообщения — включает или отключает проверку входящих сообщений.
Отправленные сообщения — включает или отключает проверку отправленных сообщений.
Прочитанные сообщения — включает или отключает проверку прочитанных сообщений.

Действие, применяемое к зараженному сообщению

Ничего не предпринимать — в этом случае программа будет выявлять зараженные вложения, но не будет выполнять никаких действий с сообщениями электронной почты.
Удалить сообщение — программа будет уведомлять пользователя о заражениях и удалять сообщения.
Переместить сообщение в папку "Удаленные" — зараженные сообщения будут автоматически перемещаться в папку «Удаленные».
Переместить сообщение в папку — зараженные сообщения будут автоматически перемещаться в указанную папку.

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

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

Принять результаты сканирования из других модулей — если установлен этот флажок, модуль защиты электронной почты будет принимать результаты сканирования от других модулей защиты (сканирование каталогов POP3, IMAP).

8.3.3.1 Протоколы электронной почты

Включить защиту электронной почты с помощью фильтрации протоколов: IMAP и POP3 — самые распространенные протоколы, используемые для получения электронной почты в почтовых клиентах. ESET File Security обеспечивает защиту этих протоколов вне зависимости от используемого почтового клиента.

ESET File Security также поддерживает сканирование протоколов IMAPS и POP3S, которые для передачи информации между сервером и клиентом используют зашифрованный канал. ESET File Security проверяет соединения, использующие методы шифрования SSL и TLS. Программа будет выполнять сканирование трафика только на портах, которые указаны как использующие протокол IMAPS/POP3S, вне зависимости от версии операционной системы.

Настройка модуля сканирования IMAPS/POP3S: зашифрованные соединения не будут сканироваться, если используются параметры по умолчанию. Чтобы включить сканирование зашифрованных соединений, перейдите к элементу Проверка протоколов SSL/TLS.

По номеру порта определяется тип порта. Ниже приведены порты, используемые по умолчанию.

Имя порта	Номер порта	Описание
POP3	110	Используемый по умолчанию незашифрованный порт POP3.
IMAP	143	Используемый по умолчанию незашифрованный порт IMAP.
Защищенный протокол IMAP (IMAP4-SSL)	585	Включение фильтрации протокола SSL/TLS. Номера портов следует разделять запятыми.
IMAP4 по SSL (IMAPS)	993	Включение фильтрации протокола SSL/TLS. Номера портов следует разделять запятыми.
Защищенный протокол POP3 (SSL-POP)	995	Включение фильтрации протокола SSL/TLS. Номера портов следует разделять запятыми.

8.3.3.2 Предупреждения и уведомления

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

Чтобы настроить параметры этой функции, в разделе **Дополнительные настройки** последовательно щелкните элементы **Интернет и электронная почта** > **Защита почтового клиента** > **Предупреждения и уведомления**.

Параметры ThreatSense: расширенная настройка модуля сканирования для защиты от вирусов, которая позволяет настраивать объекты сканирования, способы обнаружения и т. д. Щелкните этот элемент, чтобы отобразилось окно тщательной настройки модуля сканирования.

После проверки к сообщению электронной почты может быть прикреплено уведомление с результатами сканирования. Можно выбрать такие варианты: **Добавлять уведомление к полученным и прочитанным сообщениям электронной почты, Добавлять примечание в поле темы полученных и прочитанных зараженных сообщений** или **Добавлять уведомление к отправленным сообщениям**. Обратите внимание, что в некоторых случаях уведомления могут быть опущены в проблемных HTML-сообщениях или сфабрикованы некоторыми вирусами. Уведомления могут быть добавлены к входящим и прочитанным сообщениям или к исходящим сообщениям (или и к тем, и к другим). Доступны следующие варианты.

- **Никогда**: уведомления не будут добавляться вообще.
- **Только к зараженным сообщениям**: будут отмечены только сообщения, содержащие злонамеренные программы (по умолчанию).

- **Ко всем сканируемым сообщениям**: программа будет добавлять уведомления ко всем сканируемым сообщениям электронной почты.

Добавлять примечание в поле темы отправленных зараженных сообщений: установите этот флажок, если необходимо, чтобы защита электронной почты добавляла предупреждения о вирусах в тему зараженных сообщений. Эта функция позволяет осуществлять простую фильтрацию зараженных сообщений по теме (если поддерживается почтовым клиентом). Кроме того, она повышает уровень доверия получателя, а в случае обнаружения заражения предоставляет важную информацию об уровне угрозы для конкретного сообщения 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%* обозначает обнаруженную угрозу.

8.3.3.3 Панель инструментов MS Outlook

Защита Microsoft Outlook работает в виде подключаемого модуля. После установки ESET File Security панель инструментов, содержащая приведенные ниже функции защиты от вирусов, добавляется в Microsoft Outlook.

ESET File Security: если щелкнуть этот значок, откроется главное окно ESET File Security.

Повторно сканировать сообщения — позволяет запустить проверку электронной почты вручную. Можно указать сообщения, которые будут проверяться, и активировать повторное сканирование полученных сообщений. Для получения дополнительных сведений см. раздел Защита почтового клиента.

Настройки модуля сканирования — на экран выводятся параметры защиты почтового клиента.

8.3.3.4 Панель инструментов Outlook Express и Почты Windows

Защита для Outlook Express и почты Windows функционирует в качестве подключаемого модуля. После установки ESET File Security панель инструментов, содержащая приведенные ниже функции защиты от вирусов, добавляется в Outlook Express или Почту Windows.

ESET File Security: если щелкнуть этот значок, откроется главное окно программы ESET File Security.

Повторно сканировать сообщения: позволяет запустить проверку электронной почты вручную. Можно указать сообщения, которые будут проверяться, и активировать повторное сканирование полученных сообщений. Для получения дополнительных сведений см. раздел Защита почтового клиента.

Настройки модуля сканирования: на экран выводятся параметры защиты почтового клиента.

Интерфейс пользователя

Настроить вид: этот параметр позволяет изменить внешний вид панели инструментов в почтовом клиенте. Для того чтобы настроить внешний вид независимо от параметров почтового клиента, снимите этот флажок.

Показывать надписи: отображение описаний значков.

Текст справа: описания размещаются не снизу, а справа от значков.

Большие значки: отображение в меню значков крупного размера.

8.3.3.5 Окно подтверждения

Это уведомление предназначено для подтверждения того, что пользователю действительно нужно выполнить выбранное действие, и для предотвращения тем самым возможных ошибок. В окне также есть возможность отключить подтверждения.

8.3.3.6 Повторное сканирование сообщения

Панель инструментов ESET File Security, интегрированная в почтовые клиенты, дает пользователю возможность указать ряд параметров для проверки электронной почты. С помощью параметра **Повторно сканировать сообщения** можно включить два описанные далее режима сканирования.

Все сообщения в текущей папке: сканируются сообщения в отображаемой в данный момент папке.

Только выбранные сообщения: сканируются только помеченные пользователем сообщения.

Повторно сканировать уже сканированные сообщения — дает пользователю возможность выполнить еще одно сканирование сообщений, которые уже были просканированы ранее.

8.3.4 Защита доступа в Интернет

Функция защиты доступа в Интернет отслеживает соединения между веб-браузерами и удаленными серверами, чтобы обеспечить защиту от интернет-угроз. Данная функция работает в соответствии с правилами протоколов HTTP (протокол передачи гипертекста) и HTTPS (зашифрованный обмен данными).

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

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

- Основная — позволяет включать и отключать защиту доступа в Интернет. Если защита отключена, перечисленные ниже параметры станут неактивными.

Веб-протоколы — дает возможность настроить отслеживание для стандартных протоколов, которые используются в большинстве веб-браузеров.

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

> **ПРИМЕЧАНИЕ.**
> В Windows Vista и более поздних версиях, HTTP-трафик отслеживается для всех портов и приложений. В Windows XP/2003 можно изменить порты, используемые протоколом HTTP, последовательно выбрав элементы **Дополнительные настройки** (F5) > **Интернет и электронная почта** > **Защита доступа в интернет** > **Веб-протоколы** > **Настройка модуля сканирования HTTP**. HTTP-трафик всех приложений отслеживается на указанных портах для всех приложений и на всех портах для приложений, помеченных как веб-клиенты и почтовые клиенты.

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

По умолчанию сканирование зашифрованных соединений отключено. Чтобы включить сканирование зашифрованных соединений, перейдите к элементу Проверка протокола SSL в разделе «Дополнительные настройки» (**F5**), выберите элементы **Интернет и электронная почта** > **Проверка протокола SSL**, а затем щелкните **Включить фильтрацию протокола SSL**.

- Управление URL-адресами — здесь можно задавать HTTP-адреса, которые следует блокировать, разрешать или исключать из проверки.

- Параметр ThreatSense — дает возможность настраивать определенные параметры, например тип сканирования (сообщения электронной почты, архивы, исключения, ограничения и т. д.) и метод обнаружения для защиты доступа в Интернет.

8.3.4.1 Основная информация

Укажите, нужно ли включить (по умолчанию) или отключить **защиту доступа в Интернет**. Если защита отключена, перечисленные ниже параметры станут неактивными.

ПРИМЕЧАНИЕ.
Настоятельно рекомендуется не отключать защиту доступа в Интернет. Кроме того, чтобы получить доступ к этой функции, в главном окне программы ESET File Security выберите **Настройка** > **Компьютер** > **Защита доступа в Интернет**.

8.3.4.2 Управление URL-адресами

В разделе управления URL-адресами можно задавать HTTP-адреса, которые будут блокироваться, разрешаться или исключаться из проверки. Нажмите **Изменить** для создания списка в дополнение к предварительно заданным. Это может быть полезно, если вы хотите логически разделить разные группы адресов.

ПРИМЕР
Один список заблокированных адресов может содержать адреса, полученные из внешнего общедоступного черного списка, а второй — адреса, добавленные вами. Таким образом внешний список можно легко обновить, не внося изменений в ваш личный список.

- Посещение веб-сайтов из списка заблокированных адресов невозможно, кроме случаев, когда их адреса также добавлены в список разрешенных.

- Веб-сайты из списка адресов, для которых отключена проверка, загружаются без проверки на вредоносный код.

Параметр Фильтрация протоколов SSL/TLS должен быть включен в случае, когда кроме HTTP-сайтов требуется фильтровать также сайты, использующие протокол HTTPS. В противном случае в список добавляются только посещенные вами домены HTTPS-сайтов, а не полный URL-адрес.

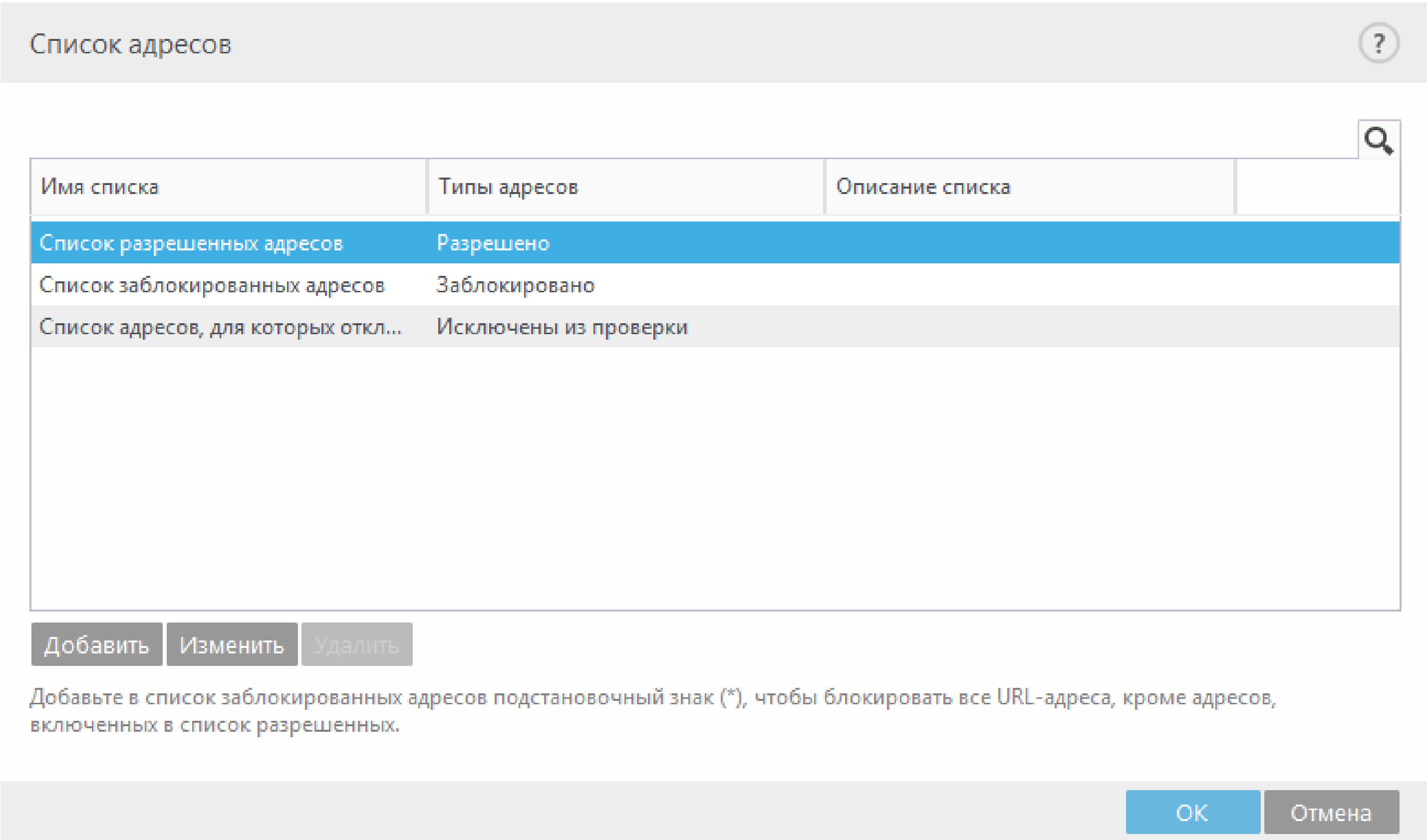
Во всех списках можно использовать символы «*» (звездочка) и «?» (вопросительный знак). Звездочка означает любое количество символов, а вопросительный знак — только один символ. Работать с содержимым списка исключенных адресов следует особенно аккуратно, так как он должен содержать только доверенные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

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

8.3.4.2.1 Список адресов

По умолчанию доступны следующие три списка.

- **Список адресов, для которых отключена проверка**. Для всех добавленных в этот список адресов не будет выполняться проверка на наличие вредоносного кода.
- **Список разрешенных адресов** — если установлен флажок «Предоставить доступ только к разрешенным HTTP-адресам», а в списке заблокированных адресов указан символ звездочки («*» — блокировать все адреса без исключений), пользователю будет предоставлен доступ только к разрешенным адресам. Адреса в этом списке остаются доступными, даже если они включены в список заблокированных адресов.
- **Список заблокированных адресов** — пользователь не сможет получить доступ к адресам из этого списка, если они не включены также в список разрешенных адресов.



Добавить. Добавление нового URL-адреса в список (если адресов несколько, их следует указывать через разделитель).

Изменить. Изменение существующего адреса в списке. Удалять можно только те адреса, которые были добавлены посредством команды «Добавить».

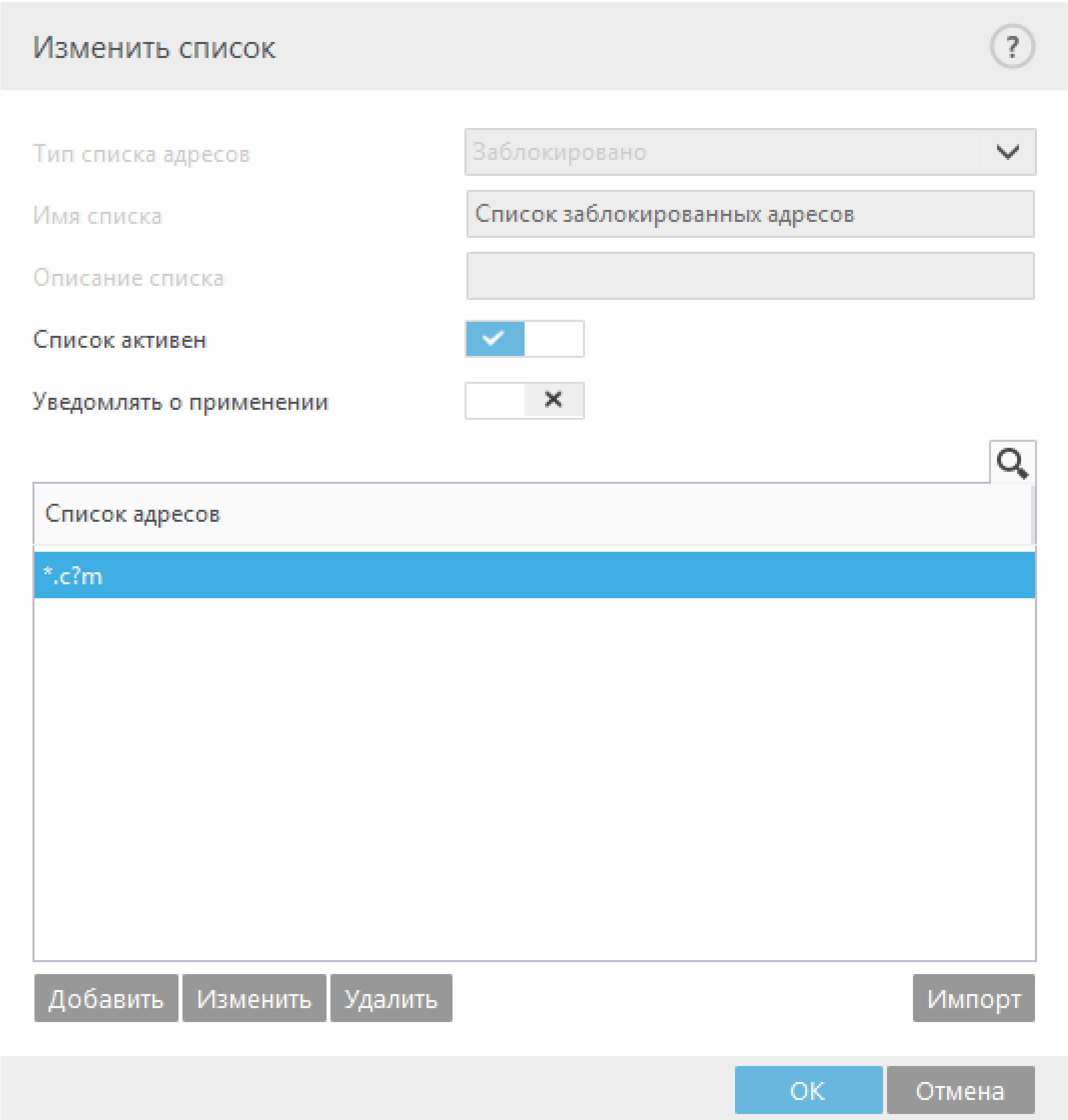
Удалить. Удаление адресов из списка. Удалять можно только те адреса, которые были добавлены посредством команды «Добавить».

8.3.4.2.1.1 Создание списка

Можно создать новый список в дополнение к предварительно определенным списка́м адресов. В списке будут содержаться требуемые URL-адреса/маски доменов, которые будут блокироваться, разрешаться или исключаться из проверки. При создании нового списка укажите следующее:

- **Тип списка адресов** — выберите тип (**Исключены из проверки**, **Заблокированы** или **Разрешены**) в раскрывающемся списке.
- **Имя списка** — укажите название списка. При изменении одного из трех предварительно заданных списков это поле будет неактивно.
- **Описание списка** — введите краткое описание списка (необязательно). При изменении одного из трех предварительно заданных списков поле будет неактивно.
- **Список активен** — данный переключатель позволяет деактивировать список. При необходимости его можно позже активировать.
- **Уведомлять о применении** — воспользуйтесь этим параметром, если требуется получать уведомления о том, что при оценке посещенного HTTP-сайта использовался определенный список.

ПРИМЕР
Когда доступ к веб-сайту блокируется или разрешается по причине его присутствия в списке заблокированных или разрешенных адресов, отображается соответствующее уведомление, в котором указывается имя списка, где фигурирует этот веб-сайт.



Нажмите **Добавить**, чтобы указать URL-адрес/маску домена. Выберите адрес из списка и щелкните **Удалить**, чтобы удалить его. Щелкните **Изменить**, чтобы внести изменения в существующую запись.

