ESET MAIL SECURITY

ДЛЯ MICROSOFT EXCHANGE SERVER

Инструкция по установке и руководство пользователя

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

Щелкните здесь, чтобы загрузить актуальную версию этого документа

ENJOY SAFER TECHNOLOGY™

ESET **MAIL SECURITY**

Программный продукт ESET Mail Security разработан компанией ESET, spol. s r.o..

Служба поддержки клиентов: www.eset.com/support

Испр. 15/03/2016

Содержание

Содержание

1. Введение

ESET Mail Security 6 для Microsoft Exchange Server — это интегрированное решение, которое защищает почтовые ящики от различных типов вредоносных программ, в том числе вложений, зараженных червями и троянскими программами, документов, в которых содержатся вредоносные сценарии, а также от фишинга и спама. ESET Mail Security обеспечивает три типа защиты: защита от вирусов, защита от спама и применение пользовательских правил. ESET Mail Security фильтрует вредоносное содержимое на уровне почтового сервера, прежде чем оно попадет в папку «Входящие» почтового клиента получателя.

Программа ESET Mail Security поддерживает Microsoft Exchange Server 2003 и более поздние версии, а также Microsoft Exchange Server в кластерной среде. В более новых версиях (начиная с Microsoft Exchange Server 2003) поддерживаются также конкретные роли (почтовый ящик, концентратор, пограничный сервер). Вы можете удаленно управлять ESET Mail Security в больших сетях с помощью ESET Remote Administrator.

Обеспечивая защиту Microsoft Exchange Server, ESET Mail Security имеет в своем составе также служебные программы для защиты самого сервера (резидентная защита, защита доступа в Интернет и защита почтового клиента).

1.1 Новые возможности в версии 6

- Средство управления карантином почты. Администратор может проверять объекты в этом разделе хранилища и, по своему решению, удалять или освобождать их. Эта функция позволяет с легкостью управлять сообщениями электронной почты, которые агент транспорта поместил в карантин.
- Веб-интерфейс карантина почты. Интернет-альтернатива средству управления карантином почты.
- Защиты от спама: этот базовый компонент подвергся основательной переработке, и теперь в нем используется новая удостоенная наград подсистема с улучшенной производительностью.
- Сканирование базы данных по требованию. Модуль сканирования базы данных по требованию использует интерфейс API веб-служб Exchange для подключения к серверу Microsoft Exchange Server по протоколу HTTP или HTTPS. Кроме того, модуль сканирования использует параллельное сканирование для улучшения производительности.
- Правила. Позволяет администраторам вручную задавать условия фильтрации электронной почты и действия, которые необходимо выполнить с отфильтрованными сообщениями. Правила для последней версии <%PN%> были изменены и теперь обеспечивают большую гибкость и предоставляют пользователям еще больше возможностей.
- Кластер ESET. Объединение рабочих станций с узлами дополнительно автоматизирует управление, так как становится возможным распределять политики конфигурации по всем элементам кластера (подобное происходит и при использовании ESET File Security 6 для Microsoft Windows Server). Создавать кластеры можно с помощью установленного узла, который может затем установить и запустить все узлы удаленно. При этом серверные продукты ESET могут обмениваться такими данными, как конфигурация и оповещения, а также выполнять синхронизацию данных, необходимых для надлежащей работы группы экземпляров продуктов. Это позволяет применять одну конфигурацию продукта для всех элементов кластера. Отказоустойчивый кластер Windows и кластер балансировки сетевой нагрузки (NLB) поддерживаются продуктом ESET Mail 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.
- Установка на основе компонентов: пользователь может выбрать, какие компоненты нужно добавить или удалить.
- Исключения для процессов: пользователь может исключить определенные процессы из сканирования на

наличие вирусов при доступе. Из-за высокой важности выделенных серверов (сервера приложений, сервера хранилища и т. д.) необходимо регулярно выполнять резервное копирование, чтобы своевременно восстанавливать данные после любых неустранимых ошибок. Чтобы ускорить резервное копирование, сделать процесс целостнее, а службу — доступнее, во время резервного копирования используются техники, которые конфликтуют с защитой от вирусов, действующей на файловом уровне. Подобные проблемы могут возникнуть и при попытке динамического переноса виртуальных машин. Единственный эффективный способ избежать обеих ситуаций — это отключить антивирусное программное обеспечение. Если исключить некоторые процессы (например, процессы в решении резервного копирования), то все операции с файлами, которые касаются исключенных процессов, игнорируются и считаются безопасными. Таким образом факторы, мешающие резервному копированию, сводятся к минимуму. Рекомендуется проявлять осторожность при создании исключений, так как исключенное средство резервного копирования может взаимодействовать с зараженными файлами, не вызывая предупреждений (поэтому расширенные разрешения можно использовать только в модуле защиты в режиме реального времени).

- Сборщик журналов ESET: автоматически собирает информацию о конфигурации и многочисленных журналах ESET Mail Security. Сборщик журналов ESET упростит сбор диагностических сведений, необходимых техническим специалистам ESET для устранения проблемы.
- eShell (ESET Shell): eShell 2.0 теперь доступен в ESET Mail Security. eShell — это интерфейс командной строки, в котором опытные пользователи и администраторы найдут исчерпывающий спектр параметров для управления серверными продуктами ESET.
- 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.
- Улучшенная интеграция с ESET Remote Administrator, в том числе возможность добавить в расписание сканирование по требованию.

1.2 Страницы справочной системы

Уважаемый клиент, добро пожаловать в ESET Mail Security. Это руководство поможет вам использовать ESET Mail Security максимально эффективно.

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**.

Дополнительные сведения о любом окне программы можно получить, нажав клавишу F1, когда это окно открыто. Откроется страница справки, содержащая информацию о текущем окне.