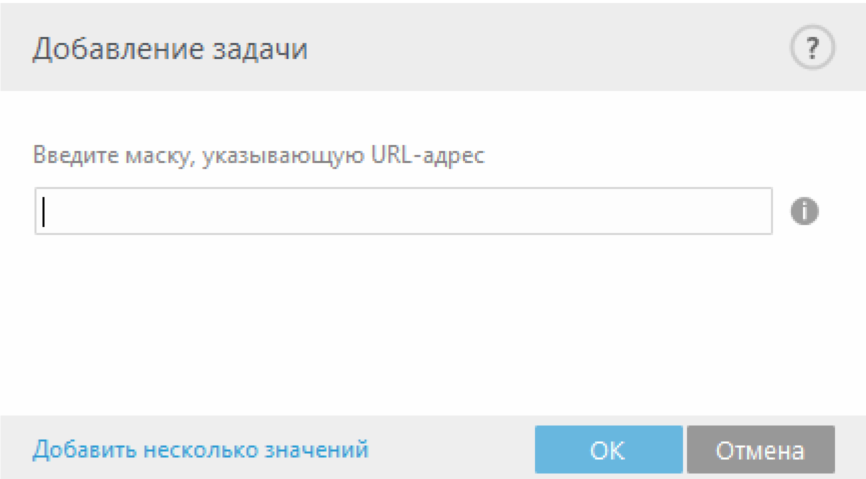
ПРИМЕЧАНИЕ.
Удалить можно только пользовательские списки адресов.

ESET File Security позволяет пользователям блокировать доступ к указанным веб-узлам и предотвращать отображение их содержимого в веб-браузере. Пользователь может указать адреса, которые необходимо исключить из проверки. Если полное имя удаленного сервера неизвестно или пользователь хочет указать группу удаленных серверов, то для идентификации такой группы можно использовать так называемые маски. Эти маски обозначаются символами «?» и «*».

- Используйте «?», чтобы заменить любой символ.
- Используйте «*», чтобы заменить текстовую строку.

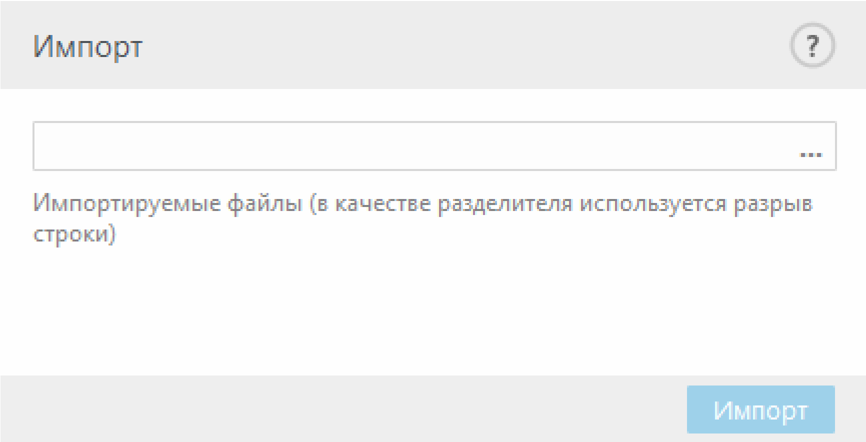
ПРИМЕР
**.c?m* применяется ко всем адресам, у которых последняя часть начинается с буквы «c», заканчивается буквой «m» и содержит неизвестный символ между ними (например, .com, .cam и т. д.).

Начальная последовательность «*.» перед именем домена интерпретируется особым образом. Прежде всего, в данном случае подстановочный знак «*» не может представлять символ косой черты («/»). Смысл этого исключения — избежать обхода маски, например маска *.domain.com не будет соответствовать адресу *http://любой_домен.com/любой_путь#.domain.com* (такой суффикс можно присоединить к любому URL-адресу, не влияя на загрузку). Вторая особенность в том, что «*.» в этом особом случае также соответствует пустой строке. Это дает возможность обозначить одной маской целый домен, включая все возможные поддомены. Например, маска *.domain.com также соответствует *http://domain.com*. Использовать маску **domain.com* было бы неверно, поскольку она также совпала бы с *http://anotherdomain.com*.



Выбрав параметр **Добавить несколько значений**, вы можете добавлять несколько расширений файлов, разделенных переводом строки, запятыми или точками с запятой. Если разрешен ввод нескольких значений, адреса будут отображаться в виде списка.

- **Импорт** — импортируйте текстовый файл с URL-адресами (в качестве разделителя следует использовать разрыв строки, например `*.txt` с кодировкой UTF-8).



8.3.5 Защита от фишинга

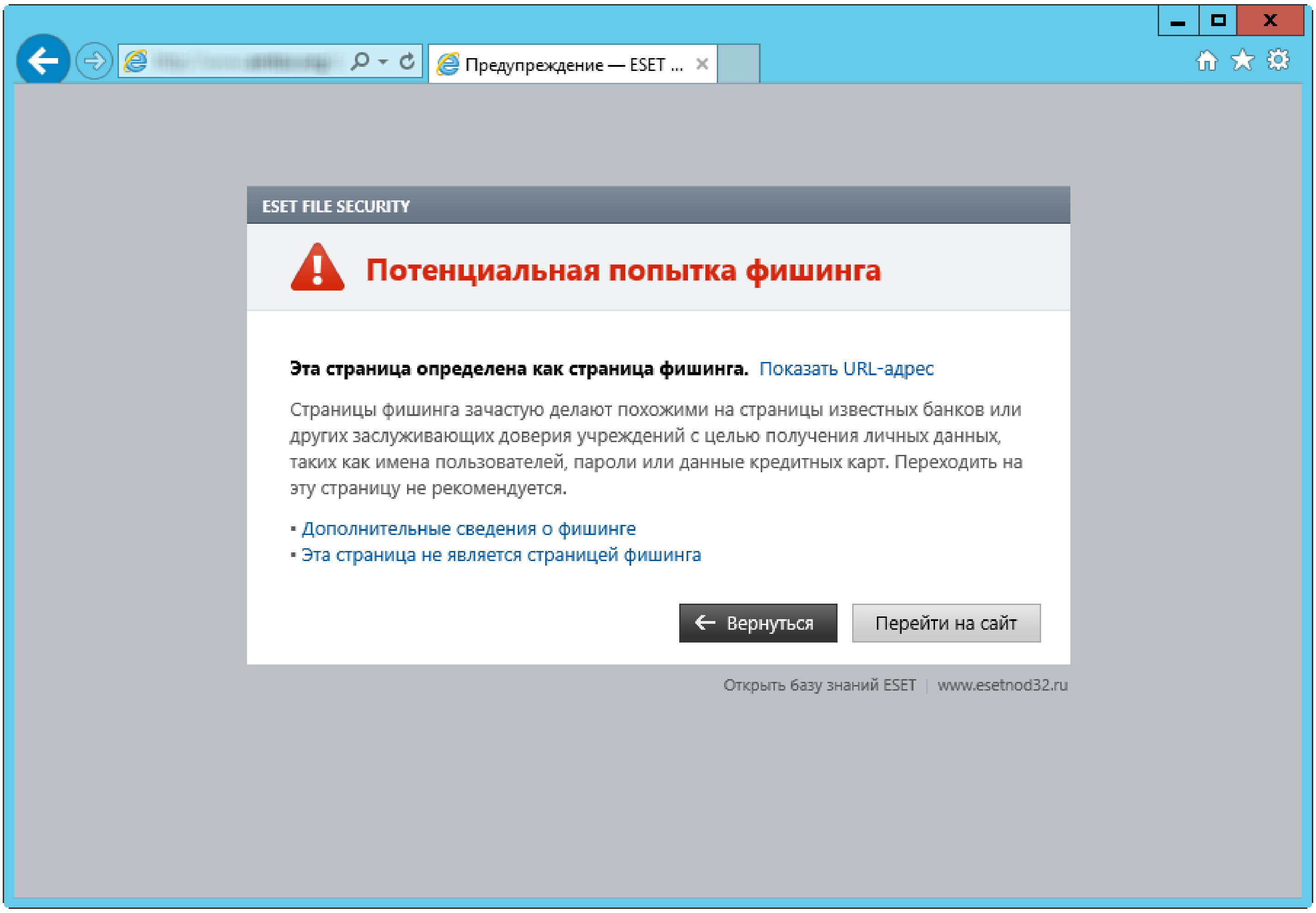
Термин «фишинг» обозначает преступную деятельность, в рамках которой используется социальная инженерия (манипулирование пользователями, направленное на получение конфиденциальной информации). Фишинг часто используется для получения доступа к конфиденциальным сведениям, таким как номера банковских счетов,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

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

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

Доступ к фишинговому веб-сайту

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



ПРИМЕЧАНИЕ.
Время, в течение которого можно получить доступ к потенциальному фишинговому веб-сайту, занесенному в «белый» список, по умолчанию ограничивается несколькими часами. 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, 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.).

8.4 Контроль устройств

ESET File Security обеспечивает автоматический контроль устройств (компакт- и DVD-дисков, USB-устройств). 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- или DVD-диск;
- USB-принтер;
- FireWire-хранилище;
- устройство Bluetooth;
- устройство чтения смарт-карт;
- устройство обработки изображений;
- модем;
- LPT/COM-порт;
- переносное устройство;
- все типы устройств.

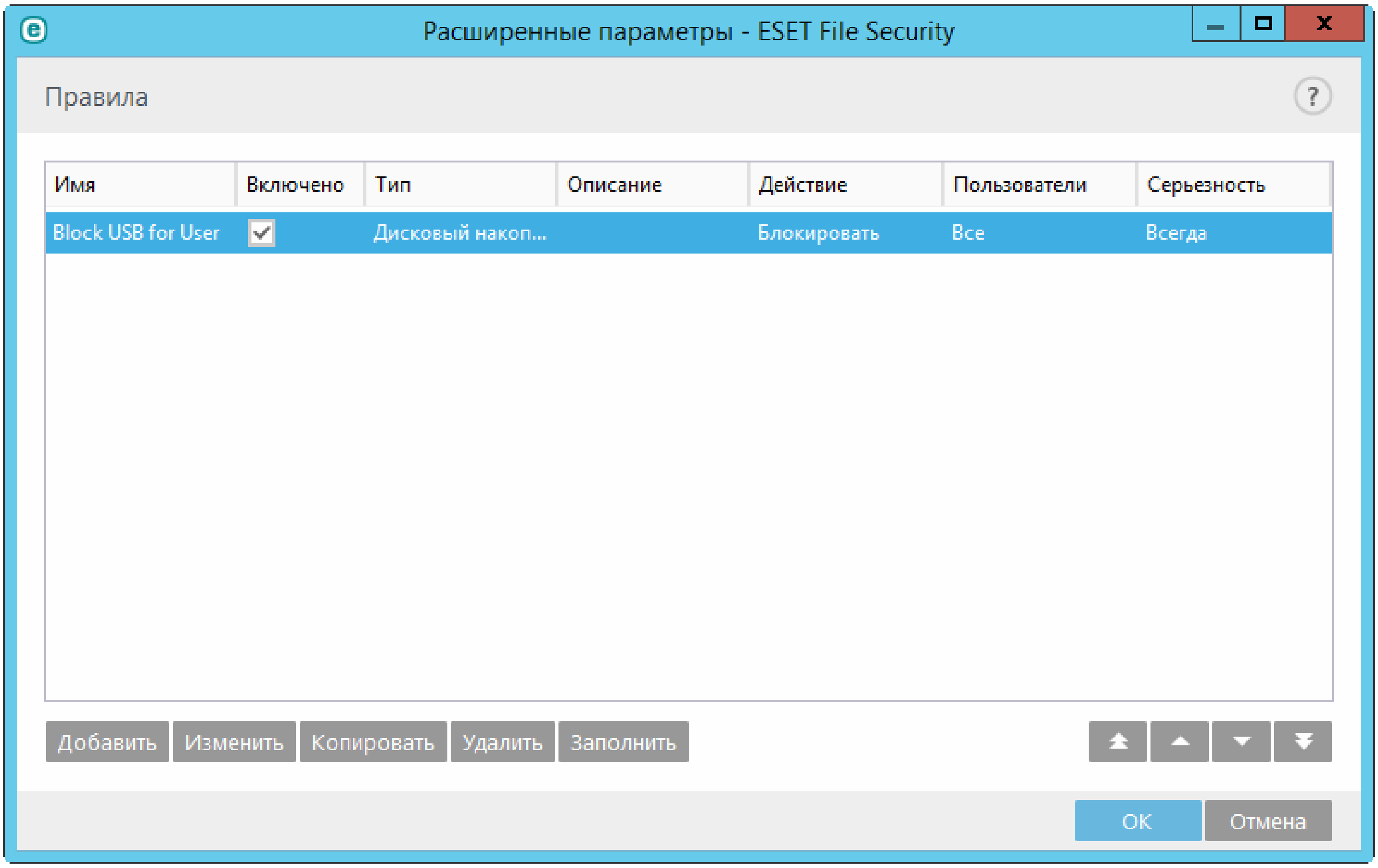
Если рядом с параметром **Интеграция с системой** включить переключатель, в программе ESET File Security включается функция контроля устройств. Чтобы это изменение вступило в силу, необходимо перезапустить компьютер.

Правила и Группы функции контроля устройств станут активными, что позволит изменить их параметры.

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

8.4.1 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, их групп или в соответствии с несколькими дополнительными параметрами, которые задаются в конфигурации правил. Список правил содержит несколько описаний для каждого правила, в частности его имя, тип внешнего устройства, выполняемое действие при обнаружении устройства и серьезность для записи в журнал.

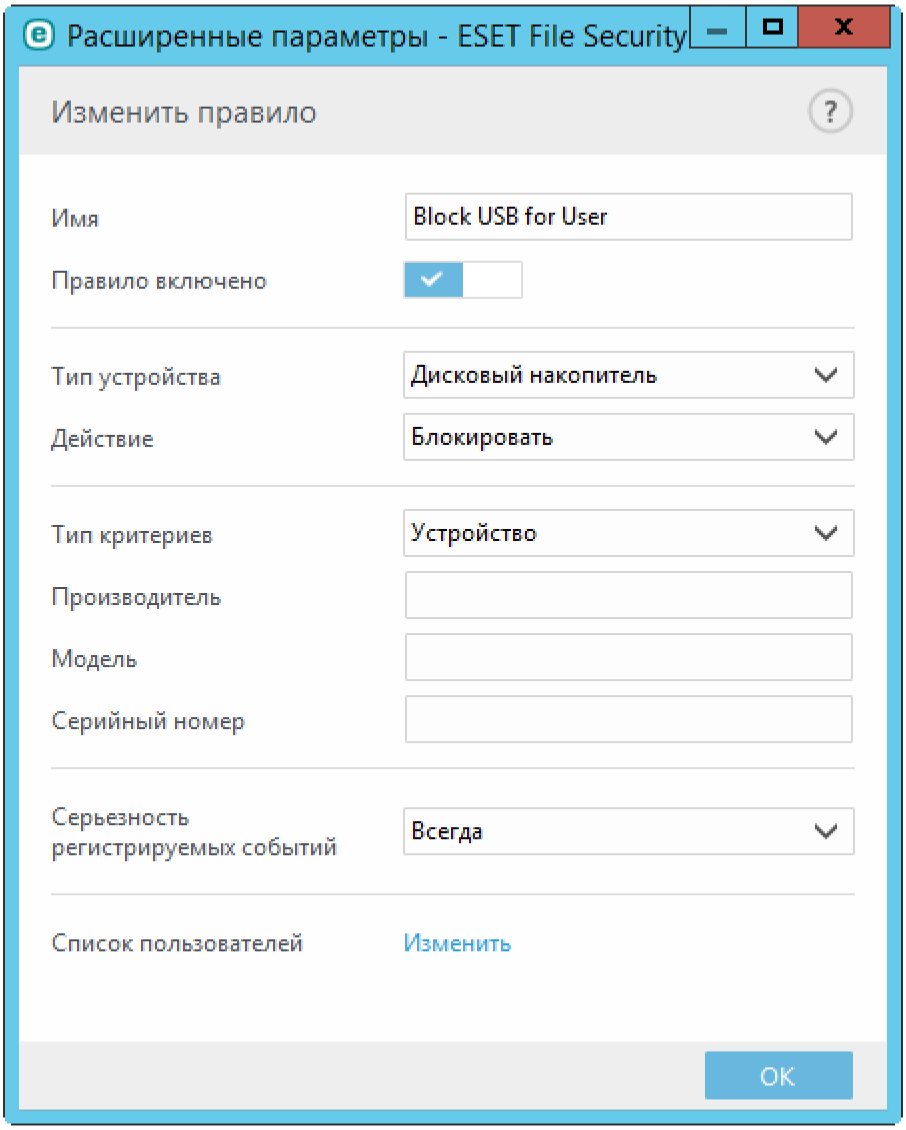
Для управления правилами используйте следующие кнопки в нижней части окна.

- Добавить — добавление нового правила.
- Изменить — изменение настроек существующего правила.
- **Копировать** — с помощью этой команды создается правило на основе параметров выбранного правила.
- **Удалить** — удаление выбранного правила. Кроме того, можно воспользоваться флажком рядом с тем или иным правилом, чтобы отключить его. Это может быть полезно, если вы не хотите полностью удалять правило и собираетесь воспользоваться им позднее.
- Заполнить — обнаружение параметров для съемных носителей, подключенных к компьютеру.
- Правила приведены в порядке их приоритета: правила с более высоким приоритетом располагаются вверху. Чтобы выделить несколько правил и применить к ним необходимые действия, например удалить или переместить к началу либо концу списка, воспользуйтесь элементами **Сверху/Вверх/Вниз/Снизу** (кнопки со стрелками).

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

8.4.2 Добавление правил контроля устройств

Правило контроля устройств определяет действие, выполняемое при подключении к компьютеру устройств, которые соответствуют заданным критериям.



Чтобы упростить идентификацию правила, введите его описание в поле **Имя**. Чтобы включить или отключить это правило, щелкните переключатель рядом с элементом **Правило включено**. Это может быть полезно, если полностью удалять правило не нужно.

Тип устройства

В раскрывающемся меню выберите тип внешнего устройства (дисковый накопитель, портативное устройство, Bluetooth, FireWire и т. д.). Список типов устройств предоставляет операционная система. Их можно просмотреть с помощью диспетчера устройств, в котором отображается все подключенное к компьютеру оборудование. 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 создания изображений являются сканеры или камеры, эти устройства не предоставляют информацию о пользователях, а только информацию об их действиях. Это означает, что устройства обработки изображений могут быть заблокированы 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, разрешено это устройство или заблокировано, и при этом создается запись журнала. Устройства не запоминаются. Уведомления отображаются при каждом повторном подключении одного и того же устройства.

Обратите внимание, что не для всех типов устройств доступен полный список прав (действий). Если на устройстве есть место для хранения данных, будут доступны все четыре действия. Если устройства не предназначены для хранения данных, доступны только два действия (например, право **Только чтение** неприменимо к Bluetooth-устройствам: доступ к ним можно только разрешить или заблокировать).

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 не указать три описанные выше дескриптора, то правило будет игнорировать их при проверке устройств. Для параметров фильтрации во всех текстовых полях не учитывается регистр и не поддерживаются подстановочные знаки (*, ?).

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

- **Всегда** — записываются все события.
- **Диагностика** — регистрируется информация, необходимая для тщательной настройки программы.
- **Информация** — в журнал вносятся информационные сообщения, в том числе сообщения об успешном выполнении обновления, а также все перечисленные выше записи.
- **Предупреждение** — записывается информация обо всех критических ошибках и предупреждениях.
- **Ничего** — журналы не создаются.

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.
С помощью правил пользователя можно фильтровать все устройства (например, устройства обработки изображений предоставляют информацию только о вызванных действиях, но не о пользователях).

8.4.3 Обнаруженные устройства

С помощью кнопки **Заполнить** можно ознакомиться со следующей информацией о подключенных на данный момент устройствах: тип устройства, производитель, модель и серийный номер (если есть). Если выбрать устройство в списке обнаруженных устройств и нажать кнопку **ОК**, в открывшемся окне редактора правил можно ознакомиться с предварительно заданной информацией (все параметры можно настраивать).

8.4.4 Группы устройств

Окно групп устройств разделено на две части. В правой части окна отображается список устройств, входящих в выбранную группу, а в левой части — список созданных групп. Выберите группу, содержащую устройства, которые нужно отобразить на правой панели.

ВНИМАНИЕ!
Наличие внешнего устройства, подключенного к компьютеру, может представлять угрозу безопасности.

Открыв окно групп устройств и выбрав группу, вы можете добавлять устройства в список или удалять их из него. Добавлять устройства в группу также можно посредством импорта данных об устройствах из файла. Или же можно нажать кнопку **Заполнить**. В этом случае все устройства, подключенные к компьютеру, отобразятся в окне **Обнаруженные устройства**. Выберите устройства из этого списка и нажмите кнопку **ОК**, чтобы добавить их в группу.

ПРИМЕЧАНИЕ.
Вы можете создать разные группы устройств, к которым будут применяться разные правила. Можно также создать одну группу устройств, настроенную для **чтения и записи** или **только для чтения**. Благодаря этому, когда к компьютеру подключаются нераспознанные устройства, функция контроля устройств их блокирует.

Доступны указанные ниже функции.

- **Добавить**: создание новой группы устройств путем ввода имени или добавление устройства в существующую группу (в зависимости от того, где именно нажата кнопка). При необходимости можно указать такие сведения, как имя поставщика, модель и серийный номер.
- **Изменить** — позволяет изменить имя выбранной группы или параметры устройств, которые она содержит (производитель, модель, серийный номер).
- **Удалить** — удаляет выбранную группу или устройство (в зависимости от того, в какой части окна нажата кнопка).
- **Импорт** — импорт списка серийных номеров устройств из файла.
- Заполнить — обнаружение параметров для съемных носителей, подключенных к компьютеру.