Программа ESET Mail 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.

1.3 Используемые методы

Ниже описаны три метода, используемых для сканирования сообщений электронной почты.

- Защита базы данных почтовых ящиков: метод, ранее известный как сканирование почтовых ящиков с помощью VSAPI. Защита этого типа доступна только для Microsoft Exchange Server 2010, 2007 и 2003 с ролью сервера почтовых ящиков (Microsoft Exchange 2010 и 2007) или тылового сервера (Microsoft Exchange 2003). Сканирование этого типа можно выполнить на одиночном сервере, на котором активированы несколько ролей Exchange Server и который установлен на одном компьютере (если среди этих ролей есть роль сервера почтовых ящиков или тылового сервера).
- Защита почтового транспорта: метод, ранее известный как фильтрация сообщений на уровне SMTP-сервера.

Этот метод предоставляется транспортным агентом и доступен только для Microsoft Exchange Server (начиная с версии 2007) с ролью пограничного транспортного сервера или транспортного сервера-концентратора. Сканирование этого типа можно выполнить на одиночном сервере, на котором активированы несколько ролей Exchange Server и который установлен на одном компьютере (если среди этих ролей есть любая из упомянутых выше серверных ролей).

- Сканирование базы данных по требованию: функция, позволяющая выполнить или запланировать сканирование базы данных почтовых ящиков Exchange. Эта функция доступна только для сервера Microsoft Exchange Server (начиная с версии 2007), на котором активирована роль сервера почтовых ящиков или транспортного сервера-концентратора. Сказанное относится также к одиночному серверу, на котором активированы несколько ролей Exchange Server и который установлен на одном компьютере (если среди этих ролей есть любая из упомянутых выше серверных ролей). Дополнительные сведения о ролях в Exchange 2013 см. в разделе Роли Exchange Server 2013.

1.3.1 Защита базы данных почтовых ящиков

Процесс сканирования почтовых ящиков запускается и контролируется Microsoft Exchange Server. Сообщения в базе данных хранилища Microsoft Exchange Server сканируются непрерывно. В зависимости от версии Microsoft Exchange Server, версии интерфейса VSAPI и пользовательских параметров процесс сканирования можно запустить в любой из следующих ситуаций.

- Пользователь открывает электронную почту, например в почтовом клиенте (электронная почта всегда сканируется с применением последней базы данных сигнатур вирусов).
- В фоновом режиме, когда ресурсы Microsoft Exchange Server используются в малых количествах.
- Упреждающим образом (на основе внутреннего алгоритма Microsoft Exchange Server).

В настоящий момент интерфейс VSAPI используются для сканирования модулем защиты от вирусов и защиты на основе правил.

1.3.2 Защита почтового транспорта

Фильтрация на уровне SMTP-сервера осуществляется специализированным подключаемым модулем. В Microsoft Exchange Server 2000 и 2003 этот подключаемый модуль (приемник событий) регистрируется на SMTP-сервере в составе служб IIS. В Microsoft Exchange Server 2007/2010 этот подключаемый модуль регистрируется в качестве агента транспорта на ролях «Пограничный сервер» или «Концентратор» сервера Microsoft Exchange Server.

Фильтрация на уровне SMTP-сервера агентом транспорта обеспечивает защиту в форме защиты от вирусов, защиты от спама и пользовательских правил. В отличие от фильтрации посредством VSAPI фильтрация на уровне SMTP-сервера выполняется до того, как просканированное сообщение электронной почты попадает в почтовый ящик Microsoft Exchange Server.

1.3.3 Сканирование базы данных по требованию

Так как сканирование всей базы данных электронной почты может быть сопряжено с нежелательной нагрузкой на систему, вы можете выбрать, какие отдельные базы данных и почтовые ящики нужно сканировать. Чтобы свести к минимуму использование ресурсов системы, вы можете выполнить еще более глубокую фильтрацию объектов сканирования, указав метку времени нужных сообщений.

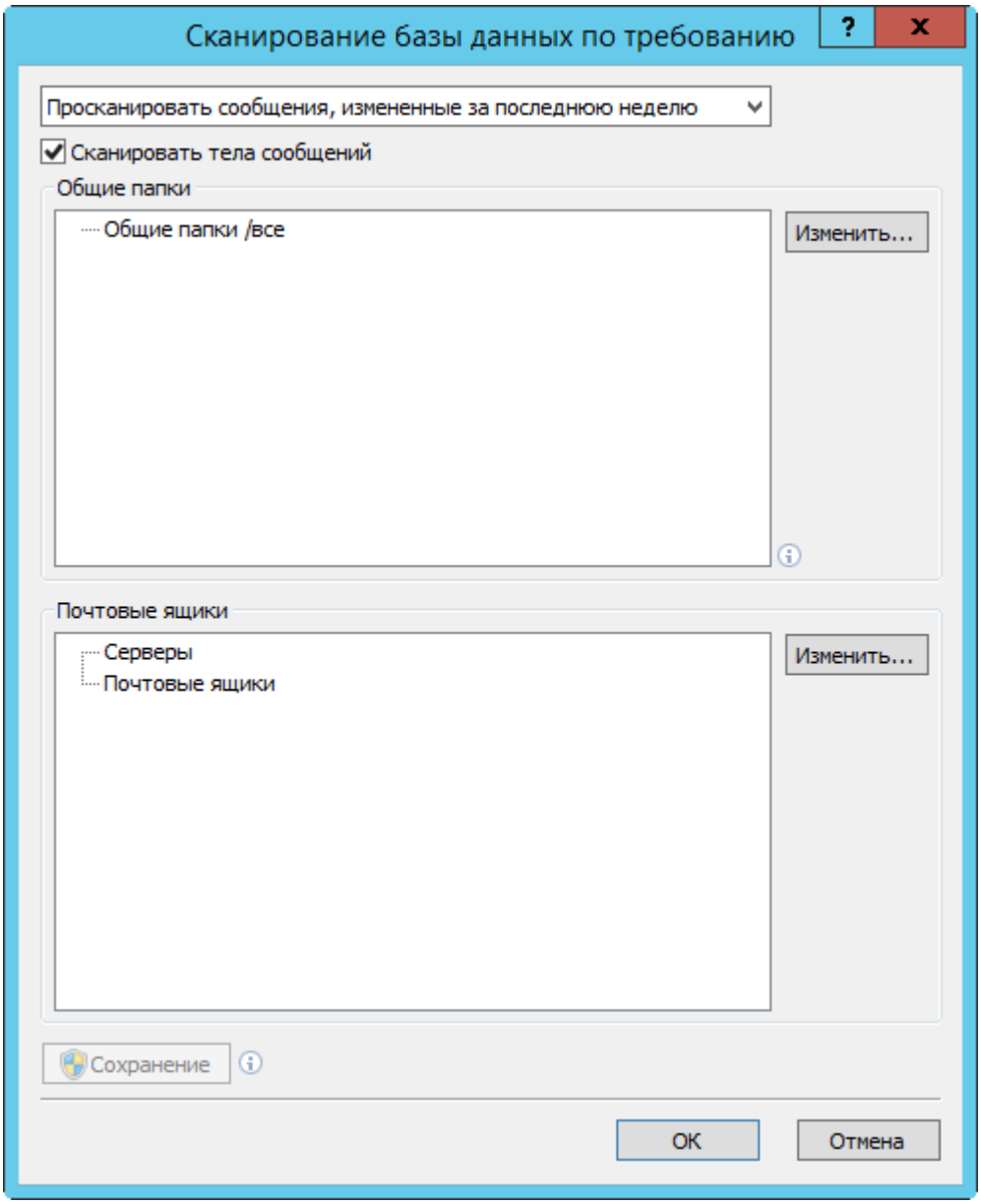
В общих папках и пользовательских почтовых ящиках сканируются такие типы элементов:

- электронная почта,
- публикации,
- элементы календаря (встречи и визиты),
- задачи,
- контакты,
- журнал.

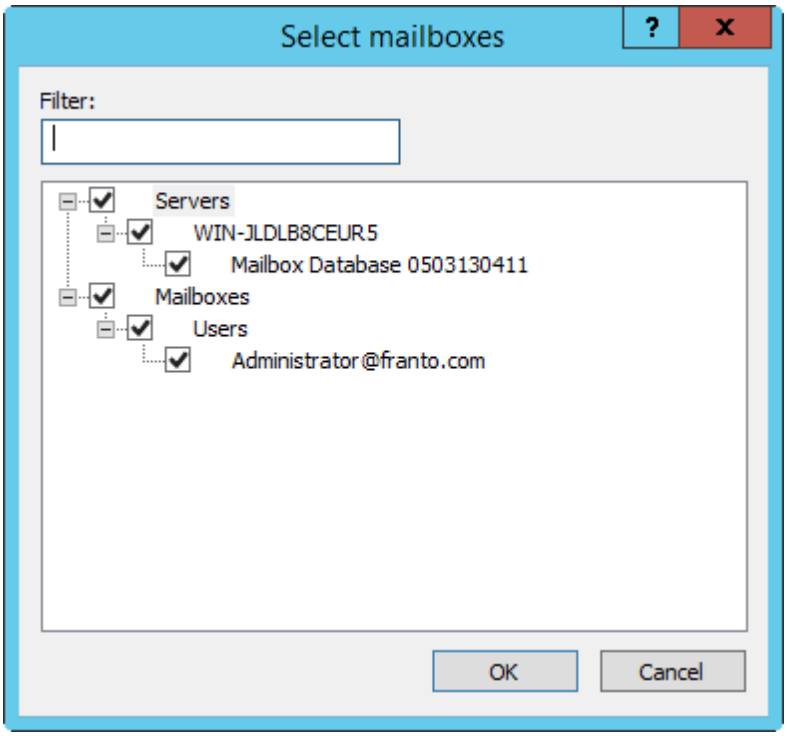
В раскрывающемся списке можно выбрать сканируемые сообщения на основании их метки времени. Например, сообщения, измененные за последнюю неделю. Если нужно, вы можете просканировать все сообщения.

Чтобы включить или отключить сканирование тел сообщений, установите или снимите флажок **Сканировать тела сообщений**.

Чтобы выбрать общую папку, которую нужно просканировать, щелкните **Изменить**.



Установите флажки возле баз данных и почтовых ящиков сервера, которые нужно просканировать. **Фильтр** дает возможность быстро находить базы данных и почтовые ящики, особенно если в вашей инфраструктуре Exchange много почтовых ящиков.



Чтобы сохранить выбранные объекты сканирования и заданные параметры в профиль сканирования по требованию, нажмите кнопку **Сохранить**.

1.4 Типы защиты

Существует три типа защиты.

- Защита от вирусов
- Защита от спама
- Применение пользовательских правил

1.4.1 Защита от вирусов

Защита от вирусов — одна из основных функций программного продукта ESET Mail Security. Защита от вирусов предотвращает вредоносные атаки на компьютер путем контроля файлов, электронной почты и связи через Интернет. Если обнаруживается угроза, представляемая вредоносным кодом, модуль защиты от вирусов может устранить ее, сначала заблокировав, а затем очистив, удалив или поместив на карантин.