Завершив настройки, нажмите кнопку **ОК**. Чтобы закрыть окно **Группы устройств** без сохранения изменений, нажмите кнопку **Отмена**.

ПРИМЕЧАНИЕ.
Обратите внимание, что полный список действий (разрешений) доступен не для всех типов устройств. Все четыре действия доступны для запоминающих устройств. Если устройство не предназначено для хранения данных, доступны будут только три действия. Например, право **Только чтение** неприменимо к Bluetooth-устройствам, поэтому доступ к ним можно только разрешить, заблокировать или разрешить с предупреждением.

8.5 Сервис

Ниже приведены дополнительные параметры для всех служебных программ, доступных на вкладке **Служебные программы** в главном окне программы ESET File Security.

- Файлы журналов
- Прокси-сервер
- Уведомление по электронной почте
- Режим презентации
- Диагностика
- Кластер

8.5.1 ESET LiveGrid

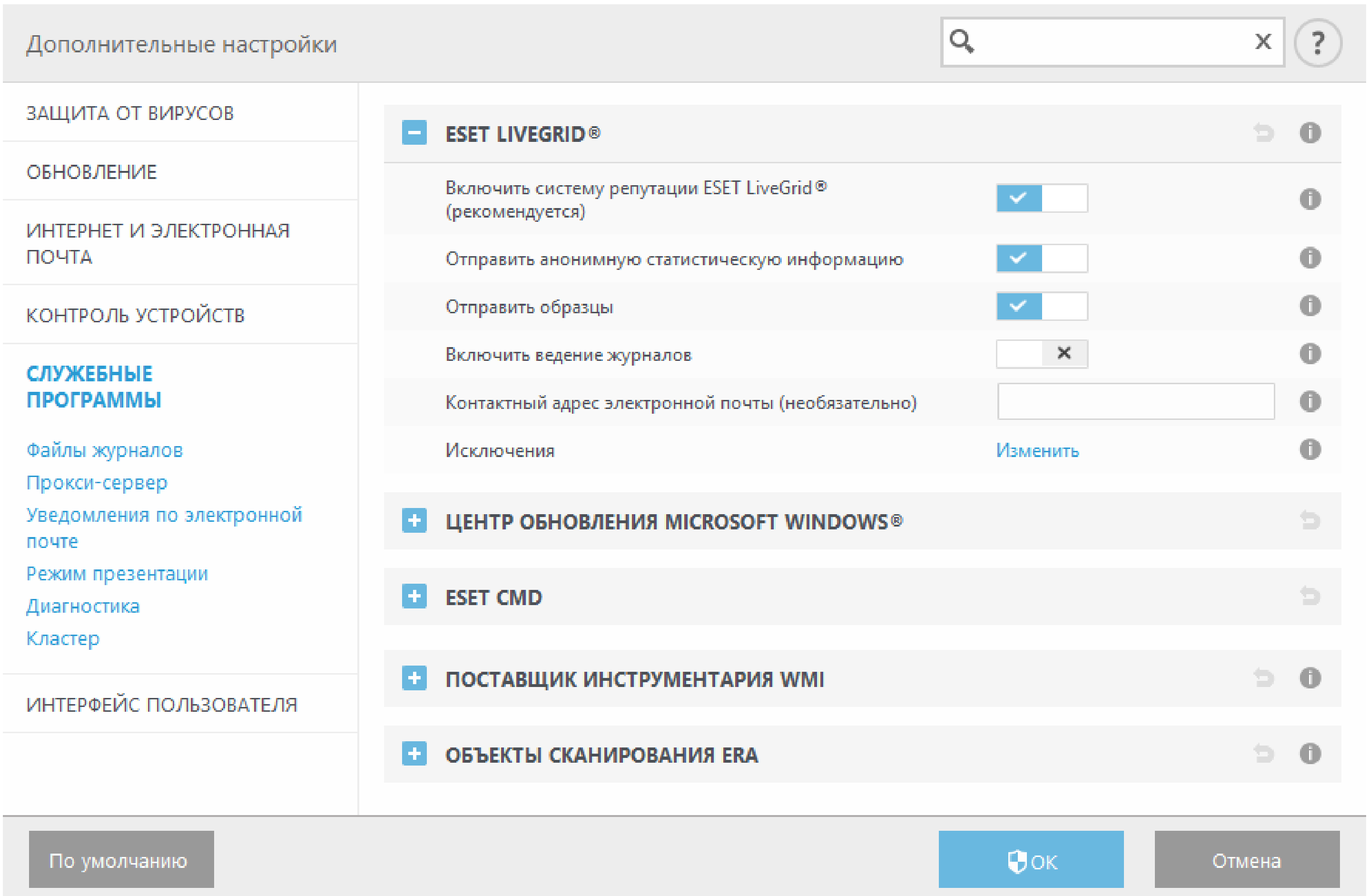
Сеть ESET LiveGrid — это современная система раннего обнаружения угроз, состоящая из нескольких облачных технологий. Она обнаруживает возникающие угрозы, пользуясь принципом репутации, и оптимизирует процесс сканирования благодаря использованию «белого» списка. За счет потоковой передачи информации об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

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

ESET LiveGrid собирает о компьютерах пользователей информацию, которая связана с новыми обнаруженными угрозами. Это может быть образец 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 File Security отправляет подозрительные файлы в вирусную лабораторию ESET для тщательного анализа. Всегда исключаются файлы с определенными расширениями, такими как *.doc* и *.xls*. Добавить можно также другие расширения, если вы или ваша организация предпочли бы не отправлять некоторые файлы.

Система репутации ESET LiveGrid использует «белый» и «черный» списки, которые хранятся в облаке. Чтобы открыть настройки ESET LiveGrid, нажмите клавишу F5. В окне **Дополнительные настройки** последовательно щелкните **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 (включая информацию о системе).

Отправить образцы — компании ESET на анализ отправляются подозрительные образцы, похожие на угрозы, и/или образцы с необычными характеристиками или поведением.

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

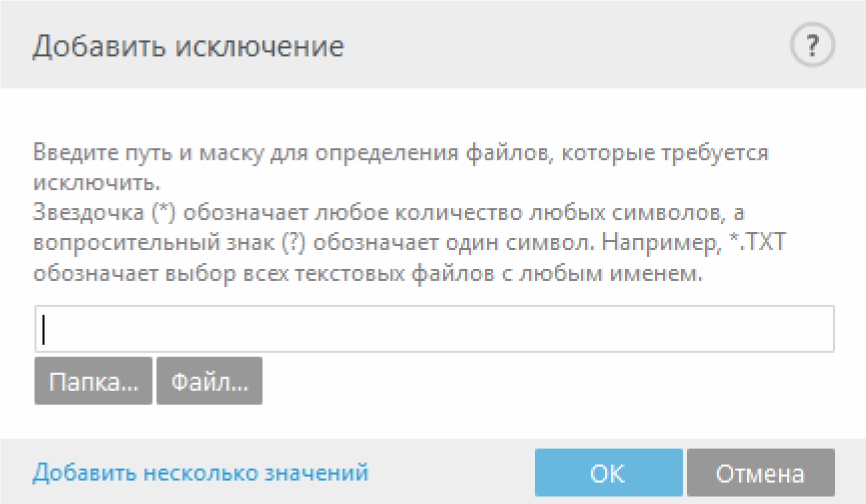
Контактный адрес электронной почты (необязательно) — вместе с подозрительными файлами можно отправить контактный адрес электронной почты, чтобы специалисты ESET могли обратиться к вам, если для анализа потребуется дополнительная информация. Имейте в виду, что компания ESET не отправляет ответы пользователям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

Исключения: 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, например 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 список исключенных файлов можно дополнять.

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.

8.5.1.1 Фильтр исключений

С помощью параметра **Изменить** рядом с элементом «Исключения» в ESET LiveGrid можно настроить способ отправки сведений об угрозах в антивирусную лабораторию ESET для анализа.



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

8.5.2 Центр обновления Windows

Обновления Windows содержат важные исправления потенциально опасных уязвимостей и повышают общий уровень безопасности компьютера. По этой причине обновления Microsoft Windows следует устанавливать сразу после их появления. Программное обеспечение ESET File Security уведомляет пользователя об отсутствующих обновлениях в соответствии с выбранным уровнем. Доступны следующие уровни.

- **Без обновлений**: запросы на загрузку обновлений системы не отображаются.
- **Необязательные обновления**: отображаются запросы на загрузку обновлений, имеющих низкий и более высокие уровни приоритета.
- **Рекомендуемые обновления**: отображаются запросы на загрузку обновлений, имеющих обычный и более высокие уровни приоритета.
- **Важные обновления**: отображаются запросы на загрузку обновлений, помеченных как важные и имеющих более высокий уровень приоритета.
- **Критические обновления**: пользователю предлагается загрузить только критические обновления.

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

8.5.3 ESET CMD

Это функция, позволяющая применять расширенные команды ECMD. Она позволяет экспортировать и импортировать параметры с помощью командной строки (ecmd.exe). До недавнего времени экспортировать параметры можно было только через графический интерфейс пользователя. Конфигурацию ESET File Security можно экспортировать в файл с расширением *XML*.

Если включена функция ESET CMD, доступны два метода авторизации:

- **Нет** — без авторизации. Этот метод не рекомендуется, так как он разрешает импортировать любую неподписанную конфигурацию, что представляет собой потенциальный риск.

- **Пароль для расширенной настройки** — пароль требуется для импорта конфигурации из файла с расширением *XML*. Этот файл должен быть подписан (сведения о подписании файла конфигурации с расширением *XML* представлены далее). Новую конфигурацию можно импортировать только после того, как будет указан пароль, заданный в разделе Настройка доступа. Если настройка доступа не включена, пароль не совпадает или файл конфигурации в формате *XML* не подписан, импорт конфигурации выполнен не будет.

После включения ESET CMD можно использовать командную строку для импорта и экспорта конфигураций программы ESET File Security. Это можно сделать вручную или создать сценарий с целью автоматизации.

ВАЖНО!
Для использования расширенных команд ECMD необходимо запустить их с правами администратора или открыть командную строку Windows (cmd) командой **Запуск от имени администратора**. В противном случае появляется сообщение **Error executing command.**. Кроме того, при экспорте конфигурации папка назначения должна существовать. Команда экспорта работает даже при отключенном параметре ESET CMD.

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

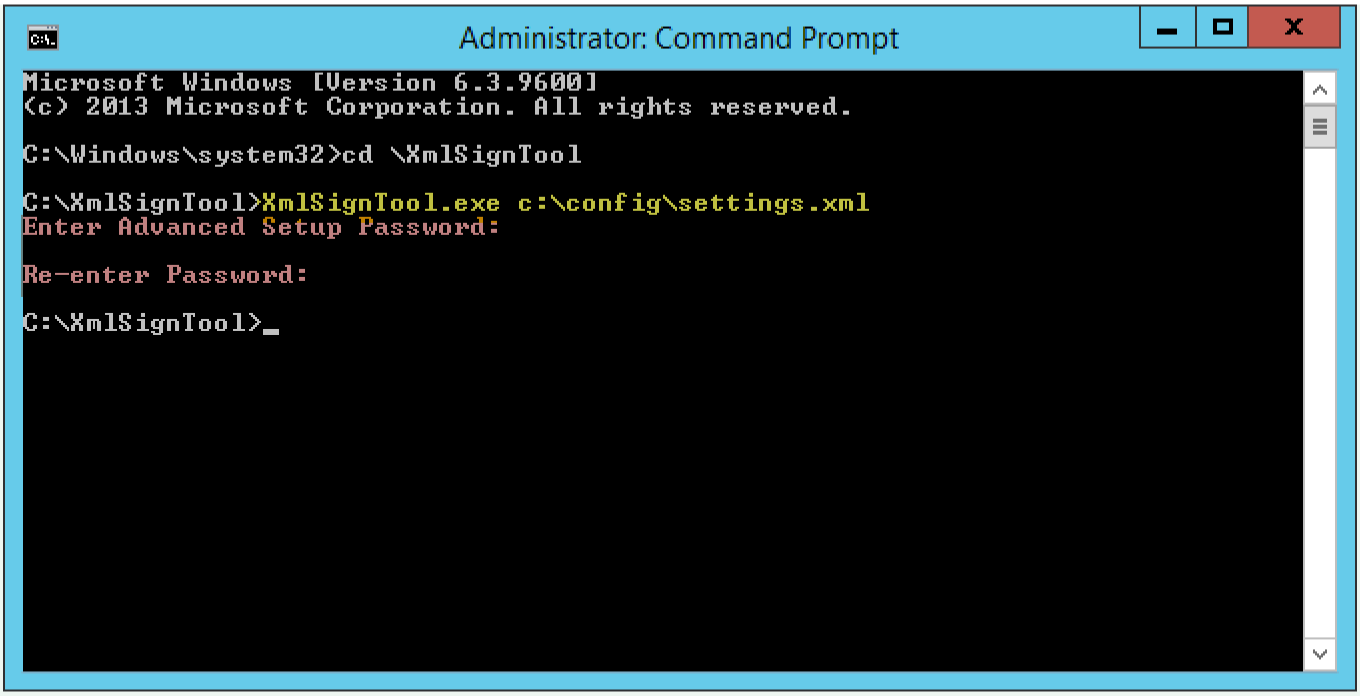
Команда импорта настроек:
`ecmd /setcfg c:\config\settings.xml`

ПРИМЕЧАНИЕ.
Расширенные команды ECMD можно выполнять только локально. Запуск клиентской задачи **Выполнение команды** с помощью ERA является невозможным.

Для подписания файла конфигурации в формате *XML* выполните следующие действия.

1. Загрузите средство **XmlSignTool** со страницы загрузки служебных программ и утилит ESET и извлеките его.
2. Откройте командную строку Windows (cmd) с помощью команды **Запуск от имени администратора**.
3. Перейдите в расположение файла `XmlSignTool.exe`
4. Выполните команду для подписания файла конфигурации в формате *XML*, например: `XmlSignTool <путь_к_файлу_xml>`
5. Введите пароль для дополнительных настроек, а затем введите его еще раз по запросу средства XmlSignTool. Теперь файл конфигурации в формате *XML* подписан и может использоваться для импорта в другом экземпляре ESET File Security с функцией ESET CMD с помощью метода парольной авторизации.

ПРИМЕР
Команда подписания экспортированного файла конфигурации:
`XmlSignTool c:\config\settings.xml`



ПРИМЕЧАНИЕ.

Если пароль в разделе [Настройка доступа]() изменится и потребуется импортировать конфигурацию, подписанную ранее с помощью старого пароля, можно подписать файл конфигурации в формате *XML* заново с помощью текущего пароля. Это позволит использовать старый файл конфигурации без необходимости экспортировать его на другой компьютер с работающей программой ESET File Security перед импортом.

8.5.4 Поставщик инструментария WMI

Сведения об инструментарии WMI

Инструментарий управления Windows (WMI) — это реализация корпорацией Майкрософт инициативы «управление предприятием через Интернет». Это отраслевая инициатива, направленная на разработку стандартной технологии, с помощью которой в корпоративной среде можно было бы получать доступ к административной информации.

Дополнительные сведения об инструментарии WMI см. в статье по адресу http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642(v=vs.85).aspx

Поставщик инструментария ESET WMI

Поставщик инструментария ESET WMI нужен для удаленного мониторинга программ ESET, работающих в корпоративной среде, без использования специальных программ или средств ESET. Делая доступными с помощью инструментария WMI базовые сведения о программе, состоянии и статистике, мы значительно расширяем возможности мониторинга программ ESET для администраторов предприятий. Инструментарий WMI позволяет администраторам пользоваться рядом методов доступа (командной строкой, сценариями и сторонними инструментами корпоративного мониторинга), чтобы отслеживать состояние программ ESET.

Текущая версия инструментария предоставляет доступ только для чтения к базовым сведениям о программе, установленных компонентах и состоянии защиты, данным статистики отдельных модулей сканирования, а также к журналам программы.

Поставщик инструментария WMI дает возможность считывать состояния и журналы продукта с помощью стандартных средств и инфраструктуры Windows WMI.

8.5.4.1 Предоставляемые данные

Все классы WMI, связанные с продуктом ESET, расположены в пространстве имен «root\ESET». Ниже приводится более подробное описание классов, которые используются в настоящее время.

Общие:

- ESET_Product
- ESET_Features
- ESET_Statistics

Журналы:

- ESET_ThreatLog
- ESET_EventLog
- ESET_ODFileScanLogs
- ESET_ODFileScanLogRecords
- ESET_ODServerScanLogs
- ESET_ODServerScanLogRecords
- ESET_MailServerLog

Класс ESET_Product

Класс ESET_Product может существовать только в одном экземпляре. Свойства этого класса относятся к основной информации об установленном продукте ESET:

- **ID** — идентификатор типа продукта, например emsl.
- **Name** — название продукта, например «ESET Mail Security».
- **FullName** — полное название продукта, например «ESET Mail Security for IBM Domino».
- **Version** — версия продукта, например 6.5.14003.0.
- **VirusDBVersion** — версия базы данных вирусов, например 14533 (20161201).
- **VirusDBLastUpdate** — отметка о времени последнего обновления вирусной базы данных. В строке содержится отметка о времени в формате даты и времени WMI, например 20161201095245.000000+060.
- **LicenseExpiration** — время окончания срока действия лицензии. В строке содержится отметка о времени в формате даты и времени WMI..
- **KernelRunning** — логическое значение, указывающее, запущена ли служба`ekrn` на компьютере, например «TRUE».
- **StatusCode** — цифра, указывающая на состояние защиты программы: **0** — зеленый (ОК), **1** — желтый (предупреждение), **2** — красный (ошибка).
- **StatusText** — сообщение, объясняющее, почему код состояния (StatusCode) не равняется нулю (это сообщение не отображается, если код состояния равняется нулю).

Класс ESET_Features

Класс ESET_Features имеет несколько экземпляров. Их число зависит от количества компонентов программы. Каждый экземпляр содержит следующие сведения:

- **Name** — имя компонента (список имен приведен ниже).
- **Status** — состояние компонента: 0 — неактивно, 1 — отключено, 2 — включено.

Список строк с компонентами программы, которые сейчас признаются:

- **CLIENT_FILE_AV** — защита файловой системы от вирусов в реальном времени.
- **CLIENT_WEB_AV** — защита клиента от вирусов при доступе в Интернет.
- **CLIENT_DOC_AV** — защита документов клиента от вирусов.
- **CLIENT_NET_FW** — персональный файервол клиента.
- **CLIENT_EMAIL_AV** — защита электронной почты клиента от вирусов.
- **CLIENT_EMAIL_AS** — защита электронной почты клиента от спама.
- **SERVER_FILE_AV** — защита файлов, хранящихся в защищенном серверном продукте, от вирусов в режиме реального времени, например файлов в базе данных контента SharePoint при использовании программы ESET File Security.

- **SERVER_EMAIL_AV** — защита от вирусов сообщений электронной почты в защищенном серверном продукте, например сообщений в MS Exchange или IBM Domino.
- **SERVER_EMAIL_AS** — защита от спама сообщений электронной почты в защищенном серверном продукте, например сообщений в MS Exchange или IBM Domino.
- **SERVER_GATEWAY_AV** — защита защищенных сетевых протоколов в шлюзе от вирусов.
- **SERVER_GATEWAY_AS** — защита защищенных сетевых протоколов в шлюзе от спама.

Класс ESET_Statistics

Класс ESET_Statistics имеет несколько экземпляров. Их число зависит от количества модулей сканирования в программе. Каждый экземпляр содержит следующие сведения:

- Scanner — код строки, имеющий отношение к определенному модулю сканирования, например «CLIENT_FILE».
- Total — общее количество просканированных файлов.
- Infected — количество найденных зараженных файлов.
- Cleaned — количество очищенных файлов.
- Timestamp — отметка о времени последнего изменения этой статистики. В формате даты и времени WMI эта отметка выглядит так: 20130118115511.000000+060.
- ResetTime — отметка о времени последнего сброса счетчика статистики. В формате даты и времени WMI эта отметка выглядит так: 20130118115511.000000+060.
- Список строк с модулями сканирования, которые сейчас признаются:
- CLIENT_FILE
- CLIENT_EMAIL
- CLIENT_WEB
- SERVER_FILE
- SERVER_EMAIL
- SERVER_WEB

Класс ESET_ThreatLog

Класс ESET_ThreatLog имеет несколько экземпляров, каждый из которых представляет запись из журнала «Обнаруженные угрозы». Каждый экземпляр содержит следующие сведения:

- **ID** — уникальный идентификатор записи журнала.
- **Timestamp** — отметка о времени создания записи журнала (в формате даты и времени WMI).
- **LogLevel** — серьезность записи журнала, выраженная цифрой в диапазоне 0–8. Эти цифры соответствуют следующим уровням: отладка, информационная сноска, информация, важная информация, предупреждение, ошибка, предупреждение о безопасности, критическая ошибка, критическое предупреждение о безопасности.
- **Scanner** — имя модуля сканирования, создавшего данное событие журнала.
- **ObjectType** — тип объекта, сгенерировавшего это событие журнала.
- **ObjectName** — имя объекта, сгенерировавшего это событие журнала.
- **Threat** — имя угрозы, найденной в объекте, который описывают свойства ObjectName и ObjectType.
- **Action** — действие после идентификации угрозы.
- **User** — учетная запись пользователя, обусловившая создание события журнала.
- **Information** — дополнительное описание события.

ESET_EventLog

Класс ESET_EventLog имеет несколько экземпляров, каждый из которых представляет запись из журнала «События». Каждый экземпляр содержит следующие сведения:

- **ID** — уникальный идентификатор записи журнала.
- **Timestamp** — отметка о времени создания записи журнала (в формате даты и времени WMI).
- **LogLevel** — серьезность записи журнала, выраженная цифрой в диапазоне 0–8. Эти цифры соответствуют следующим уровням: отладка, информационная сноска, информация, важная информация, предупреждение, ошибка, предупреждение о безопасности, критическая ошибка, критическое предупреждение о безопасности.
- **Module** — имя модуля сканирования, создавшего данное событие журнала.

- **Event**: описание события.
- **User** — учетная запись пользователя, обусловившая создание события журнала.

ESET_ODFileScanLogs

Класс ESET_ODFileScanLogs имеет несколько экземпляров, каждый из которых представляет запись о сканировании файлов по требованию. Этот список идентичен показываемому в графическом интерфейсе списку журналов «Сканирование ПК по требованию». Каждый экземпляр содержит следующие сведения:

- **ID** — уникальный идентификатор журнала сканирования по требованию.
- **Timestamp** — отметка о времени создания журнала (в формате даты и времени WMI).
- **Targets** — просканированные папки и объекты.
- **TotalScanned** — общее количество просканированных объектов.
- **Infected** — количество найденных зараженных объектов.
- **Cleaned** — количество очищенных объектов.
- **Status** — состояние процесса сканирования.

ESET_ODFileScanLogRecords

Класс ESET_ODFileScanLogRecords имеет несколько экземпляров, каждый из которых представляет запись в одном из журналов сканирования, представленных экземплярами класса ESET_ODFileScanLogs. Экземпляры этого класса содержат записи журнала о всех сканированиях по требованию или журналах. Если требуется экземпляр только какого-то одного журнала сканирования, необходимо выполнить фильтрацию по свойству LogID. Каждый экземпляр класса содержит следующие сведения:

- **LogID** — идентификатор журнала сканирования, содержащего данную запись (идентификатор одного из экземпляров класса ESET_ODFileScanLogs).
- **ID** — уникальный идентификатор записи журнала сканирования.
- **Timestamp** — отметка о времени создания записи журнала (в формате даты и времени WMI).
- **LogLevel** — серьезность записи журнала, выраженная цифрой в диапазоне 0–8. Эти цифры соответствуют следующим уровням: отладка, информационная сноска, информация, важная информация, предупреждение, ошибка, предупреждение о безопасности, критическая ошибка, критическое предупреждение о безопасности.
- **Log** — сообщение журнала.

ESET_ODServerScanLogs

Класс ESET_ODServerScanLogs имеет несколько экземпляров, каждый из которых представляет запись о сканировании сервера по требованию. Каждый экземпляр содержит следующие сведения:

- **ID** — уникальный идентификатор журнала сканирования по требованию.
- **Timestamp** — отметка о времени создания журнала (в формате даты и времени WMI).
- **Targets** — просканированные папки и объекты.
- **TotalScanned** — общее количество просканированных объектов.
- **Infected** — количество найденных зараженных объектов.
- **Cleaned** — количество очищенных объектов.
- **RuleHits** — общее количество совпадений по правилам.
- **Status** — состояние процесса сканирования.

ESET_ODServerScanLogRecords

Класс ESET_ODServerScanLogRecords имеет несколько экземпляров, каждый из которых представляет запись в одном из журналов сканирования, представленных экземплярами класса ESET_ODServerScanLogs. Экземпляры этого класса содержат записи журнала о всех сканированиях по требованию или журналах. Если требуется экземпляр только какого-то одного журнала сканирования, необходимо выполнить фильтрацию по свойству LogID. Каждый экземпляр класса содержит следующие сведения:

- **LogID** — идентификатор журнала сканирования, содержащего данную запись (идентификатор одного из экземпляров класса ESET_ ODServerScanLogs).
- **ID** — уникальный идентификатор записи журнала сканирования.
- **Timestamp** — отметка о времени создания записи журнала (в формате даты и времени WMI).

- **LogLevel** — серьезность записи журнала, выраженная цифрой в диапазоне 0–8. Эти цифры соответствуют следующим уровням: отладка, информационная сноска, информация, важная информация, предупреждение, ошибка, предупреждение о безопасности, критическая ошибка, критическое предупреждение о безопасности.
- **Log** — сообщение журнала.

ESET_GreylistLog

Класс ESET_GreylistLog имеет несколько экземпляров, каждый из которых представляет запись из журнала «Серый список». Каждый экземпляр содержит следующие сведения:

- **ID** — уникальный идентификатор записи журнала.
- **Timestamp** — отметка о времени создания записи журнала (в формате даты и времени WMI).
- **LogLevel** — серьезность записи журнала, выраженная цифрой в диапазоне 0–8. Эти цифры соответствуют следующим уровням: отладка, информационная сноска, информация, важная информация, предупреждение, ошибка, предупреждение о безопасности, критическая ошибка, критическое предупреждение о безопасности.
- **HELODomain** — имя домена HELO.
- **IP** — исходный IP-адрес.
- **Sender** — отправитель сообщений электронной почты.
- **Recipient** — получатель сообщений электронной почты.
- **Action** — выполненное действие.
- **TimeToAccept** — количество минут, по прошествии которых сообщение электронной почты будет принято.

8.5.4.2 Получение доступа к предоставляемым данным

Далее описывается несколько способов получения доступа к данным ESET WMI из командной строки Windows и PowerShell, которые подходят для любой установленной версии ОС Windows. Кроме того, существует множество других способов получения доступа к данным из других средств и языков сценария.

Командная строка без сценариев

Инструмент `wmic` командной строки может использоваться для получения доступа к различным предварительно заданным или любым настраиваемым классам инструментария WMI.

Чтобы отобразить полную информацию о продукте на локальном компьютере:

```
wmic /namespace:\\root\ESET Path ESET_Product
```

Чтобы отобразить номер версии продукта только для продукта на локальном компьютере:

```
wmic /namespace:\\root\ESET Path ESET_Product Get Version
```

Чтобы отобразить полную информацию о продукте на удаленном компьютере с IP-адресом 10.1.118.180:

```
wmic /namespace:\\root\ESET /node:10.1.118.180 /user:Administrator Path ESET_Product
```

PowerShell

Получить и отобразить полную информацию о продукте на локальном компьютере:

```
Get-WmiObject ESET_Product -namespace 'root\ESET'
```

Получить и отобразить полную информацию о продукте на удаленном компьютере с IP-адресом 10.1.118.180:

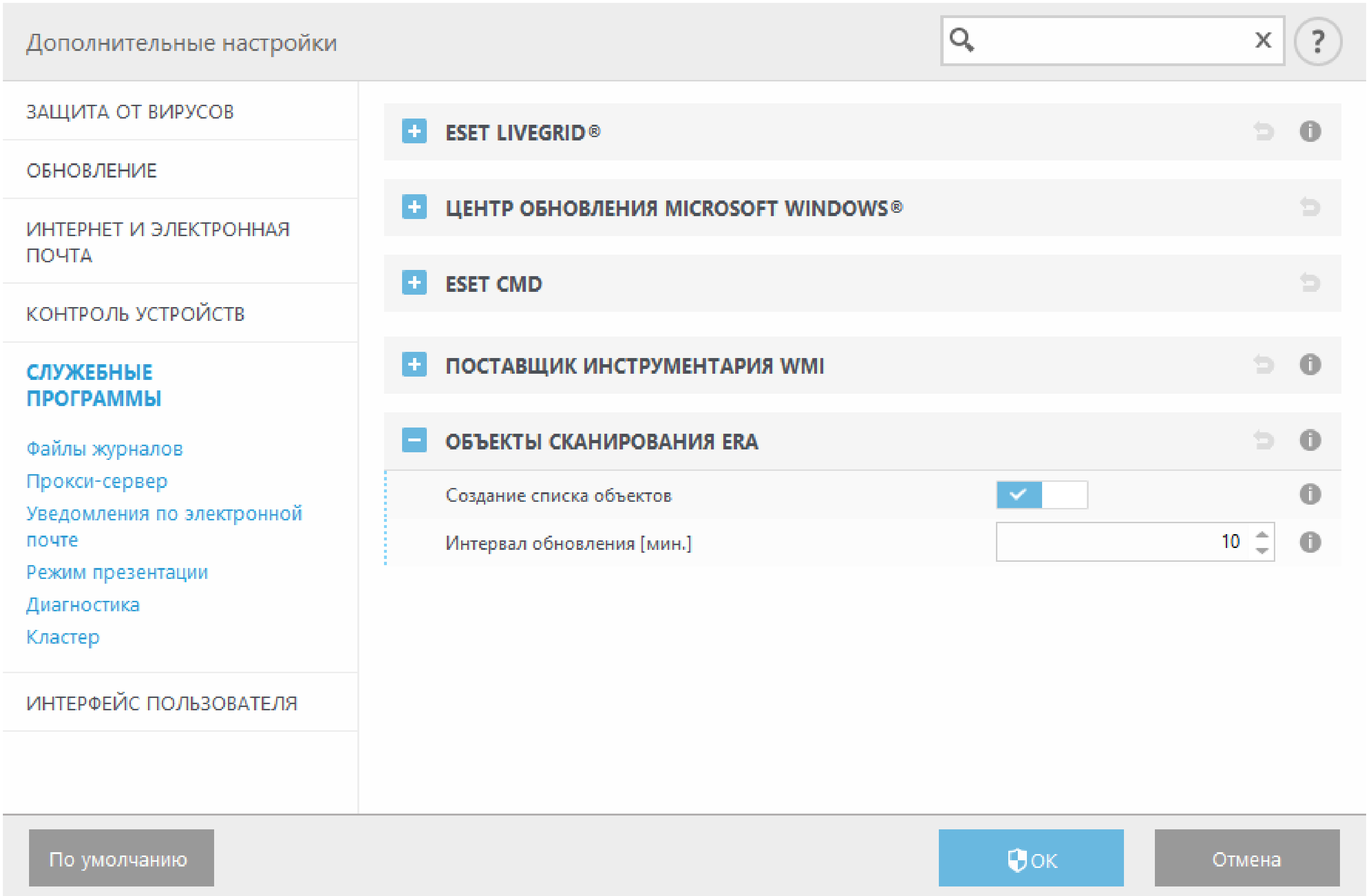
```
$cred = Get-Credential            # запрашивает учетные данные пользователя и сохраняет их в виде
переменной
Get-WmiObject ESET_Product -namespace 'root\ESET' -computername '10.1.118.180' -cred $cred
```

8.5.5 Объекты сканирования ERA

Эта функция позволяет решению ESET Remote Administrator использовать объект сканирования для сканирования Hyper-V при выполнении клиентской задачи **Сканирование сервера** на сервере, на котором установлена программа ESET File Security. Настройка объектов сканирования в ERA доступна, только если установлен агент ERA и присутствует Hyper-V, в ином случае эта настройка будет неактивной.

При включении функции **Создание списка объектов** ESET File Security создает список доступных объектов сканирования. Этот список создается время от времени в соответствии с заданным **интервалом обновления**.

ПРИМЕЧАНИЕ.
При первом включении функции **Создание списка объектов** на создание списка службе ERA требуется около половины указанного **интервала обновления**. Поэтому, если **интервал обновления** составляет 60 минут, службе ERA потребуется около 30 минут, чтобы получить список объектов сканирования. Если нужно, чтобы служба ERA получила список быстрее, установите меньшее значение для интервала обновления. Потом его всегда можно увеличить.



При запуске клиентской задачи **Сканирование сервера** решение ERA создает список и предлагает пользователю выбрать объекты для сканирования Hyper-V на заданном сервере.

8.5.6 Файлы журналов

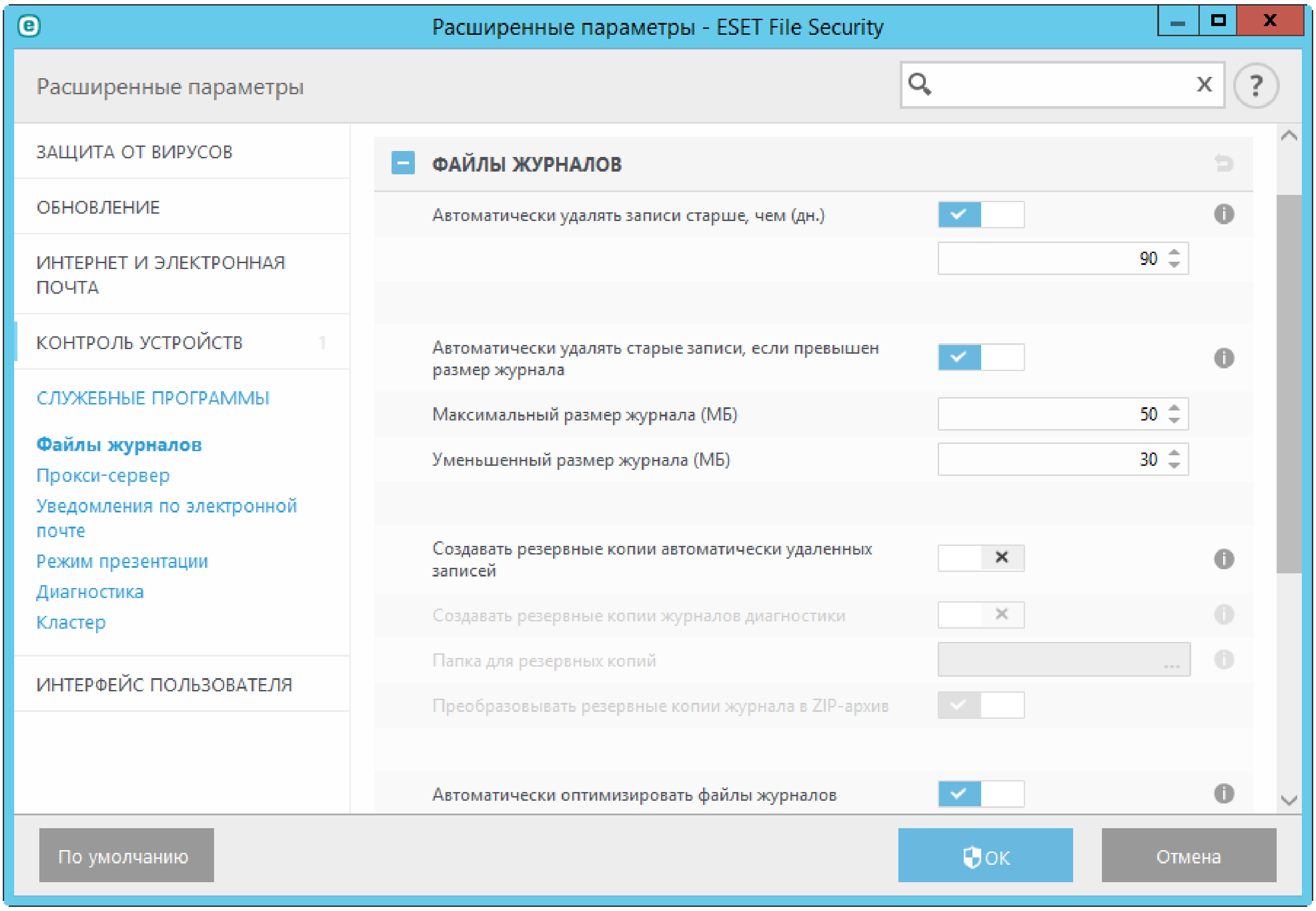
С помощью этого раздела можно изменять конфигурацию ведения журналов программы ESET File Security. Записи вносятся в журнал **События** (`C:\ProgramData\ESET\ESET File Security\Logs\warnlog.dat`) и доступны для просмотра в средстве просмотра файлов журнала. При помощи переключателей можно включать и отключать определенные функции:

Ведение журнала диагностики

Ведение журнала диагностики кластера — ведение журнала кластера будет выполняться в рамках ведения общего журнала диагностики.

ПРИМЕЧАНИЕ.
Чтобы начать запись журналов, включите на уровне программы функцию **Ведение журнала диагностики**. Сделать это можно в главном меню в разделе **Настройка** > Служебные программы. Когда ведение журнала будет включено, ESET File Security начнет создавать подробные журналы с учетом функций, включенных в этом разделе.

Файлы журналов — определение способа управления журналами. Это важно в основном для предотвращения чрезмерного использования диска. Настройки по умолчанию разрешают автоматическое удаление старых журналов для экономии дискового пространства.



Записи в журнале, созданные раньше, чем указано в поле **Автоматически удалять записи старше, чем (дн.)**, автоматически будут удаляться.
Автоматически удалять старые записи, если превышен размер журнала: если размер журнала превышает **максимальный размер журнала (МБ)**, удаление старых записей будет происходить, пока не будет достигнут **уменьшенный размер журнала [МБ]**.

Создавать резервные копии автоматически удаленных записей: резервные копии автоматически удаленных записей журнала и файлов будут создаваться в указанном каталоге и при необходимости сжиматься.

Создавать резервные копии журналов диагностики: будут создаваться резервные копии автоматически удаленных журналов диагностики. Если этот параметр не включен, резервные копии записей журналов диагностики создаваться не будут.
Папка для резервных копий: папка для хранения резервных копий журнала. Вы можете разрешить **сжатие резервных копий журналов в ZIP-архивы**.

Автоматически оптимизировать файлы журналов: если этот флажок установлен, файлы журналов автоматически дефрагментируются, когда процент фрагментации превышает значение, указанное в поле **Если количество неиспользуемых записей превышает (%)**.

Чтобы начать дефрагментацию файлов журналов, щелкните элемент **Оптимизировать**. Все пустые записи журналов удаляются для улучшения производительности и скорости обработки журналов. Такое улучшение особенно заметно, если в журналах содержится большое количество записей.

Чтобы разрешить хранение журналов в формате, отличном от формата файлы журналов, щелкните элемент **Включить текстовый протокол**.

- **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 *virlog.txt* сохраняется раздел **Обнаруженные угрозы** файлов журналов, если для хранения журналов используется текстовый формат файлов).

- **Тип** — если выбрать формат файлов **Текст**, журналы будут сохраняться в текстовый файл, данные в котором будут разделены табуляцией. То же касается формата **CSV**. Если выбрать вариант **Событие**, файлы журнала будут храниться не в файле, а в журнале событий Windows (его можно просмотреть с помощью компонента «Просмотр событий» на панели управления).

- Команда **Удалить** удаляет все сохраненные файлы, выбранные в раскрывающемся меню **Тип**.

ПРИМЕЧАНИЕ.
Для более быстрого решения проблем специалисты ESET иногда могут запрашивать у пользователей журналы с их компьютеров. Сборщик журналов ESET облегчает сбор необходимой информации. Дополнительные сведения о сборщике журналов ESET см. в нашей статье базы знаний.

8.5.6.1 Фильтрация журнала

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

Введите ключевое слово для поиска в поле **Найти текст**. С помощью раскрывающегося меню **Искать в столбцах** уточните поисковый запрос.

Типы записей — выберите один или несколько типов записей журнала в раскрывающемся меню.

- **Диагностика** — в журнал вносится информация, необходимая для тщательной настройки программы, и все перечисленные выше записи.
- **Информация** — в журнал вносятся информационные сообщения, в том числе сообщения об успешном выполнении обновления, а также все перечисленные выше записи.
- **Предупреждения** — в журнал вносится информация обо всех критических ошибках и предупреждениях.
- **Ошибки** — в журнал вносится информация об ошибках загрузки файлов и критических ошибках.
- **Критические ошибки** — в журнал вносятся только критические ошибки (ошибки запуска защиты от вирусов).

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

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

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

8.5.6.2 Найти в журнале

В дополнение к фильтрации журнала можно использовать в файлах журналов функцию поиска. Но использовать ее можно и независимо от фильтрации журнала. Эта функция полезна, когда в журналах нужно найти определенные записи. Как и фильтрация журнала, данная функция поиска помогает найти нужную информацию, особенно если количество записей слишком велико.

Во время поиска в журналах можно **найти текст**, введя ту или иную строку, воспользоваться раскрывающимся меню **Искать в столбцах**, чтобы фильтровать по столбцам, выбрать **типы записей** и задать **период времени**, чтобы искать только соответствующие ему записи. Если указать определенные параметры поиска, только отвечающие таким условиям записи отображаются в окне «Файлы журналов».

Найти текст — введите строку (слово целиком или частично). Будут найдены только записи, в которых содержится эта строка. Остальные записи будут опущены.