1.4.2 Защита от спама

Чтобы угрозы в электронной почте можно было обнаруживать максимально эффективно, в защите от спама совмещается целый ряд технологий («черные» списки реального времени, «черные» списки серверов на основе DNS, технология создания цифровых отпечатков, проверка репутации, анализ содержимого, фильтр Байеса, правила, работа с «белыми» и «черными» списками вручную и т. д.). Модуль сканирования защиты от спама формирует значение вероятности для каждого просканированного сообщения электронной почты в процентах (от 0 до 100).

Решение ESET Mail Security может фильтровать спам также с помощью метода работы с «серыми» списками (отключены по умолчанию). Данный метод основан на спецификации RFC 821, согласно которой, поскольку SMTP считается ненадежным транспортным протоколом, каждый агент передачи сообщений должен повторно пытаться доставить сообщение после временного сбоя доставки. Многие нежелательные сообщения однократно отправляются на адреса, которые содержит автоматически созданный список адресов

электронной почты. При работе с «серыми» списками вычисляется контрольное значение (хэш) для адреса отправителя конверта, адреса получателя конверта и IP-адреса отправляющего агента передачи сообщений. Если сервер не может найти контрольное значение для этих трех параметров в собственной базе данных, он отказывается принимать сообщение и возвращает код временного отказа (например, 451). Нормальный сервер попытается повторно доставить сообщение через некоторое время. Контрольное значение для этих трех параметров будет храниться в базе данных проверенных подключений после второй попытки, благодаря чему впоследствии любое сообщение с соответствующими характеристиками будет доставляться.

1.4.3 Применение пользовательских правил

Защита на основе пользовательских правил применяется для сканирования и с помощью VSAPI, и с помощью агента транспорта. Интерфейс пользователя ESET Mail Security позволяет создавать отдельные правила, которые также можно использовать совместно. Если в одном правиле используется несколько условий, такие условия будут объединены логическим оператором AND. Впоследствии правило будет выполняться только тогда, когда выполняются все условия. Если создано несколько правил, будет применен логический оператор OR, то есть программа будет выполнять первое правило, для которого соблюдены все условия.

В последовательности действий по сканированию в качестве первого метода используется работа с «серыми» списками (при условии, что она включена). На последующих этапах всегда будут выполняться следующие методы: защита на основе пользовательских правил, затем сканирование модулем защиты от вирусов и, наконец, сканирование модулем защиты от спама.

1.5 Интерфейс пользователя

ESET Mail Security имеет графический интерфейс пользователя, задача которого заключается в том, чтобы быть настолько интуитивно понятным, насколько возможно. Графический интерфейс пользователя дает возможность быстро и просто использовать основные функции программы.

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

В окне расширенных параметров можно конфигурировать параметры в соответствии со своими потребностями. В меню слева можно выбрать следующие категории: **Сервер**, **Компьютер**, **Обновление**, **Интернет и электронная почта**, **Контроль устройств**, **Сервис** и **Интерфейс пользователя**. Некоторые из основных категорий содержат подкатегории. Если щелкнуть элемент (категорию или подкатегорию) в меню слева, параметры, соответствующие этому элементу, отображаются на правой панели.

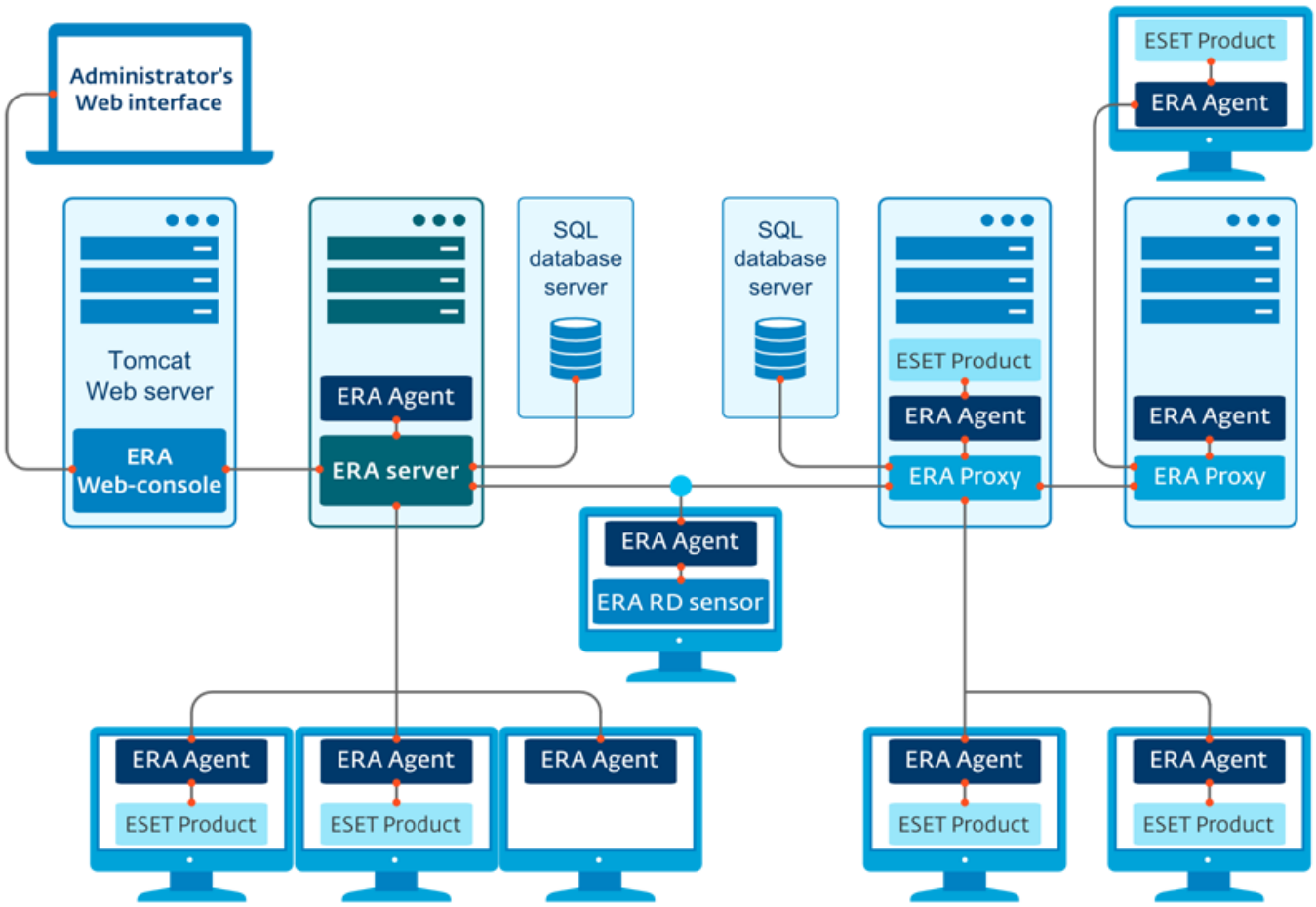
Дополнительные сведения о графическом интерфейсе см. здесь.