Искать в столбцах — выберите, какие столбцы будут учитываться при поиске. Для использования в поиске можно отметить один столбец или сразу несколько. По умолчанию отмечаются все столбцы:

- **Время**
- **Просканированная папка**
- **Событие**
- **Пользователь**

Типы записей — выберите один или несколько типов записей журнала в раскрывающемся меню.

- **Диагностика** — в журнал вносится информация, необходимая для тщательной настройки программы, и все перечисленные выше записи.
- **Информация** — в журнал вносятся информационные сообщения, в том числе сообщения об успешном выполнении обновления, а также все перечисленные выше записи.
- **Предупреждения** — в журнал вносится информация обо всех критических ошибках и предупреждениях.
- **Ошибки** — в журнал вносится информация об ошибках загрузки файлов и критических ошибках.
- **Критические ошибки** — в журнал вносятся только критические ошибки (ошибки запуска защиты от вирусов).

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

- **Не указано** (по умолчанию) — поиск по периоду времени не выполняется, поиск ведется в журнале целиком.
- **Последний день**
- **Последняя неделя**
- **Последний месяц**
- **Период времени** — вы можете указать период времени (дата и время), чтобы искать только соответствующие ему записи.

Только слова целиком: будут найдены только записи, соответствующие строке, введенной в текстовом поле **Что**, как целому слову.

С учетом регистра: будут найдены только записи, соответствующие строке, введенной в текстовом поле **Что**, с учетом регистра.

Искать вверх — поиск выполняется с текущего места вверх.

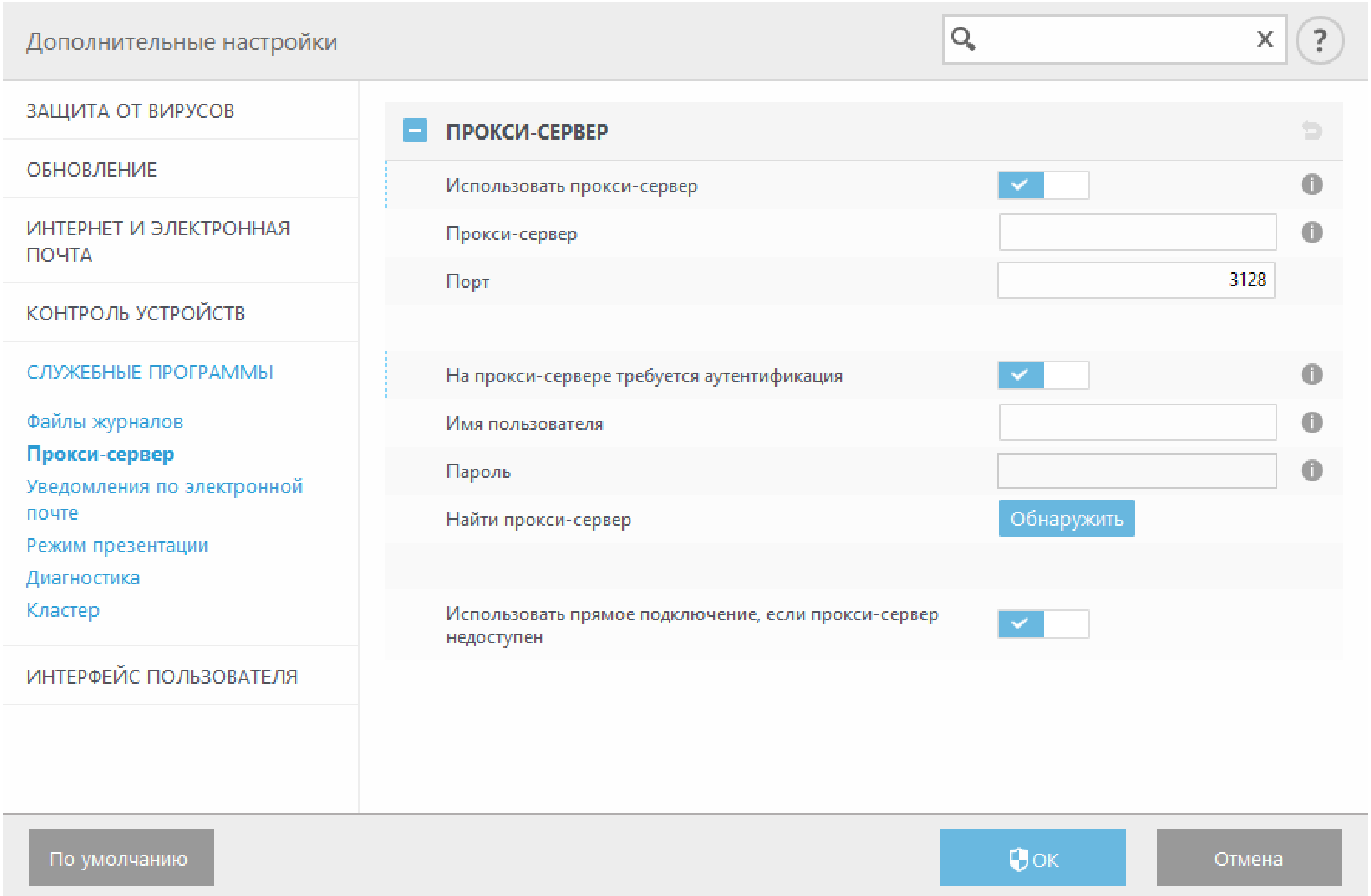
После конфигурирования параметров поиска нажмите кнопку **Найти**, чтобы начать поиск. Поиск прекращается, когда находится первая соответствующая его критериям запись. Чтобы отобразились дополнительные записи, нажмите кнопку **Найти** еще раз. Поиск в файлах журналов ведется сверху вниз, начиная с текущего положения (выделенной записи).

8.5.7 Прокси-сервер

В больших локальных сетях подключение компьютеров к Интернету может осуществляться через прокси-сервер. В этом случае необходимо задать описанные ниже параметры. Если этого не сделать, программа не сможет обновляться автоматически. В ESET File Security настройку прокси-сервера можно выполнить в двух разных разделах окна **Дополнительные настройки** (F5).

1. **Дополнительные настройки** > **Обновление** > **Профили** > **Прокси-сервер HTTP**: 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.
2. **Дополнительные настройки** > **Служебные программы** > **Прокси-сервер**: настройка прокси-сервера на этом уровне позволяет глобально задать его параметры для программы ESET File Security в целом. Они используются всеми модулями программы, которые подключаются к Интернету.

Для настройки параметров прокси-сервера на этом уровне используйте переключатель **Использовать прокси-сервер**, а затем введите адрес прокси-сервера в поле **Прокси-сервер**, а также укажите номер его **порта** в соответствующем поле.



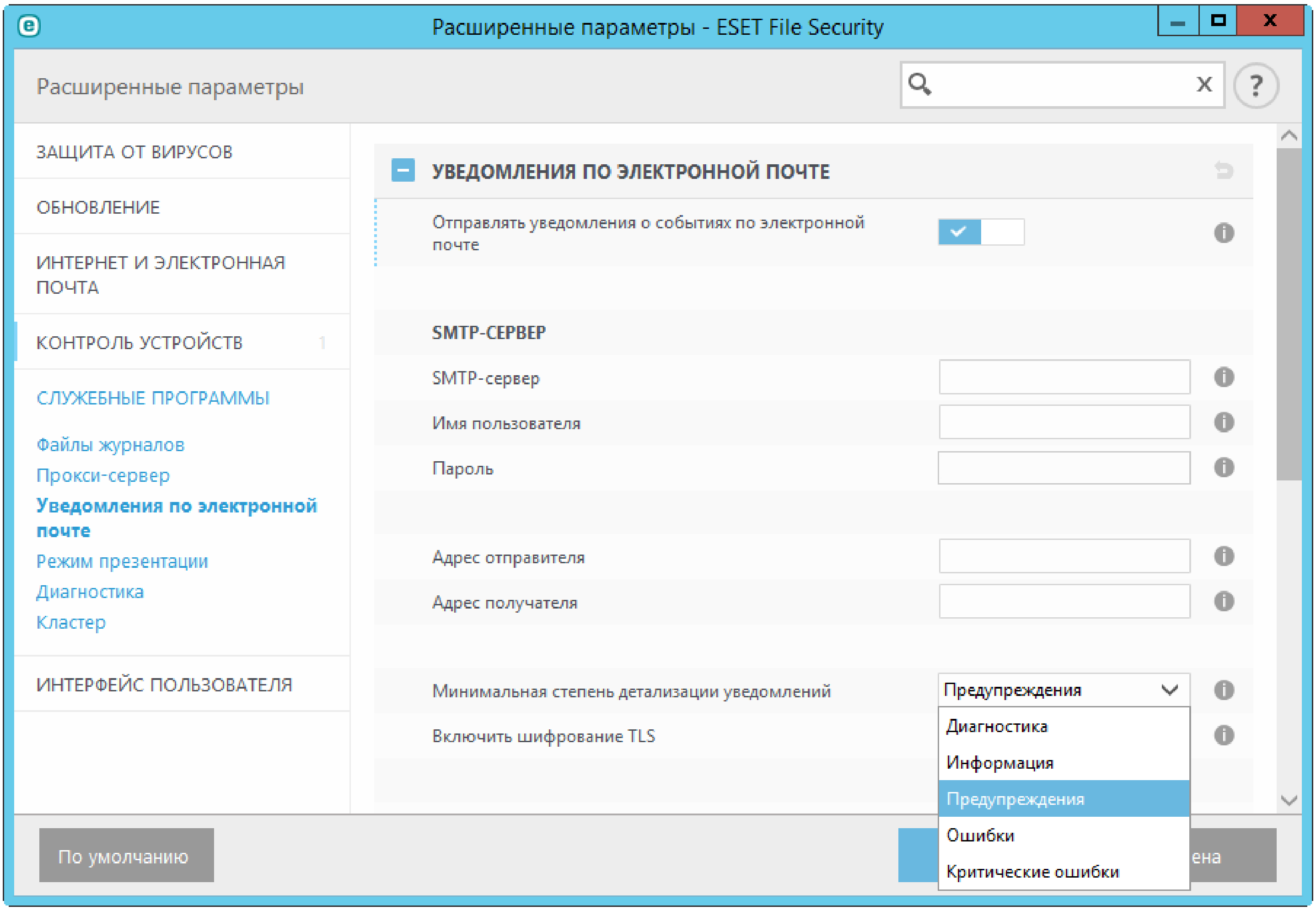
- Если для подключения требуется аутентификация на прокси-сервере, включите переключатель **Прокси-сервер требует аутентификации**, а затем укажите **имя пользователя** и **пароль** в соответствующих полях.
- Нажмите кнопку **Найти**, чтобы автоматически определить параметры прокси-сервера и подставить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

ПРИМЕЧАНИЕ.
Эта функция не позволяет получить данные аутентификации (имя пользователя и пароль), пользователь должен указать их самостоятельно.

- **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.

8.5.8 Уведомления по электронной почте

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



i ПРИМЕЧАНИЕ.
ESET File Security поддерживает SMTP-серверы, использующие шифрование TLS.

- **SMTP-сервер** — SMTP-сервер, используемый для отправки уведомлений.
- **Имя пользователя и пароль** — если требуется аутентификация на SMTP-сервере, для получения доступа к нему заполните эти поля.
- **Адрес отправителя** — введите адрес отправителя, который будет отображаться в заголовке уведомлений, полученных по электронной почте. Это то, что увидит получатель в поле **От**.
- **Адрес получателя** — укажите адрес электронной почты получателя (**Кому**) для доставки уведомлений.
- **Минимальная степень детализации уведомлений**: определяет минимальный уровень детализации уведомлений, которые следует отправлять.
- **Включить шифрование TLS** — разрешить отправку предупреждений об угрозе и уведомлений с использованием протокола TLS.

- **Интервал между отправками новых сообщений электронной почты (мин.)** — время в минутах, по истечении которого по электронной почте будут отправлены новые уведомления. Задайте для этого параметра значение 0, если нужно, чтобы уведомления отправлялись немедленно.

- **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. См. также раздел Изменение формата.
- **Формат предупреждений об угрозах**: предупреждения об угрозе и уведомления имеют предварительно заданный формат по умолчанию. Изменять этот формат не рекомендуется. Однако в некоторых случаях (например, при наличии системы автоматизированной обработки электронной почты) может понадобиться изменить формат сообщений. См. также раздел Изменение формата.

- **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).

8.5.8.1 Формат сообщений

Обмен данными между программой и удаленным пользователем или системным администратором осуществляется посредством электронной почты или сообщений в локальной сети (используется служба сообщений Windows). Формат предупреждений и уведомлений, установленный по умолчанию, будет оптимален в большинстве случаев. В некоторых случаях может понадобиться изменить формат сообщений о событиях.

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 предупреждение.
- **%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 имя **%VirusName%** используются только в предупреждениях об угрозах, а описание **%ErrorDescription%** — только в сообщениях о событиях.

8.5.9 Режим презентации

Режим презентации — 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 можно использовать также во время проведения презентаций, которые нельзя прерывать деятельностью модуля защиты от вирусов. Если этот режим включен, появление всплывающих окон и выполнение запланированных задач блокируется. Защита системы по-прежнему работает в фоновом режиме, но не требует вмешательства со стороны пользователя. Если этот режим включен, появление всплывающих окон и выполнение запланированных задач блокируется. Защита системы по-прежнему работает в фоновом режиме, но не требует вмешательства со стороны пользователя.

- Чтобы включить режим презентации вручную, последовательно выберите элементы **Настройки** > Компьютер и затем щелкните переключатель **Режим презентации**.

- В окне **Дополнительные настройки** (F5) выберите **Служебные программы** > **Режим презентации**, а затем щелкните **Автоматически включать режим презентации при выполнении приложений в полноэкранном режиме**, чтобы при запуске приложений в полноэкранном режиме продукт ESET File Security автоматически переходил в режим презентации. Включая режим презентации, вы подвергаете систему угрозе, поэтому значок Состояние мониторинга на панели задач станет оранжевым и отобразит предупреждение. Данное предупреждение отобразится также в главном окне программы, в котором будет отображена надпись **Режим презентации включен** оранжевого цвета.

Если установить флажок **Автоматически включать режим презентации при выполнении приложений в полноэкранном режиме**, режим презентации будет включаться при запуске любого приложения в полноэкранном режиме и автоматически выключаться после выхода из этого приложения. Включение режима презентации особенно удобно непосредственно при запуске игры, полноэкранного приложения или презентации.
Вы можете выбрать также значение **Автоматически отключать режим презентации через** для указания времени в минутах, по истечении которого режим презентации будет автоматически отключен.

8.5.10 Диагностика

Функция диагностики формирует дампы сбоев приложений, которые имеют отношение к процессам ESET (например, *ekrn*). Если происходит сбой приложения, формируется дамп памяти. Это может помочь разработчикам выполнять отладку и устранять различные проблемы ESET File Security. Откройте раскрывающееся меню рядом с элементом **Тип дампа** и выберите один из трех доступных вариантов.

- Чтобы отключить эту функцию, выберите элемент **Отключить** (установлено по умолчанию).
- **Мини** — регистрируется самый малый объем полезной информации, которая может помочь выявить причину неожиданного сбоя приложения. Этот тип файла дампа может быть удобно использовать, если место на диске ограничено. Однако ограниченный объем включенной в него информации может не позволить при анализе такого файла обнаружить ошибки, которые не были вызваны непосредственно потоком, выполнявшимся в момент возникновения проблемы.
- **Полный** — регистрируется все содержимое системной памяти на момент неожиданного прекращения работы программы. Полный дамп памяти может содержать данные процессов, которые выполнялись в момент создания дампа.

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

Целевой каталог — каталог, в котором будет создаваться дамп при сбое.

Открыть папку диагностики — щелкните элемент **Открыть**, чтобы открыть этот каталог в новом окне *проводника Windows*.

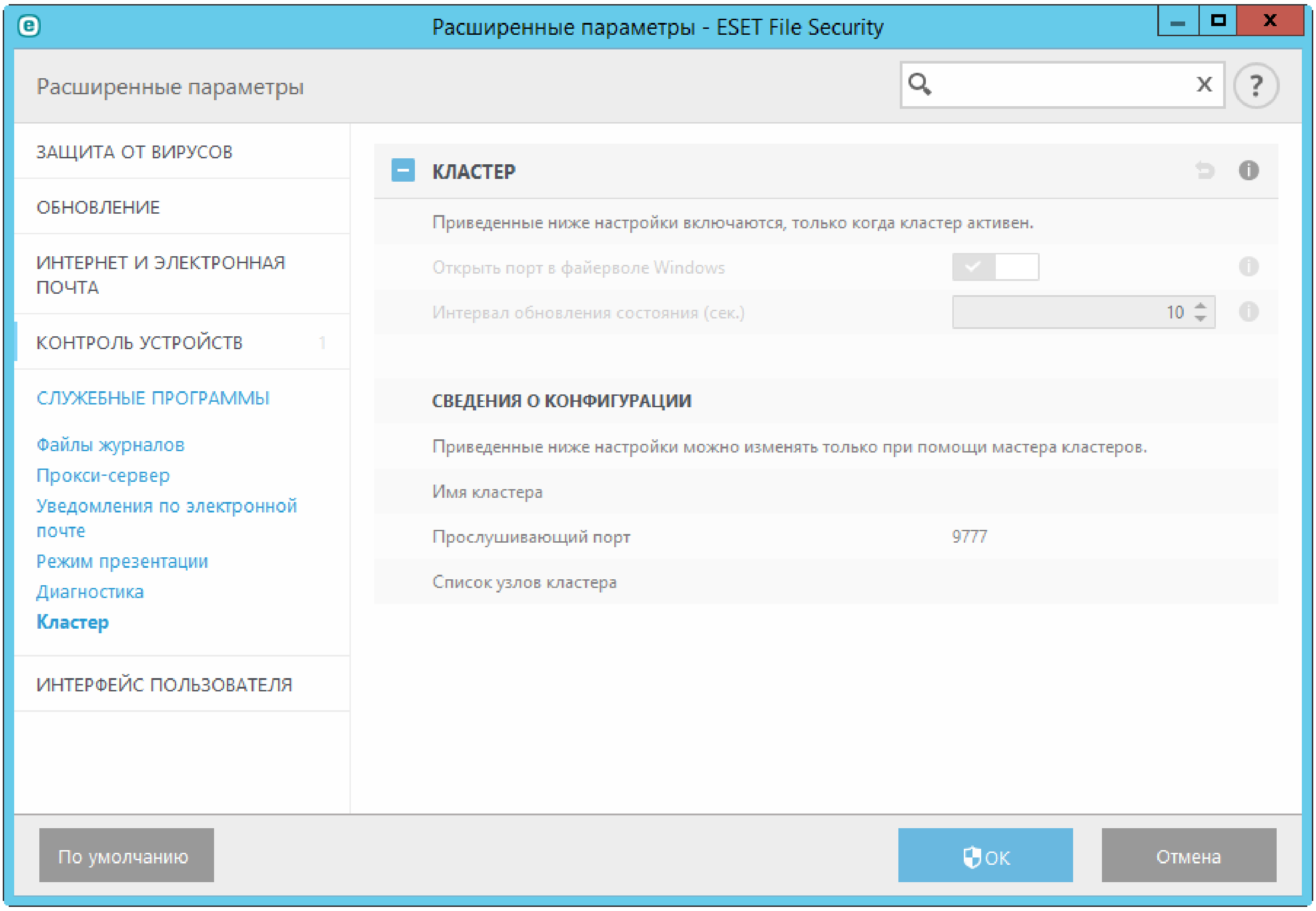
8.5.11 Служба поддержки клиентов

Отправить данные о конфигурации системы — чтобы перед отправкой получать запрос, в раскрывающемся меню выберите элемент **Отправлять всегда** или **Запрашивать подтверждение перед отправкой**.