1.6 Управление через ESET Remote Administrator

ESET Remote Administrator (ERA) — это приложение, позволяющее централизованно управлять 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. В сети могут сосуществовать операционные системы Microsoft, Linux и OS X, а также системы, работающие на мобильных устройствах (мобильных телефонах и планшетах).

На рисунке ниже представлен пример архитектуры сети, защищенной решениями ESET, которыми управляет сервер ERA.



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

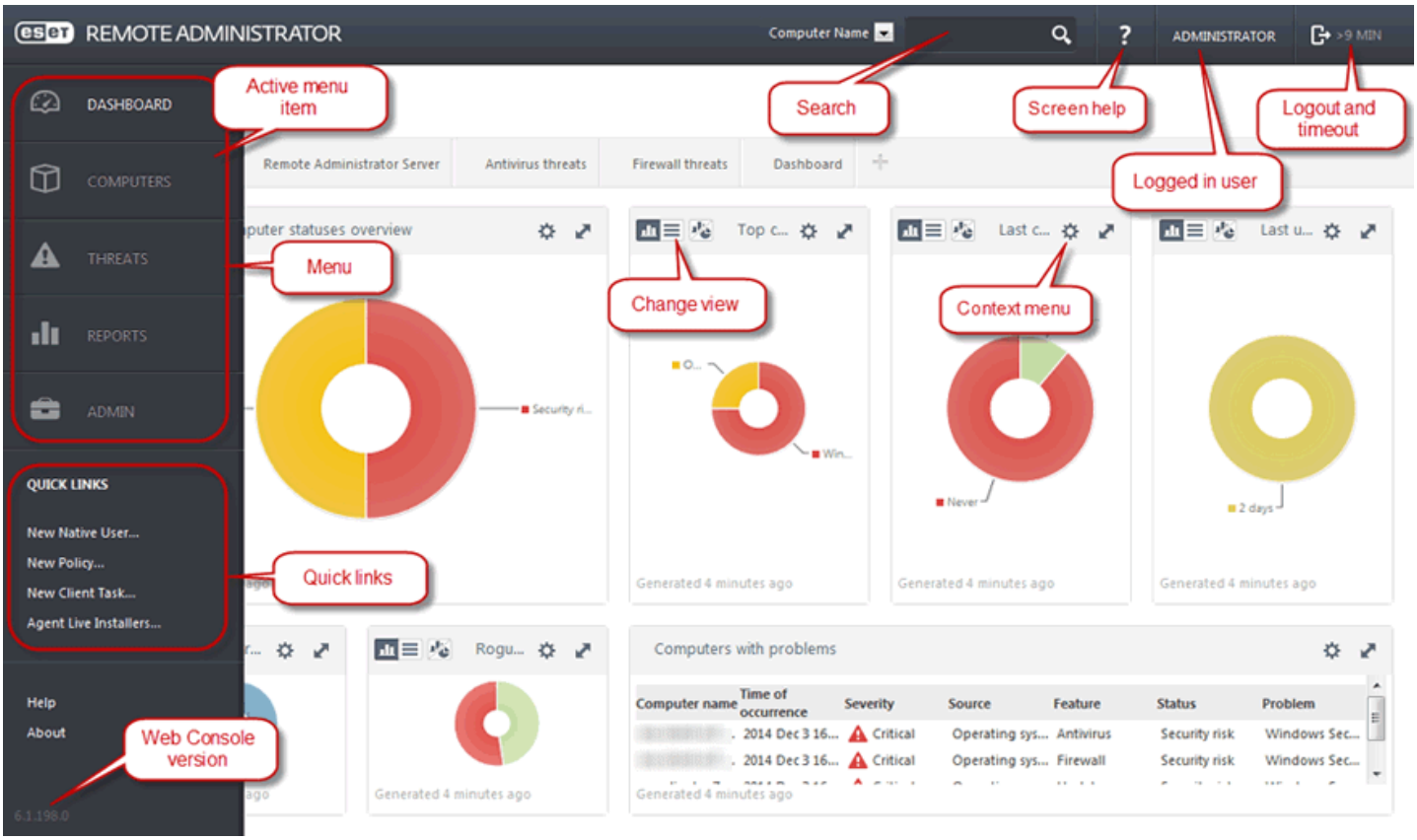
1.6.1 Сервер ERA

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

1.6.2 Веб-консоль

Веб-консоль ERA — это приложение с веб-интерфейсом, которое отображает данные, полученные с сервера ERA, и позволяет управлять решениями ESET, 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 необходимо открыть доступ к веб-серверу через Интернет, вы можете воспользоваться всеми преимуществами ESET Remote Administrator практически из любого места и с любого устройства, подключенного к Интернету.