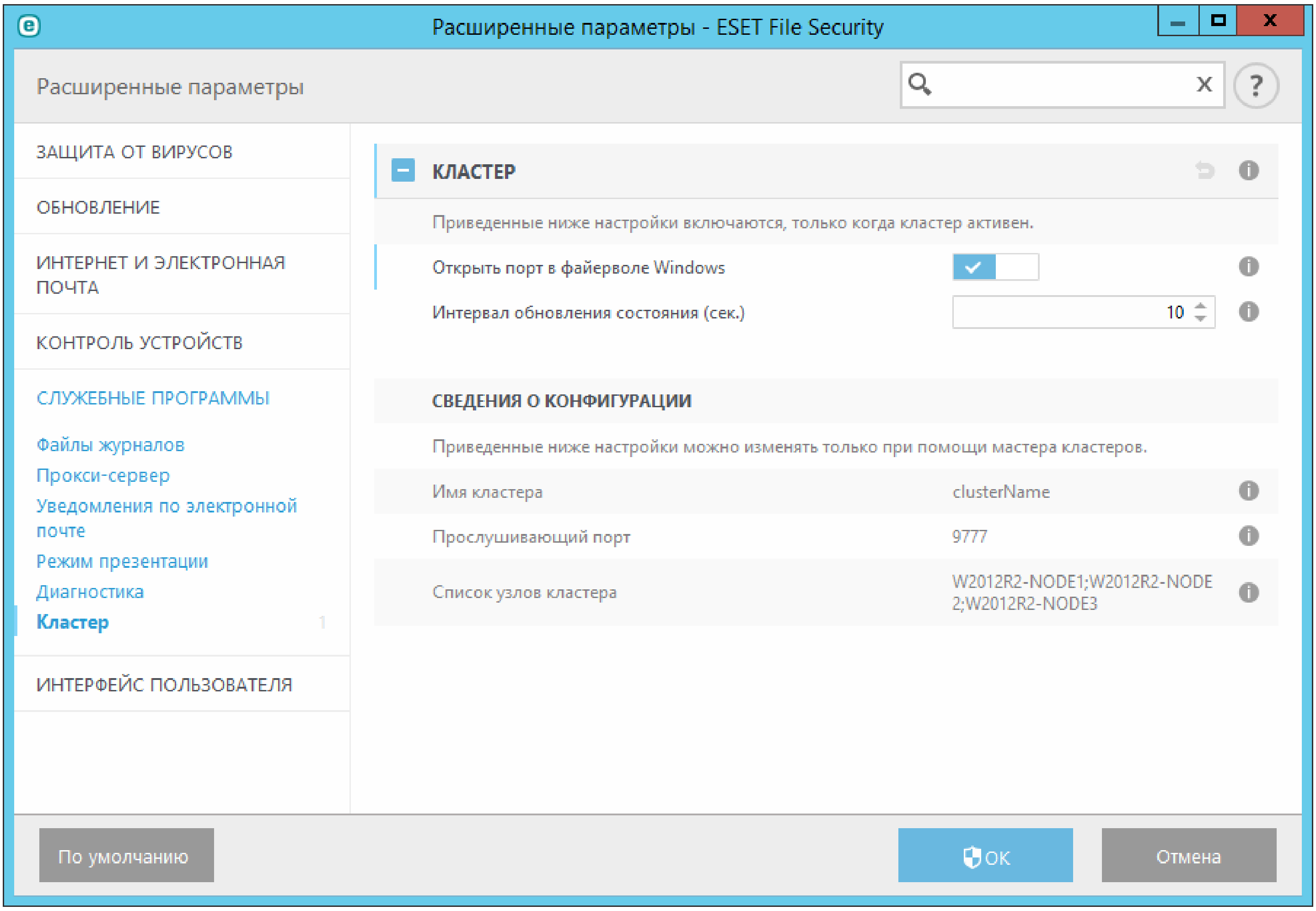
8.5.12 Кластер

Если кластер ESET настроен, параметр **Включить кластер** включается автоматически. Его можно отключить вручную с помощью переключателя в окне **Дополнительные настройки** (это можно сделать, если необходимо изменить конфигурацию, не затрагивая другие узлы в кластере ESET). Данный переключатель только включает или отключает функцию кластера ESET. Чтобы настроить или уничтожить кластер, используйте мастер кластеров или команду «Уничтожить кластер» в разделе **Сервис** > **Кластер** главного окна программы.

Кластер ESET не настроен и выключен.



Сведения и параметры кластера ESET настроены правильно.



Дополнительные сведения о кластере ESET см. здесь.

8.6 Интерфейс пользователя

В разделе **Интерфейс** можно конфигурировать поведение графического интерфейса программы. Здесь можно изменить внешний вид программы и используемые эффекты.

⊟ Элементы интерфейса

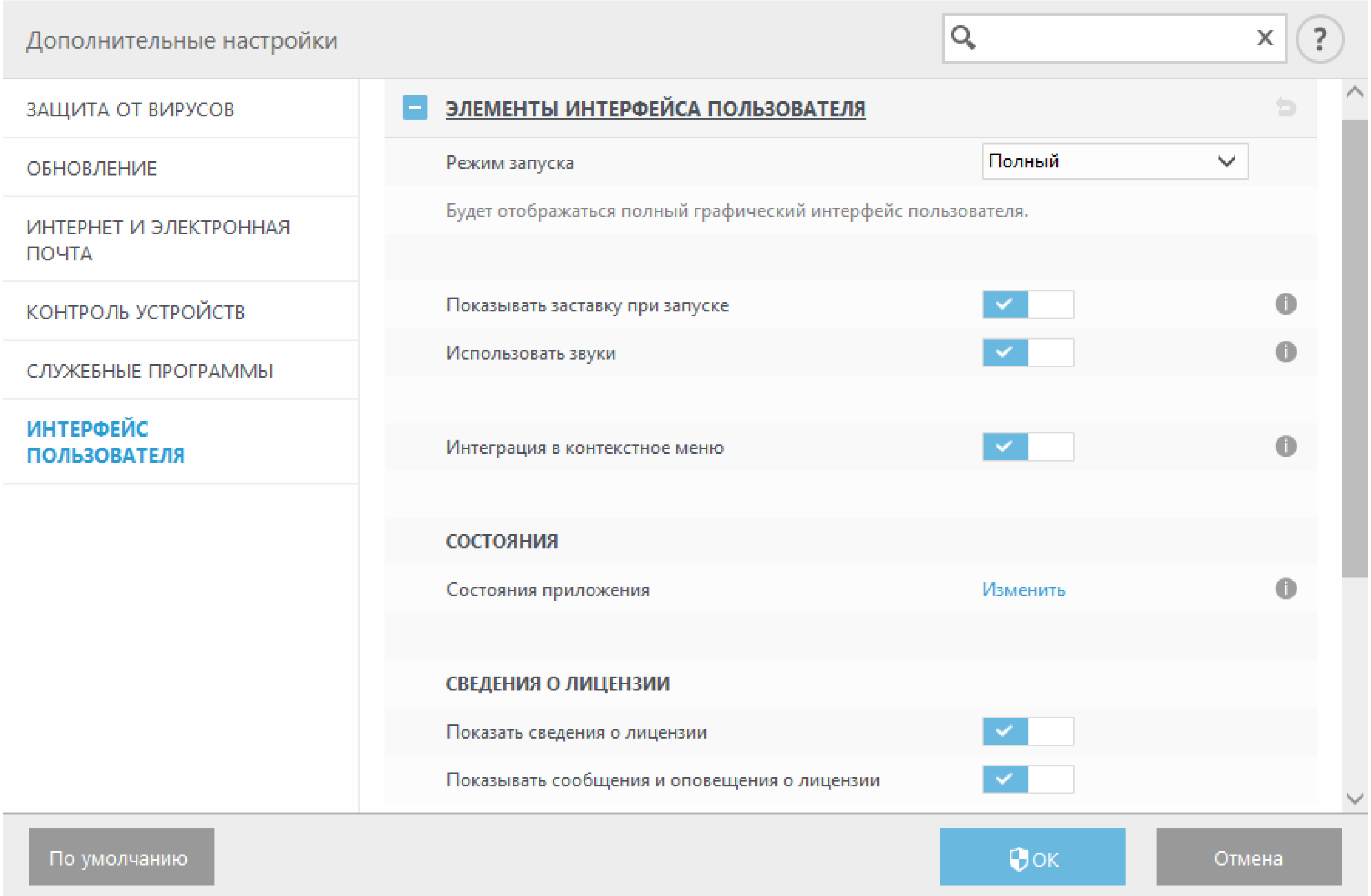
В разделе **Элементы интерфейса** можно настроить рабочую среду. Щелкните раскрывающееся меню **Режим запуска графического интерфейса пользователя** и выберите один из следующих режимов.

- ○ **Полный** — графический интерфейс будет отображаться полностью.
- ○ **Терминал** — уведомления и предупреждения не отображаются. Графический интерфейс пользователя может быть запущен только администратором. Если графические элементы снижают производительность компьютера или вызывают другие проблемы, для интерфейса пользователя необходимо задать значение **Терминал**. Кроме того, на сервере терминалов рекомендуется отключить графический интерфейс пользователя. Дополнительные сведения о программе ESET File Security, установленной на сервере терминалов, см. в разделе Отключение графического интерфейса пользователя на сервере терминалов.

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

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

- **Интеграция в контекстное меню**: можно интегрировать элементы управления ESET File Security в контекстное меню.



- **Состояния приложения** — чтобы управлять состояниями (включать их или отключать), отображаемыми в главном меню на вкладке Отслеживание, щелкните элемент Изменить. Вместо него для настройки состояний приложений можно использовать политики ESET Remote Administrator.
- **Сведения о лицензии** — когда включен этот параметр, отображаются сообщения и уведомления, касающиеся вашей лицензии.

- Предупреждения и уведомления — путем настройки параметров в разделе **Предупреждения и уведомления** можно изменить поведение системных уведомлений и предупреждений об обнаруженных угрозах. Их можно настроить в соответствии со своими потребностями. Если вы отключили отображение некоторых уведомлений, они будут присутствовать в области Отключенные сообщения и состояния. Здесь можно проверить их состояние, просмотреть дополнительные сведения или удалить их из данного окна.
- Настройка доступа — для обеспечения высокого уровня безопасности можно предотвратить несанкционированные изменения с помощью раздела **Настройка доступа**.
- Help — использовать локально установленную справку в качестве основного источника справочных сведений.
- Оболочка ESET — настроить права доступа к параметрам, функциям и данным программы через eShell можно путем изменения параметра **Политика выполнения оболочки ESET**.
- Контекстное меню — щелкните элемент правой кнопкой мыши, чтобы отобразить контекстное меню программы ESET File Security. Этот инструмент позволяет интегрировать элементы управления ESET File Security в контекстное меню.
- Режим презентации удобен для пользователей, которые хотят работать с приложением, не отвлекаясь на всплывающие окна, запланированные задачи и другие процессы, которые могут загружать системные ресурсы.

- Значок на панели задач.
- Восстановить все параметры в этом разделе/Восстановить параметры по умолчанию.

8.6.1 Предупреждения и уведомления

При помощи раздела **Предупреждения и уведомления** вкладки **Интерфейс пользователя** для программы ESET File Security можно настроить способ обработки предупреждений об угрозах и системных уведомлений (сообщений об успешном выполнении обновлений). Здесь можно настроить также время отображения и прозрачность уведомлений на панели задач (применяется только к системам, поддерживающим уведомления на панели задач).

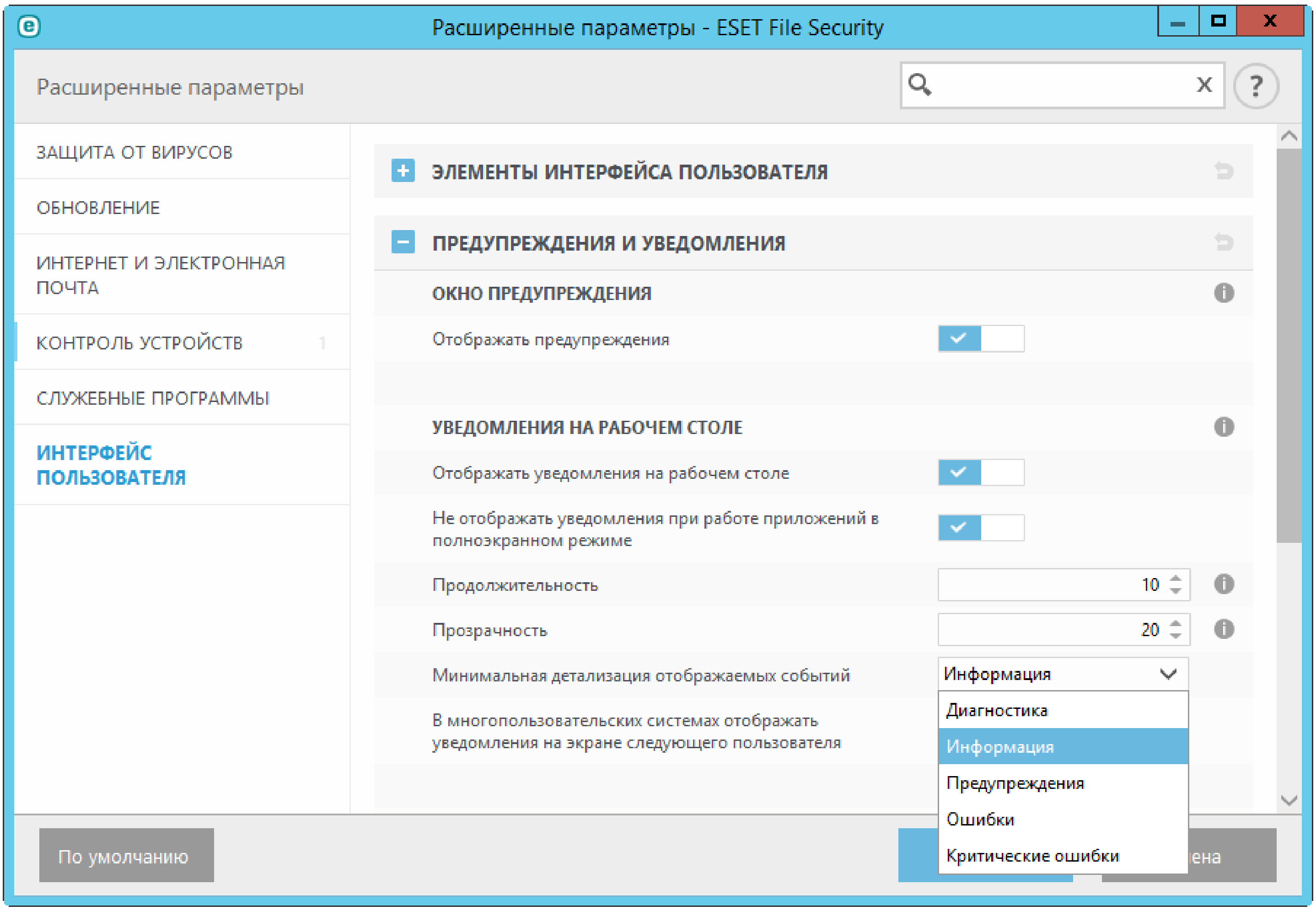
Окна предупреждений

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

Уведомления на рабочем столе

Уведомления на рабочем столе и всплывающие подсказки предназначены только для информирования и не требуют участия пользователя. Они отображаются в области уведомлений в правом нижнем углу экрана. Чтобы активировать уведомления на рабочем столе, установите флажок **Отображать уведомления на рабочем столе**. Более подробные параметры, такие как время отображения и прозрачность окна уведомлений, можно изменить, выполнив инструкции ниже.

Установите флажок **Не отображать уведомления при работе приложений в полноэкранном режиме**, чтобы запретить все неинтерактивные уведомления.



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

- **Диагностика** — в журнал вносится информация, необходимая для тщательной настройки программы, и все перечисленные выше записи.
- **Информация** — в журнал вносятся информационные сообщения, в том числе сообщения об успешном выполнении обновления, а также все перечисленные выше записи.
- **Предупреждения** — в журнал вносится информация обо всех критических ошибках и предупреждениях.
- **Ошибки** — в журнал вносится информация об ошибках загрузки файлов и критических ошибках.
- **Критические ошибки** — в журнал вносится только информация о критических ошибках (например, ошибках при запуске защиты от вирусов).

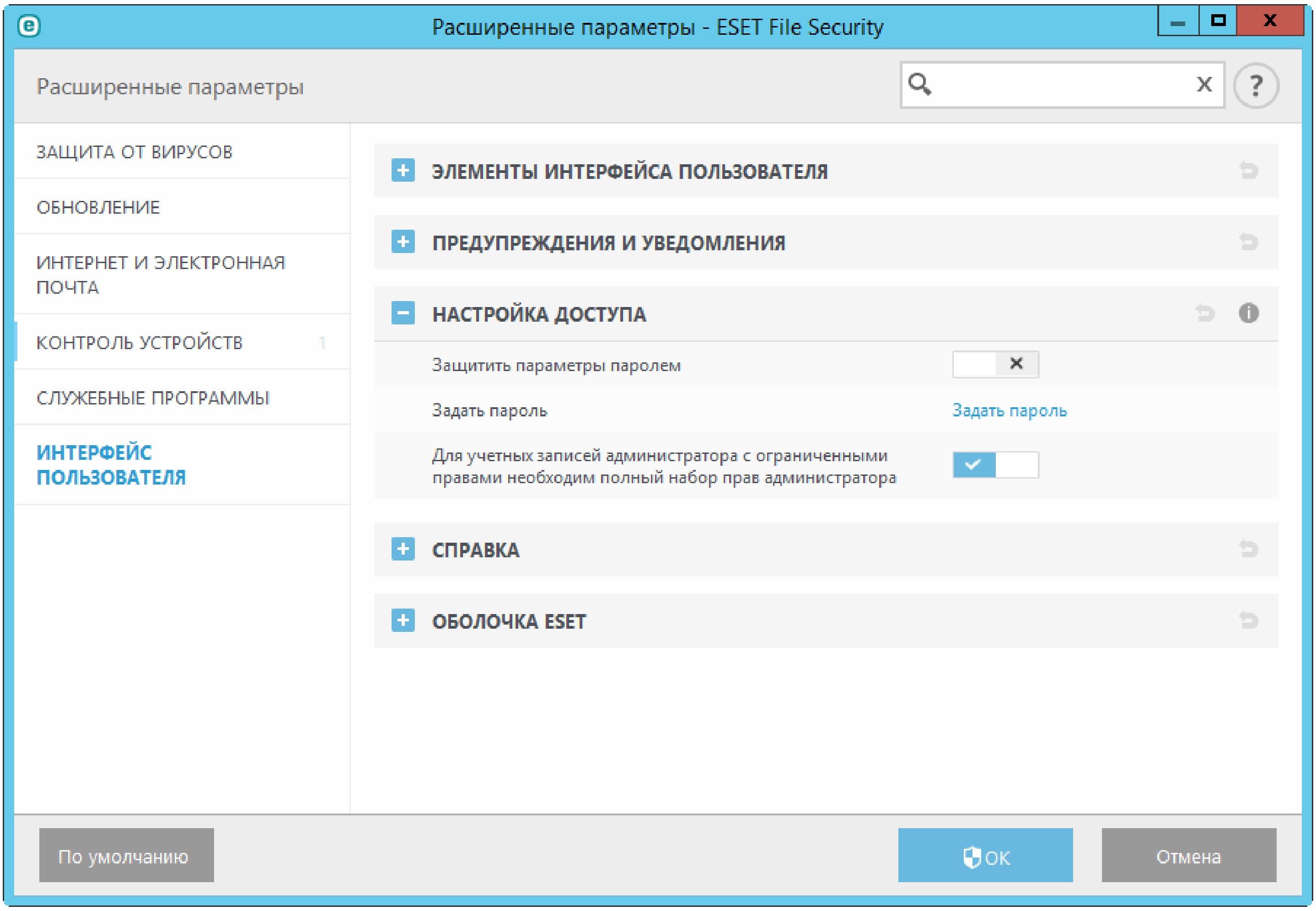
Последний параметр этого раздела позволяет настроить, кто именно должен получать уведомления в многопользовательской среде. В поле **В многопользовательских системах отображать уведомления для пользователя** указывается пользователь, который будет получать системные и прочие уведомления, если одновременно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

Окна сообщений

Чтобы по истечении определенного времени всплывающие окна закрывались автоматически, установите флажок **Автоматически закрывать окна сообщений**. Если окно предупреждения не будет закрыто пользователем, оно закрывается автоматически через указанный промежуток времени.

8.6.2 Настройка доступа

Для обеспечения максимальной безопасности системы важно правильно настроить ESET File Security. Неквалифицированное изменение параметров может привести к потере важных данных. Для предотвращения несанкционированного изменения параметры ESET File Security можно защитить паролем. Параметры защиты паролем расположены в подменю **Настройка доступа** в разделе **Интерфейс** в дереве **Дополнительные настройки** (F5).



Защитить параметры паролем: блокирует параметры настройки программы или снимает их блокировку. Щелкните этот элемент, чтобы открыть окно настройки пароля.

Чтобы задать или изменить пароль для защиты параметров настройки, щелкните элемент **Установить пароль**.

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

ПРИМЕЧАНИЕ.

Если пароль настройки доступа изменится и потребуется импортировать существующий файл конфигурации в формате *XML* (подписанный до изменения пароля) с помощью командной строки ESET CMD, не забудьте подписать его заново с помощью текущего пароля. Это позволит использовать старый файл конфигурации без необходимости экспортировать его на другом компьютере с работающей программой ESET File Security перед импортом.

8.6.2.1 Пароль

Для предотвращения несанкционированного изменения параметры ESET File Security можно защитить паролем.

8.6.2.2 Настройка пароля

Для защиты параметров установки ESET File Security от несанкционированного вмешательства необходимо установить новый пароль. Для смены пароля введите старый пароль в поле **Старый пароль**, а новый пароль — в поля **Новый пароль** и **Подтвердите пароль** и затем нажмите кнопку **OK**. Этот пароль будет необходим для внесения в будущем любых изменений в ESET File Security.

8.6.3 Справка

Если нажать клавишу **F1** или кнопку **?**, откроется окно интерактивной справки. Это окно — основной источник справочных сведений. Однако в программу включена и офлайн-справка. Офлайн-справка открывается, когда нет подключения к Интернету.

Если подключение к Интернету установлено, автоматически открывается последняя версия интерактивной справки.

8.6.4 Оболочка ESET

Настроить права доступа к параметрам, функциям и данным продукта через eShell можно путем изменения параметра **Политика выполнения оболочки ESET**. По умолчанию задано значение **Ограниченные сценарии**, но вместо него можно задать значение **Отключено**, **Только чтение** или **Полный доступ**.

- **Отключено**: решение eShell нельзя использовать. Разрешено только конфигурирование решения eShell в контексте `ui eshell` . Вы можете настроить внешний вид eShell, однако доступ к параметрам или данным любого продукта запрещен.
- **Только чтение**: решение eShell можно использовать как инструмент мониторинга. Как в интерактивном, так и в пакетном режиме все параметры можно просматривать, однако изменять параметры, свойства и данные нельзя.
- **Ограниченные сценарии**: в интерактивном режиме можно изменять все параметры, свойства и данные. В пакетном режиме решение eShell функционирует так, как если бы был включен режим «Только чтение». Однако если используются подписанные пакетные файлы, то можно настраивать параметры и изменять данные.
- **Полный доступ**: неограниченный доступ ко всем параметрам как в интерактивном, так и в пакетном режиме (при выполнении пакетных файлов). Все параметры доступны для просмотра и изменения. Для запуска eShell с полным доступом используйте учетную запись администратора. Кроме того, если включен контроль учетных записей, требуется также повышение прав.

8.6.5 Отключение графического интерфейса пользователя на сервере терминалов

В этой главе описывается, как отключать графический интерфейс пользователя программы ESET File Security, запущенной на сервере терминалов Windows для работы с сеансами пользователя.

Обычно графический интерфейс пользователя ESET File Security запускается при каждом входе удаленного пользователя на сервер и создании сеанса терминала. Обычно это нежелательно на серверах терминалов. Если нужно отключить графический интерфейс пользователя в сеансах терминала, сделать это можно с помощью eShell, выполнив команду `set ui ui gui-start-mode terminal`. Вследствие этого графический интерфейс пользователя будет переключен в режим терминала. Вот два доступных режима для запуска графического интерфейса пользователя:

```
set ui ui gui-start-mode full
set ui ui gui-start-mode terminal
```

Если нужно узнать, какой режим сейчас используется, выполните команду `get ui ui gui-start-mode`.

ПРИМЕЧАНИЕ.
Если вы установили ESET File Security на сервер Citrix, рекомендуется использовать параметры, описанные в нашей статье базы знаний.

8.6.6 Отключенные сообщения и состояния

Подтверждения — показывает список подтверждений, отображение которых можно включить или выключить.

Параметры состояний приложения — возможность включения и отключения отображения состояний в главном меню на вкладке **Отслеживание**.

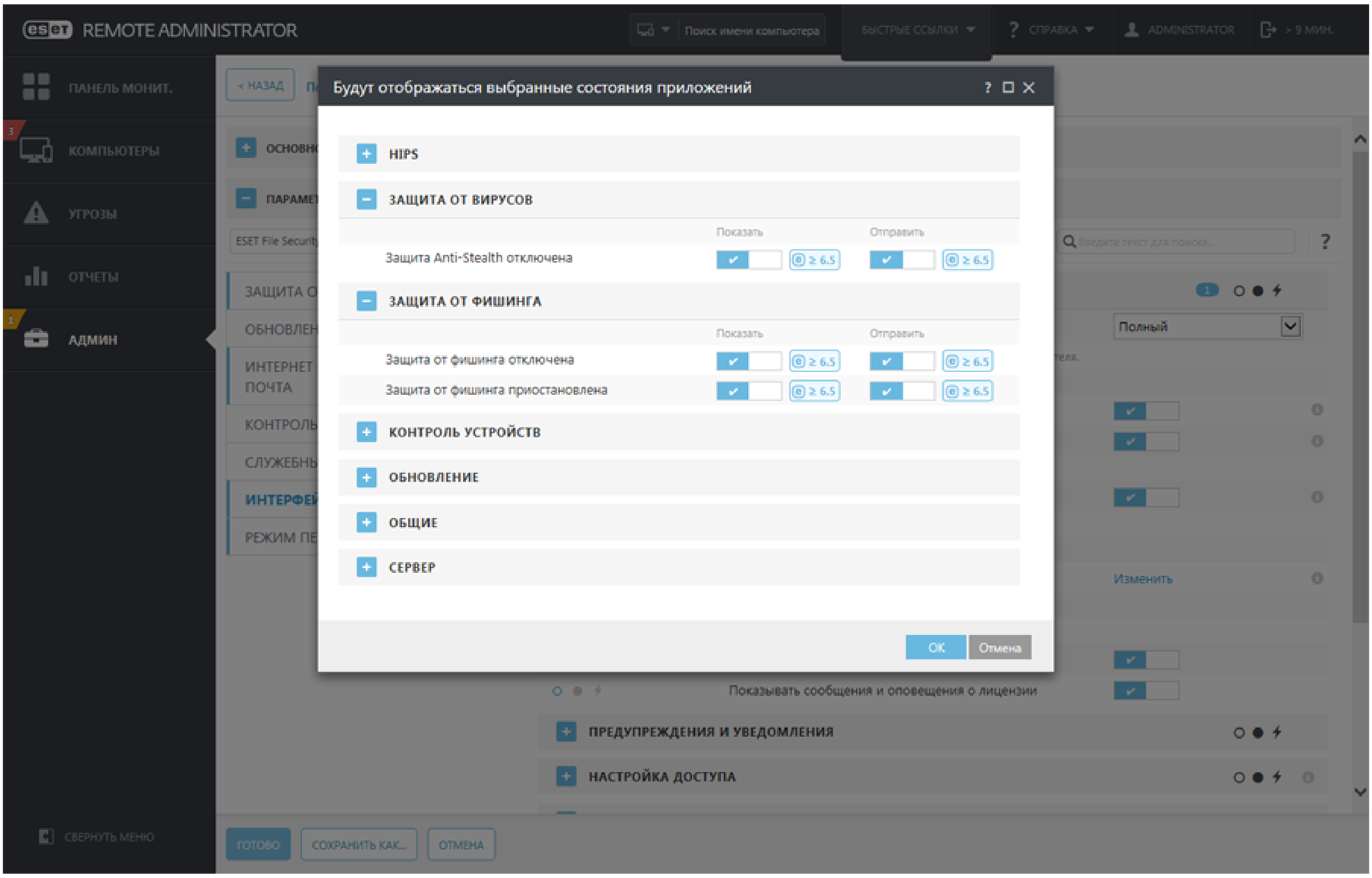
8.6.6.1 Подтверждения

В этом диалоговом окне отображаются подтверждения, выводимые ESET File Security перед выполнением какого-либо действия. Установите или снимите флажок рядом с каждым типом подтверждения, чтобы включить или отключить подтверждения этого типа.

8.6.6.2 Параметры состояний приложения

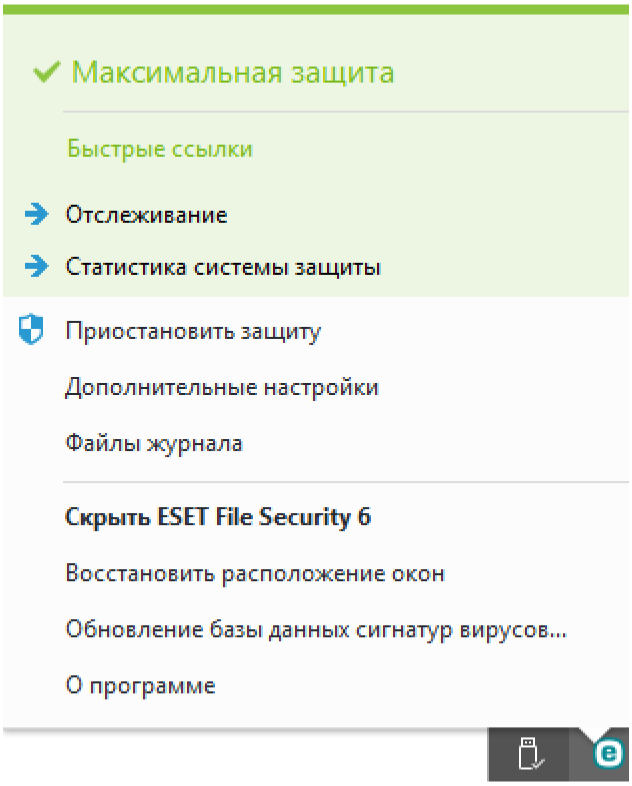
В этом диалоговом окне можно выбрать, какие состояния приложения нужно отображать, а какие — нет. Например, временное отключение защиты от вирусов и шпионских программ приведет к изменению состояния защиты, которое отображается на странице Отслеживание. Кроме того, состояние приложения отображается, если продукт не активирован или срок действия лицензии истек.

Состояниями приложения можно управлять при помощи политик ESET Remote Administrator. Для категорий и состояний в списке отображаются два параметра — **Показать** и **Отправить** состояние. Столбец «Отправить» отображается для состояний приложения только в конфигурации политики ESET Remote Administrator. В программе ESET File Security параметры отображаются со значком блокировки. Можно использовать режим переопределения, чтобы на некоторое время изменять состояния приложения.

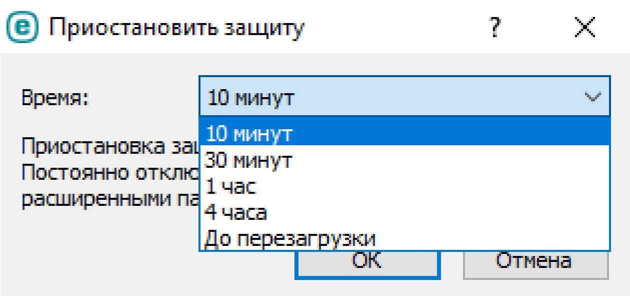


8.6.7 Значок на панели задач

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



Приостановить защиту — на экран выводится диалоговое окно для подтверждения. В нем можно отключить защиту от вирусов и шпионских программ, которая предотвращает атаки на компьютер, контролируя обмен файлами и данными через Интернет и электронную почту.



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

Дополнительные настройки — выберите этот параметр, чтобы перейти в раздел **Дополнительные настройки**. Перейти в раздел **Дополнительные настройки** можно также с помощью клавиши F5 или через меню **Настройки** > **Дополнительные настройки**.

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

Скрыть ESET File Security: позволяет скрыть окно ESET File Security.

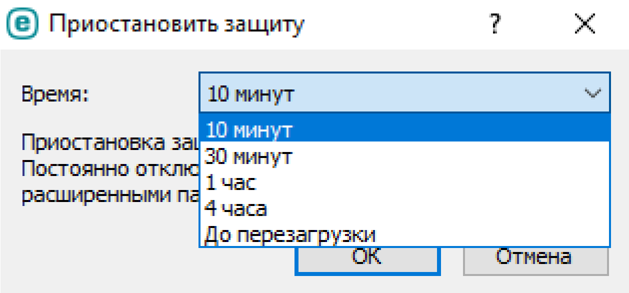
Восстановить расположение окон: для окна ESET File Security восстанавливаются размер и положение на экране по умолчанию.

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 File Security и модулях программы, а также срока действия лицензии. В нижней части окна представлена информация об операционной системе и системных ресурсах.

8.6.7.1 Приостановка защиты

Когда пользователь щелкает значок на панели задач, чтобы временно приостановить защиту от вирусов и шпионских программ, отображается диалоговое окно **Приостановка защиты**. В этом окне можно приостановить защиту от вредоносного ПО на определенный период времени (чтобы отключить защиту насовсем, необходимо использовать раздел **Дополнительные настройки**). Будьте осторожны: отключение защиты может сделать систему уязвимой для угроз.

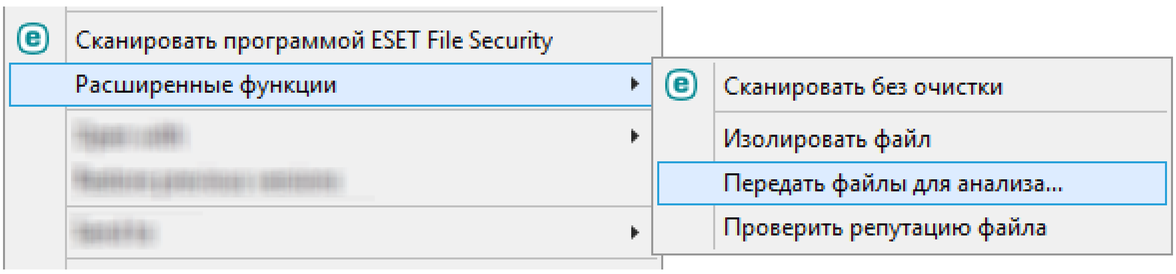


8.6.8 Контекстное меню

Если щелкнуть объект (файл) правой кнопкой мыши, отобразится контекстное меню. В меню указаны все действия, которые можно выполнить с объектом.

Элементы управления ESET File Security можно интегрировать в контекстное меню. Настройка этой функции выполняется в дереве **Дополнительные настройки**, доступ к которому можно получить, выбрав **Интерфейс** > **Элементы интерфейса**.

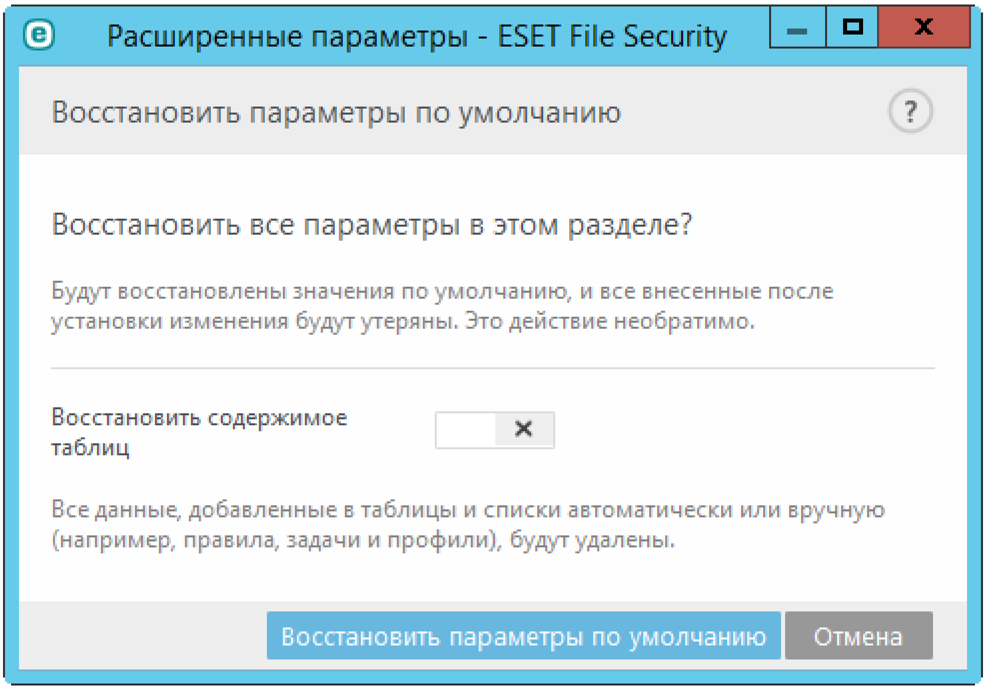
Интеграция в контекстное меню: можно интегрировать элементы управления ESET File Security в контекстное меню.



8.7 Восстановление всех параметров в разделе

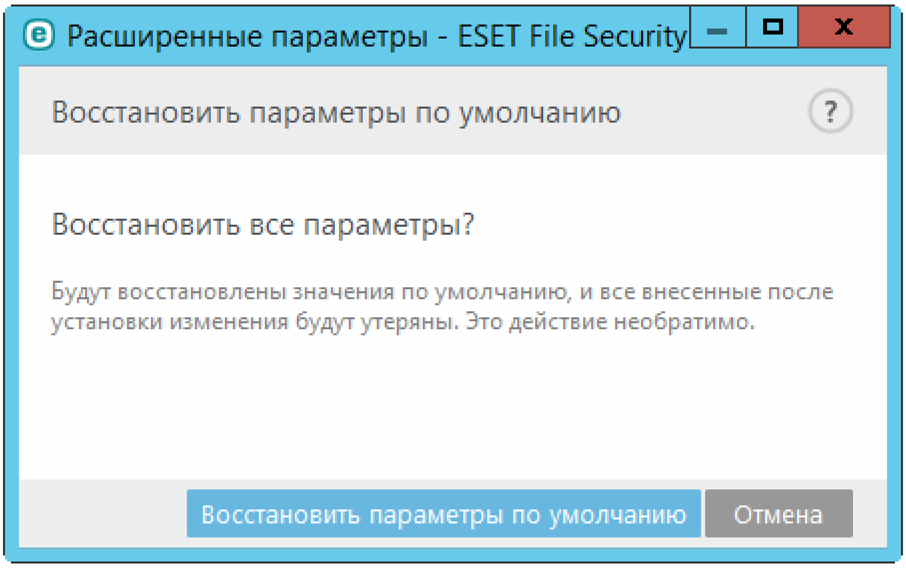
Восстановление параметров модуля по умолчанию, заданных компанией ESET. Следует помнить, что после нажатия кнопки **Восстановить параметры по умолчанию** любые внесенные изменения будут утеряны.

Восстановить содержимое таблиц — при активации этой функции все правила, задачи и профили, добавленные автоматически или вручную, будут удалены.



8.8 Восстановление параметров по умолчанию

Все параметры программы для всех модулей будут восстановлены до состояния, в котором они бы были после установки заново.



8.9 Планировщик

Планировщик предназначен для планирования следующих задач: обновление базы данных сигнатур вирусов, сканирование, проверка файлов, исполняемых при запуске системы, и обслуживание журнала. Добавлять и удалять задачи можно непосредственно в главном окне планировщика (нажмите кнопку «Добавить задачу» или «Удалить» в нижней части окна). Щелкнув правой кнопкой мыши в окне планировщика, можно выполнить следующие действия: отображение подробной информации, немедленное выполнение задачи, добавление новой задачи и удаление существующей задачи. Используйте флажки в начале каждой записи, чтобы активировать или деактивировать соответствующие задачи.

По умолчанию в планировщике отображаются следующие запланированные задачи.

- **Обслуживание журналов**
- **Регулярное автоматическое обновление**
- **Автоматическое обновление после установки модемного соединения**
- **Автоматическое обновление после входа пользователя в систему**
- **Автоматическая проверка файлов при загрузке системы** (после входа пользователя в систему)
- **Автоматическая проверка файлов при загрузке системы** (после успешного обновления базы данных сигнатур вирусов)
- **Автоматическое первое сканирование**

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

Добавление новой задачи

1. Щелкните Добавить задачу в нижней части окна.
2. Введите имя задачи.
3. Выберите тип задачи.
4. Активируйте кнопку **Включено**, если необходимо активировать задачу (это можно сделать позже, установив или сняв флажок в списке запланированных задач).
5. Нажмите кнопку **Далее** и выберите один из режимов времени выполнения, а затем укажите, когда задача будет выполнена опять.
6. Чтобы просмотреть запланированную задачу, дважды щелкните задачу в представлении Планировщик или щелкните ее правой кнопкой мыши и выберите пункт **Показать информацию о задаче**.

8.9.1 Сведения о задаче

Введите **имя задачи** и выберите в раскрывающемся меню нужный **тип задачи**.

- **Запуск внешнего приложения** — планирование выполнения внешнего приложения.
- **Обслуживание журнала** — в файлах журнала также содержатся остатки удаленных записей. Эта задача регулярно оптимизирует записи в файлах журнала для эффективной работы.
- **Проверка файлов при загрузке системы** — проверка файлов, исполнение которых разрешено при запуске системы или входе пользователя в нее.
- **Создать снимок состояния компьютера** — создание снимка состояния компьютера в решении ESET SysInspector, для которого собираются подробные сведения о компонентах системы (например, о драйверах и приложениях) и оценивается уровень риска для каждого из них.
- **Сканирование компьютера по требованию** — сканирование файлов и папок на компьютере.
- **Первое сканирование** — по умолчанию через 20 минут после установки или перезагрузки сканирование компьютера выполняется как задание с низким приоритетом.
- **Обновление** — планирование задачи обновления, в рамках которой обновляются база данных сигнатур вирусов и программные модули.
- **Сканирование Hyper-V** — планирование сканирования виртуальных дисков в Hyper-V.

Если нужно отключить задачу сразу после ее создания, щелкните переключатель возле элемента **Включено**. Вы можете активировать задачу позже, установив соответствующий флажок в представлении планировщика. Чтобы перейти к следующему этапу, нажмите кнопку **Далее**.

8.9.2 Время задачи: однократно

Укажите дату и время однократного **выполнения задачи**.

8.9.3 Время задачи

Чтобы задать время для запуска **запланированной задачи**, выберите один из приведенных далее параметров.