Вот так выглядит панель мониторинга веб-консоли.



На верхней панели веб-консоли находится инструмент **Быстрый поиск**. Чтобы выполнить поиск, в раскрывающемся меню выберите пункт **Имя компьютера**, **IPv4-** или **IPv6-адрес** или **Имя угрозы**, введите поисковую фразу в текстовом поле и щелкните значок лупы или нажмите клавишу **ВВОД**. Вы будете перенаправлены в раздел групп, где будет отображен результат поиска: имя клиента или список клиентов. Управление всеми клиентами осуществляется через веб-консоль. Вы можете войти в веб-консоль, используя популярные устройства и браузеры.

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

1.6.3 Агент

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

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

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

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

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

ПРИМЕЧАНИЕ. Прокси-сервер ESET имеет собственный агент, отвечающий за обмен данными с клиентами, другими прокси-серверами и сервером.

1.6.4 RD Sensor

RD (Rogue Detection) Sensor — это инструмент поиска компьютеров в сети. Инструмент RD Sensor является частью ESET Remote Administrator и предназначен для обнаружения компьютеров в сети. Он позволяет быстро и автоматически добавлять новые компьютеры в ESET Remote Administrator. Каждый найденный в сети компьютер отображается в веб-консоли. После этого с отдельными клиентскими компьютерами можно выполнять дальнейшие действия.

RD Sensor прослушивает сеть, обнаруживает находящиеся в ней компьютеры и направляет информацию о них серверу ERA. Затем сервер ERA Server проверяет, являются ли обнаруженные ПК неизвестными для сервера ERA Server или уже управляемыми.

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

1.6.5 Прокси-сервер

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

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

Для правильной работы прокси-сервера ERA на главном компьютере, на который вы устанавливаете прокси-сервер ERA, должен быть установлен агент ESET, а сам компьютер подключен к верхнему уровню сети (серверу ERA или прокси-серверу ERA верхнего уровня, если такой имеется).

ПРИМЕЧАНИЕ. Примеры сценариев развертывания прокси-сервера ERA см. в справке о ESET Remote Administrator в Интернете.

2. Системные требования

Поддерживаемые операционные системы

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

ПРИМЕЧАНИЕ. Самая ранняя поддерживаемая ОС — это Microsoft Windows Server 2003 с пакетом обновления 2.

Поддерживаемые версии Microsoft Exchange Server

- Microsoft Exchange Server 2003 с пакетом обновления SP1, SP2
- Microsoft Exchange Server 2007 с пакетом обновления SP1, SP2, SP3
- Microsoft Exchange Server 2010 с пакетом обновления SP1, SP2, SP3
- Microsoft Exchange Server 2013 с накопительными пакетами обновления 2, 3, 4 (SP1), 5, 6, 7, 8
- Microsoft Exchange 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.

3. Установка

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

Обратите внимание, что установочный файл необходимо запускать с помощью встроенной учетной записи администратора. 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.

Запустить установочный файл можно двумя способами.

- Войти локально с помощью учетной записи администратора и запустить установочный файл.
- Можно выполнить вход от имени другого пользователя, однако необходимо открыть командную строку с помощью пункта «Запустить от имени...» и ввести учетные данные администратора, чтобы командная строка выполнялась от имени администратора. Затем нужно ввести команду, чтобы запустить установочный файл (например, msiexec /i emsx_nt64_ENU.msi но необходимо заменить emsx_nt64_ENU.msi на точное имя 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.

Полная
Рекомендуется выбирать этот тип установки. Будут установлены все функции программы ESET Mail Security. Выбрав этот тип установки, нужно будет указать только папку, в которую следует установить продукт. Можно просто оставить установочные папки, указанные по умолчанию (рекомендуется). Затем все функции программы будут установлены автоматически.

Выборочная
Выборочный тип установки позволяет выбирать функции программы ESET Mail Security, которые будут установлены на вашу систему. Отобразится стандартный список функций и компонентов, которые можно выбрать для установки.

Кроме использования мастера установки, в командной строке можно выбрать автоматическую установку программы ESET Mail Security. Этот тип установки не требует взаимодействия с пользователем, как при использовании описанного выше мастера. Эта возможность полезна, например, для автоматизации или упрощения процесса установки. Данный тип установки также называется «установка без участия пользователя», поскольку в процессе не отображаются запросы для выполнения каких-либо действий.