- Однократно — задача выполняется один раз в указанные дату и время.
- Многократно — задача выполняется регулярно через указанный промежуток времени (в минутах).
- Ежедневно — задача выполняется каждый день в указанное время.
- Еженедельно — задача выполняется один или несколько раз в неделю в указанные дни и время.
- При определенных условиях — задача выполняется при возникновении указанного события.

Пропускать задачу, если устройство работает от аккумулятора — задача не запускается, если на момент ее планируемого запуска система работает от аккумулятора. Это относится, например, к компьютерам, работающим от источника бесперебойного питания.

Чтобы перейти к следующему этапу, нажмите кнопку **Далее**.

8.9.4 Время задачи: ежедневно

Укажите время, в которое задача должна выполняться каждый день.

8.9.5 Время задачи: еженедельно

Задача будет выполняться в выбранный день недели в указанное время.

8.9.6 Время задачи: при определенных условиях

Задача запускается в случае возникновения одного из перечисленных далее событий.

- **При каждом запуске компьютера**
- **Каждые сутки при первом запуске компьютера**
- **Модемное подключение к Интернету/VPN**
- **Успешное обновление базы данных сигнатур вирусов**
- **Успешное обновление компонентов программы**
- **Вход пользователя в систему**
- **Обнаружение угроз**

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

8.9.7 Сведения о задаче: запуск приложения

На этой вкладке можно запланировать выполнение внешнего приложения.

- **Исполняемый файл**: выберите исполняемый файл в дереве каталогов, нажмите кнопку обзора (**...**) или введите путь вручную.
- **Рабочая папка**: задайте рабочий каталог внешнего приложения. Все временные файлы выбранного в поле **Исполняемый файл** файла будут создаваться в этом каталоге.
- **Параметры** — параметры командной строки для приложения (необязательно).

Чтобы создать задачу или применить изменения в существующей запланированной задаче, щелкните **Готово**.

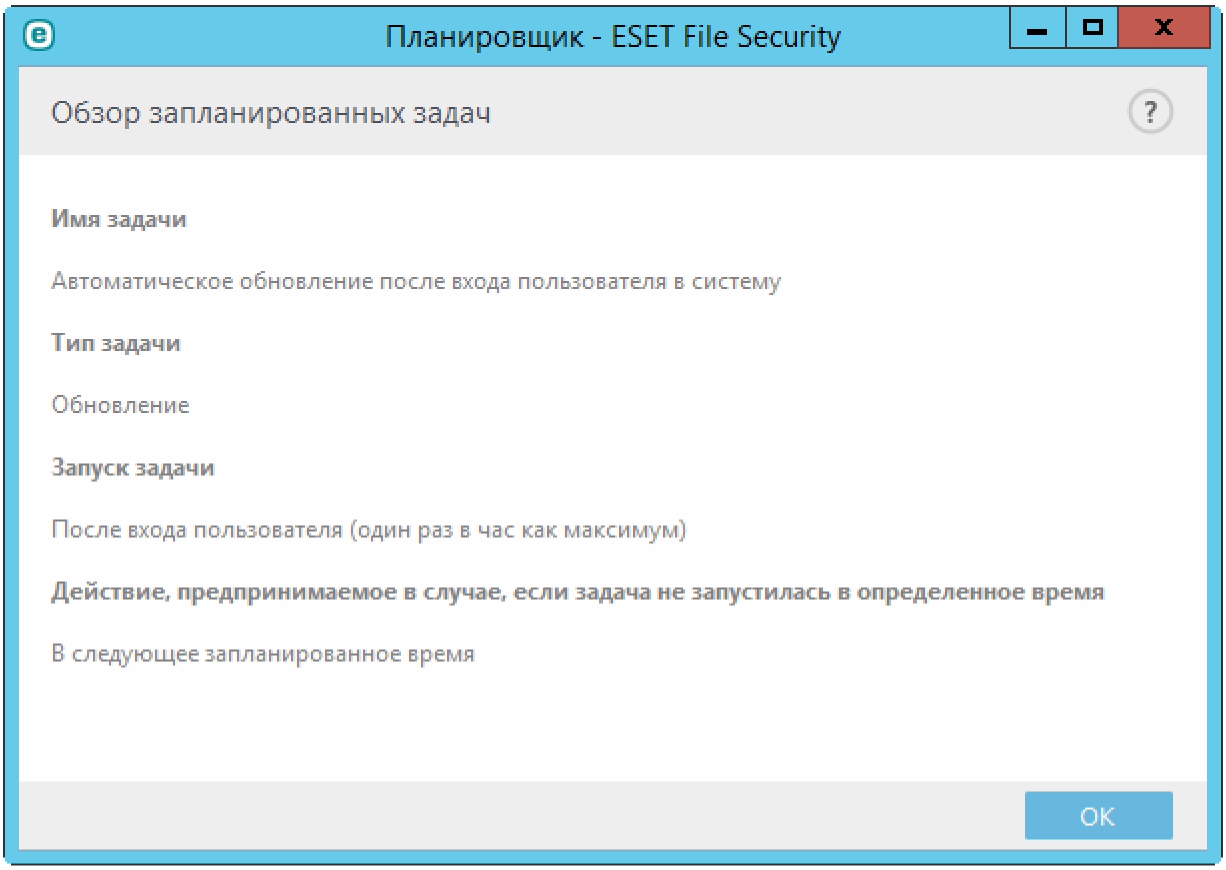
8.9.8 Пропущенная задача

Если задача не могла быть выполнена в отведенное ей время, можно указать, когда будет предпринята следующая попытка запуска задачи.

- **В следующее запланированное время**: задача будет выполнена в указанное время (например, через 24 часа).
- **Как можно скорее** — задача будет выполнена при первой возможности, когда условия, предотвращающие ее выполнение, перестанут действовать.
- **Незамедлительно, если с момента последнего запуска прошло больше времени, чем указано**, **Время с момента последнего запуска (ч)** — после выбора этих параметров задача всегда будет повторяться через указанный период времени (в часах).

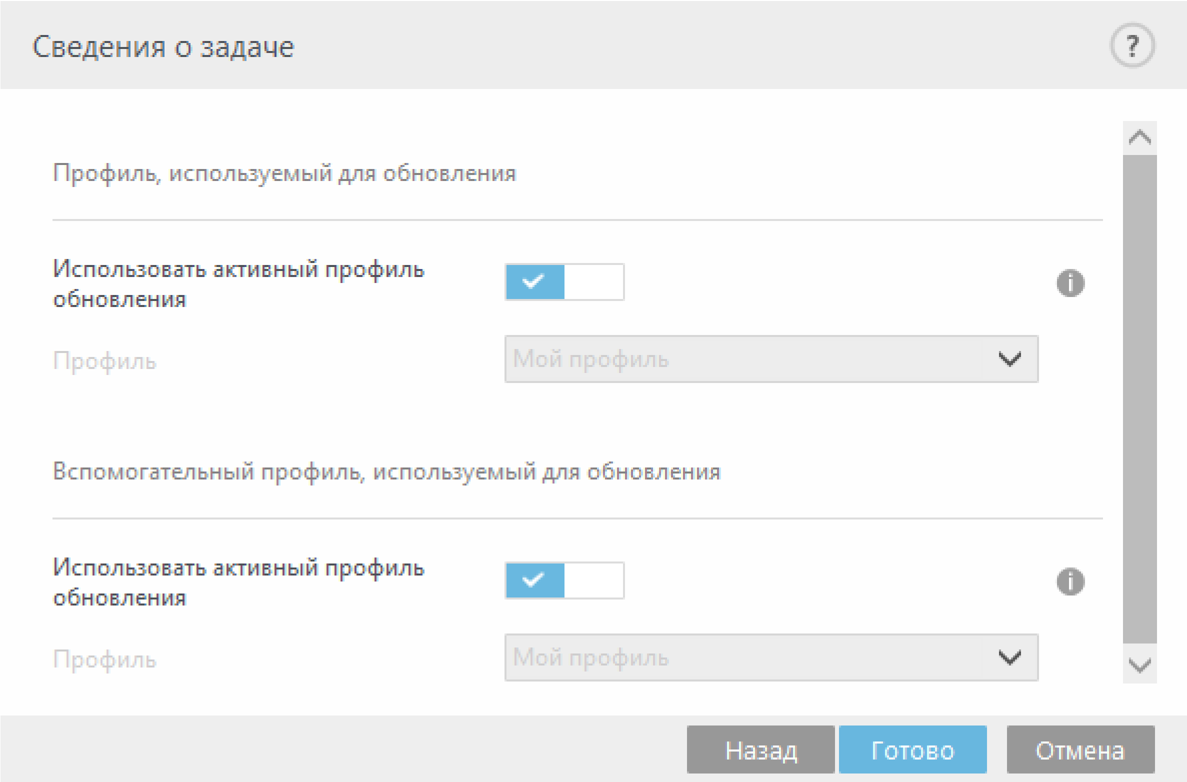
8.9.9 Обзор запланированных задач

В этом диалоговом окне отображается подробная информация о запланированной задаче. Чтобы его открыть, дважды щелкните задачу в представлении планировщика или щелкните ее правой кнопкой мыши и выберите пункт **Показать информацию о задаче**.



8.9.10 Профили обновления

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



Дополнительные сведения о профилях обновлений приведены в главе Обновление.

8.10 Карантин

- Помещение файлов на карантин
- Восстановление из карантина
- Отправка файла из карантина

8.10.1 Помещение файлов на карантин

Программа ESET File Security автоматически помещает удаленные файлы в 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 помещения файлов на карантин можно воспользоваться также контекстным меню. Щелкните правой кнопкой мыши в окне **Карантин** и выберите пункт **Карантин**.

8.10.2 Восстановление из карантина

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

Удаление из карантина: щелкните элемент правой кнопкой мыши и выберите команду **Удалить из карантина** или выберите элемент, который нужно удалить, и нажмите клавишу **DELETE** на клавиатуре. Кроме того, вы можете выделить и удалить несколько элементов одновременно.

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

8.10.3 Отправка файла из карантина

Если на карантин помещен подозрительный файл, не обнаруженный программой, или файл неверно квалифицирован как зараженный (например, путем эвристического анализа кода) и помещен на карантин, отправьте его в антивирусную лабораторию ESET. Для отправки файла из карантина щелкните его правой кнопкой мыши и выберите в контекстном меню пункт **Передать на анализ**.

8.11 Обновления операционной системы

В окне «Обновления системы» представлен список доступных обновлений, готовых для загрузки и установки. Уровень приоритета обновления отображается справа от его названия.

Нажмите **Запустить обновление системы**, чтобы начать загрузку и установку обновлений операционной системы.

Щелкните правой кнопкой мыши любую строку обновления и нажмите кнопку **Показать информацию**, чтобы вывести на экран всплывающее окно с дополнительной информацией.

9. Глоссарий

Глоссарий содержит множество технических терминов, связанных с угрозами и безопасностью в Интернете.

Выберите категорию (или см. глоссарий вирусного радара в Интернете):

- Типы заражений
- Электронная почта

9.1 Типы заражений

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

- Вирусы
- Черви
- Троянские программы
- Руткиты
- Рекламные программы
- Шпионские программы
- Ботнет
- Программы-шантажисты
- Упаковщики
- Блокировщик эксплойтов
- Расширенный модуль сканирования памяти
- Потенциально опасные приложения
- Потенциально нежелательные приложения

ПРИМЕЧАНИЕ.
Посетите нашу страницу Вирусный радар, чтобы получить дополнительные сведения о глоссарии, версиях базы данных сигнатур вирусов ESET или служебных программах.

9.1.1 Вирусы

Компьютерный вирус — это такой вид заражения, который повреждает существующие на компьютере файлы. Название было выбрано из-за сходства с биологическими вирусами, поскольку они используют похожие методы для распространения с компьютера на компьютер.

Компьютерные вирусы атакуют в основном исполняемые файлы и документы. Для размножения вирус присоединяет свое «тело» в конец заражаемого файла. Компьютерный вирус функционирует следующим образом: после запуска зараженного файла вирус активируется (это происходит перед активацией самого приложения) и выполняет возложенные на него задачи. Только после этого запускается само приложение. Вирус не может заразить компьютер, пока пользователь (по ошибке или намеренно) собственноручно не запустит вредоносную программу.

Компьютерные вирусы могут быть разными по целям и степени опасности. Некоторые из вирусов особо опасны, поскольку 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.

Важно отметить, что количество вирусов постоянно снижается по сравнению с троянскими и шпионскими программами, поскольку они не представляют для авторов экономической выгоды. Кроме того, термин «вирус» часто неправильно используют для описания всех типов заражений. Однако постепенно он выходит из употребления, и на смену ему приходит более точный термин «вредоносная программа».

Если компьютер заражен вирусом, необходимо восстановить исходное состояние зараженных файлов, т. е. очистить их с помощью программы для защиты от вирусов.

Примеры вирусов: OneHalf, Tenga и Yankee Doodle.

9.1.2 Черви

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

По этой причине черви намного более жизнеспособны, 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 выступать в качестве «транспортного средства» для других типов заражений.

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

Примеры широко известных червей: Lovsan/Blaster, Stration/Warezov, Bagle и Netsky.

9.1.3 Троянские программы

Исторически троянскими программами называли такой класс заражений, которые пытаются маскироваться под полезные программы, тем самым заставляя пользователей запускать их. Однако важно отметить, что на сегодняшний день это определение устарело и троянские программы больше не нуждаются в подобного рода маскировке. Единственной их целью является максимально быстрое проникновение в систему и выполнение своих вредоносных задач. Сегодня «троянская программа» — очень общий термин, используемый для обозначения любого заражения, которое невозможно отнести к какому-либо конкретному классу.

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

- **Загрузчик** — вредоносная программа, способная загружать другие заражения из Интернета.
- **Троян-загрузчик** — тип троянской программы, предназначенный для заражения компьютеров другими вредоносными программами.
- **Лазейка** — приложение, которое удаленно обменивается данными со злоумышленниками, помогая им получить доступ к системе и контроль над ней.
- **Клавиатурный шпион** — программа, которая регистрирует все, что пользователь набирает на клавиатуре, и отправляет эту информацию злоумышленникам.
- **Программа дозвона** — программа, предназначенная для набора номеров телефонов, вызовы на которые оплачивает вызывающий абонент. 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.

Троянская программа обычно представляет собой исполняемый файл с расширением .exe. Если на компьютере обнаружен файл, классифицированный как троянская программа, рекомендуется удалить его, поскольку он с большой вероятностью содержит вредоносный код.

Примеры широко известных троянских программ:: NetBus, Trojandownloader. Small.ZL, Slapper.

9.1.4 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 реестра Windows и т. п. По этой причине их активность практически невозможно обнаружить, используя стандартные методы тестирования.

Существует два уровня обнаружения, направленных на борьбу с руткитами.

1) Обнаружение при попытке проникновения в систему. Их еще нет в системе, то есть они неактивны. 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. В распоряжении пользователей ESET File Security есть преимущества технологии Anti-Stealth, которая позволяет обнаружить и устранить активные руткиты.

9.1.5 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. Зачастую рекламные программы 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, как в шпионских программах.

Если пользователь решает использовать бесплатный программный продукт, следует уделить особое внимание программе установки. Чаще всего программа установки предупреждает об установке дополнительной рекламной программы. Зачастую пользователь имеет возможность отказаться от этого 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 обезопасить себя, чем потом сожалеть. В случае обнаружения на компьютере файла, классифицированного как рекламная программа, рекомендуется удалить его, поскольку с высокой вероятностью он содержит вредоносный код.

9.1.6 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 списка контактов пользователя или список нажатий клавиш на клавиатуре.

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 банковских 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 шпионской программы во время установки основной программы, чтобы поощрить их к приобретению платной версии, в которой шпионской программы нет.

Примерами хорошо известного бесплатного программного обеспечения, вместе с которым поставляется шпионское, могут служить клиенты одноранговых (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, поскольку с высокой вероятностью он содержит вредоносный код.

9.1.7 Ботнет

Бот или веб-робот — это автоматизированная вредоносная программа, которая сканирует блоки сетевых адресов и заражает уязвимые компьютеры. Это позволяет хакерам получить контроль над множеством компьютеров одновременно и превратить их в ботов (называемых также «зомби»). Хакеры обычно используют боты, чтобы заразить большое количество компьютеров. Большая группа зараженных компьютеров называется ботнетом. Зараженный компьютер, являющийся частью ботнета, может использоваться для проведения распределенных атак типа «отказ в обслуживании» (DDoS) и выполнения автоматизированных задач в Интернете без вашего ведома (например, отправка спама и вирусов, кража личной и конфиденциальной информации, включающей банковские учетные данные или номера кредитных карт).

Для получения дополнительных сведений см. раздел Вирусный радар.

9.1.8 Программы-шантажисты

Определенный вид вредоносного программного обеспечения, которое используется для вымогательства. После активации программы-шантажисты блокируют доступ к устройству или данным на нем, пока жертва не заплатит выкуп.

9.1.9 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.

9.1.10 Блокировщик эксплойтов

Блокировщик эксплойтов предназначен для защиты приложений, которые обычно уязвимы для эксплойтов, например браузеров, программ для чтения PDF-файлов, почтовых клиентов и компонентов MS Office. Он осуществляет мониторинг работы процессов для выявления подозрительных действий, которые могли бы означать использование эксплойта. Он добавляет дополнительный слой защиты между пользователем и злоумышленниками. Технология, которая при этом используется, полностью отличается от технологий, ориентированных на выявление вредоносных программ.

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

9.1.11 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, предназначенными для защиты от вредоносных программ, за счет использования умышленного запутывания и/или шифрования. Когда обычной эмуляции или эвристики недостаточно для обнаружения угрозы, расширенный модуль сканирования памяти может определять подозрительные действия и сканировать угрозы, появляющиеся в системной памяти. Это решение эффективно даже против вредоносных программ с высокой степенью умышленного запутывания. В отличие от блокировщика эксплойтов это решение применяется после выполнения, поэтому существует риск того, что некоторые вредоносные действия могут быть выполнены до обнаружения угрозы. Однако, если применение других методов обнаружения не дало результатов, такое решение обеспечивает дополнительный уровень безопасности.

9.1.12 Потенциально опасные приложения

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

Потенциально опасными приложениями считаются нормальные коммерческие программы. 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.

9.1.13 Потенциально нежелательные приложения

Потенциально нежелательные приложения не всегда являются вредоносными, однако могут негативно повлиять на производительность компьютера. Обычно перед установкой таких приложений запрашивается согласие пользователя. После их установки поведение системы изменяется (по сравнению с тем, как она вела себя до установки этих приложений). Наиболее заметные изменения следующие:

- открываются новые окна, которые не появлялись ранее (всплывающие окна, реклама);
- активируются и выполняются скрытые процессы;
- повышается уровень потребления системных ресурсов;
- появляются изменения в результатах поиска;
- приложение обменивается данными с удаленными серверами.

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

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

9.2 Электронная почта

Электронная почта является современным средством общения, которое имеет множество преимуществ. Она отличается гибкостью, высокой скоростью и отсутствием посредников и сыграла ключевую роль в становлении Интернета в начале 90-х годов прошлого века.

К сожалению, вследствие высокого уровня анонимности электронная почта и Интернет оставляют пространство для таких незаконных действий, как рассылка спама. Спам может содержать нежелательные рекламные объявления, мистификации или вложения, распространяющие вредоносные программы. 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 делают его регуляцию крайне затруднительной. 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 полученные нежелательные сообщения.
- 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.

9.2.1 Рекламные объявления

Реклама в Интернете является одним из наиболее бурно развивающихся видов рекламы. Ее преимуществами являются минимальные затраты и высокая вероятность непосредственного общения с потребителем. Кроме того, сообщения доставляются практически мгновенно. Многие компании используют электронную почту в качестве эффективного маркетингового инструмента для общения со своими 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 пересекает границу 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.

9.2.2 Мистификации

Мистификацией называется ложная информация, распространяемая 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 у получателей страх, неуверенность и сомнения, побуждая их верить в то, что «не поддающийся обнаружению вирус» удаляет их файлы, крадет пароли или выполняет какие-либо другие вредоносные действия на их компьютерах.

Некоторые мистификации работают, предлагая получателям переслать сообщение своим знакомым, увеличивая тем самым 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.

9.2.3 Фишинг

Термин «фишинг» обозначает преступную деятельность, в рамках которой используются методы социальной инженерии (манипулирование пользователем, направленное на получение конфиденциальной информации). Целью фишинга является получение доступа к таким конфиденциальным данным, как номера банковских счетов, PIN-коды и т. п.

Попытка получения информации обычно представляет собой отправку сообщения якобы от доверенного лица или компании (например, финансового учреждения или страховой компании). Сообщение может казаться благонадежным и содержать изображения и текст, которые могли изначально быть получены от источника, якобы являющегося отправителем данного сообщения. Под разными предлогами (проверка данных, финансовые операции) предлагается предоставить какую-либо личную информацию, такую как номера банковских счетов, имена пользователя, пароли и т. д. Если такие данные предоставляются, они легко могут быть украдены и использованы в преступных целях.

Банки, страховые компании и другие легитимные организации никогда не запрашивают имена пользователей и пароли в незапрошенных сообщениях электронной почты.