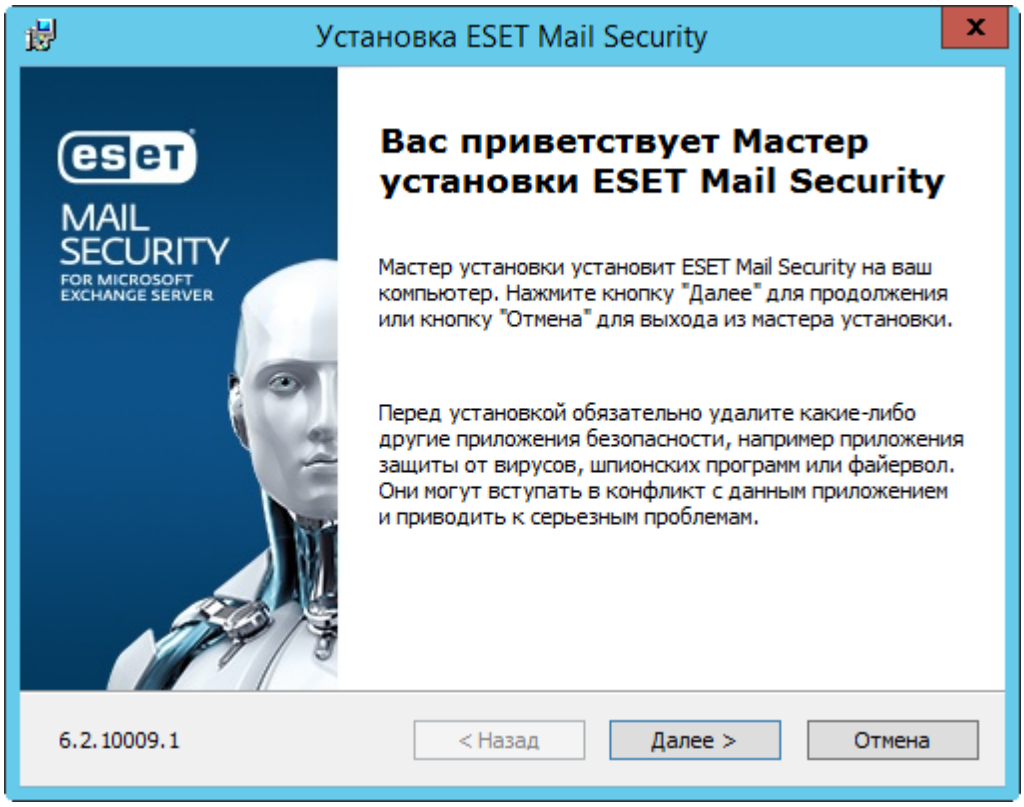
Автоматическая установка/установка без участия пользователя
Выполните установку с помощью командной строки: `msiexec /i <имя_пакета> /qn /l*xv msi.log`

ПРИМЕЧАНИЕ. Настоятельно рекомендуется устанавливать ESET Mail Security в только что установленной и сконфигурированной операционной системе, если это возможно. Однако если необходимо установить программный продукт на существующей системе, лучше всего удалить предыдущую версию ESET Mail Security, перезапустить сервер и после этого установить новую версию ESET Mail Security.

ПРИМЕЧАНИЕ. Если на вашем компьютере ранее использовалось стороннее антивирусное ПО, рекомендуется полностью удалить его, прежде чем устанавливать ESET Mail Security. Для этого можно использовать средство ESET AV Removal, которое упрощает процесс удаления.

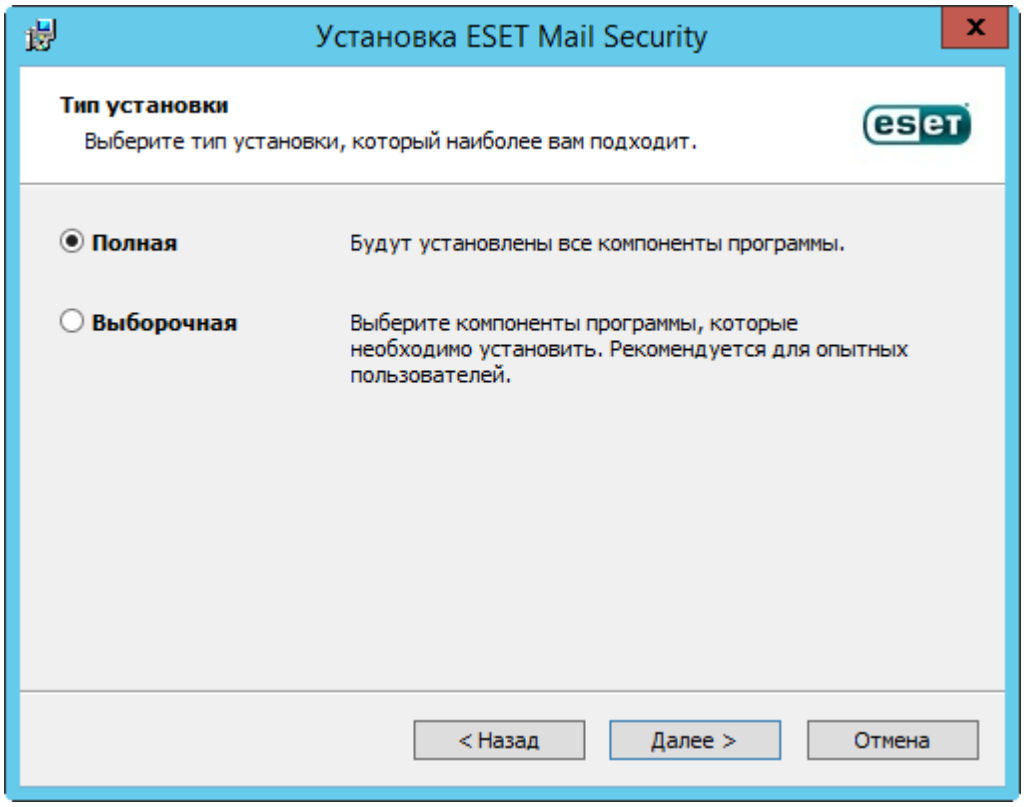
3.1 Этапы установки программы ESET Mail Security

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



Приняв условия лицензионного соглашения, выберите один из следующих типов установки:

- **Полная**: установка всех функций ESET Mail Security. Рекомендуется выбирать этот тип установки.
- **Выборочная**: можно выбрать, какие функции ESET Mail Security будут установлены.



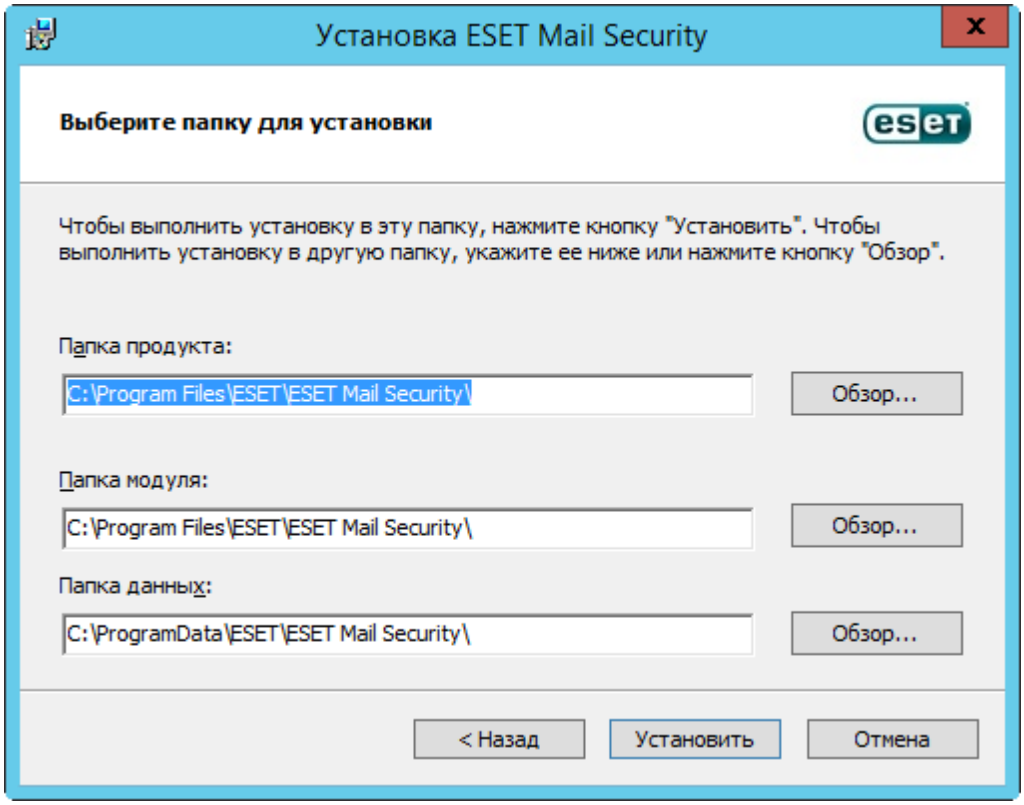
Полная установка

Этот способ также называют установкой всех компонентов. Он предусматривает установку всех компонентов

программы ESET Mail Security. Вам будет предложено выбрать расположение, в которое нужно установить ESET Mail Security. По умолчанию программа устанавливается в папку C:\Program Files\ESET\ESET Mail Security. Нажмите кнопку **Обзор**, чтобы изменить папку (не рекомендуется).

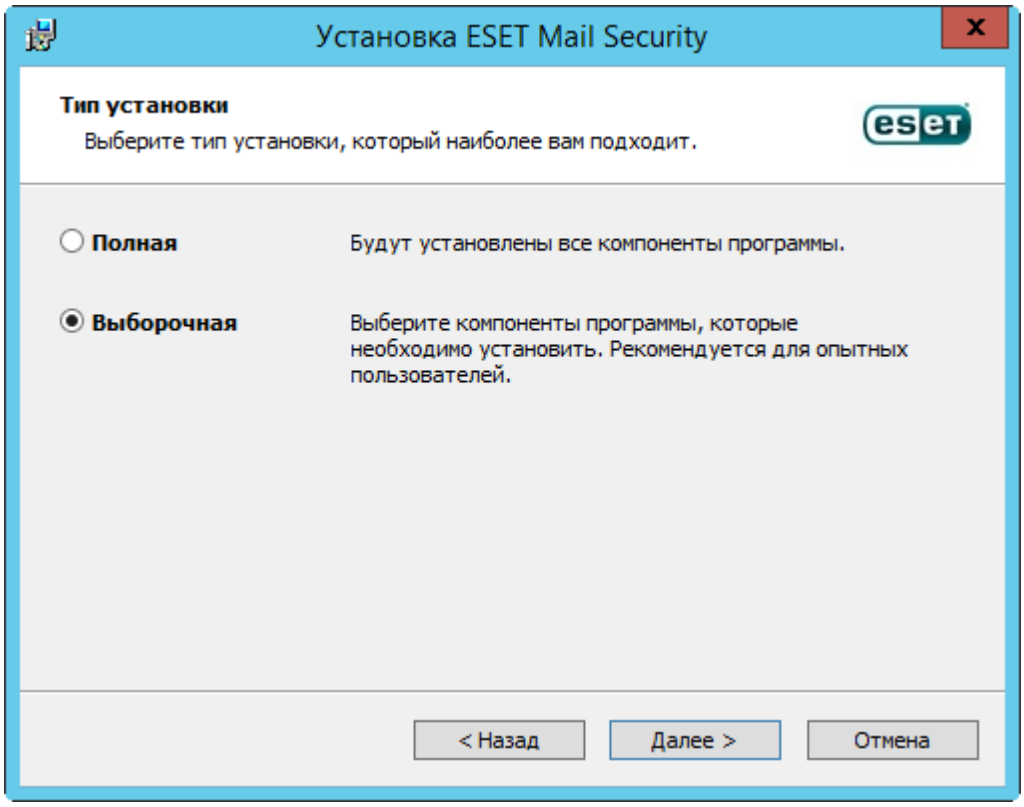
ПРИМЕЧАНИЕ. В ОС Windows Server 2008 и Windows Server 2008 R2 установка компонента **Интернет и электронная почта** отключена по умолчанию. Если нужно установить этот компонент, выберите тип установки **Выборочная**.

ПРИМЕЧАНИЕ. Если вы планируете использовать локальный карантин для сообщений электронной почты и не хотите, чтобы помещенные в карантин сообщения хранились на диске `C:`, измените путь в поле **Папка данных**, указав нужные вам диск и расположение. При этом следует принять во внимание, что в этом расположении будут храниться все файлы данных ESET Mail Security.



Выборочная установка

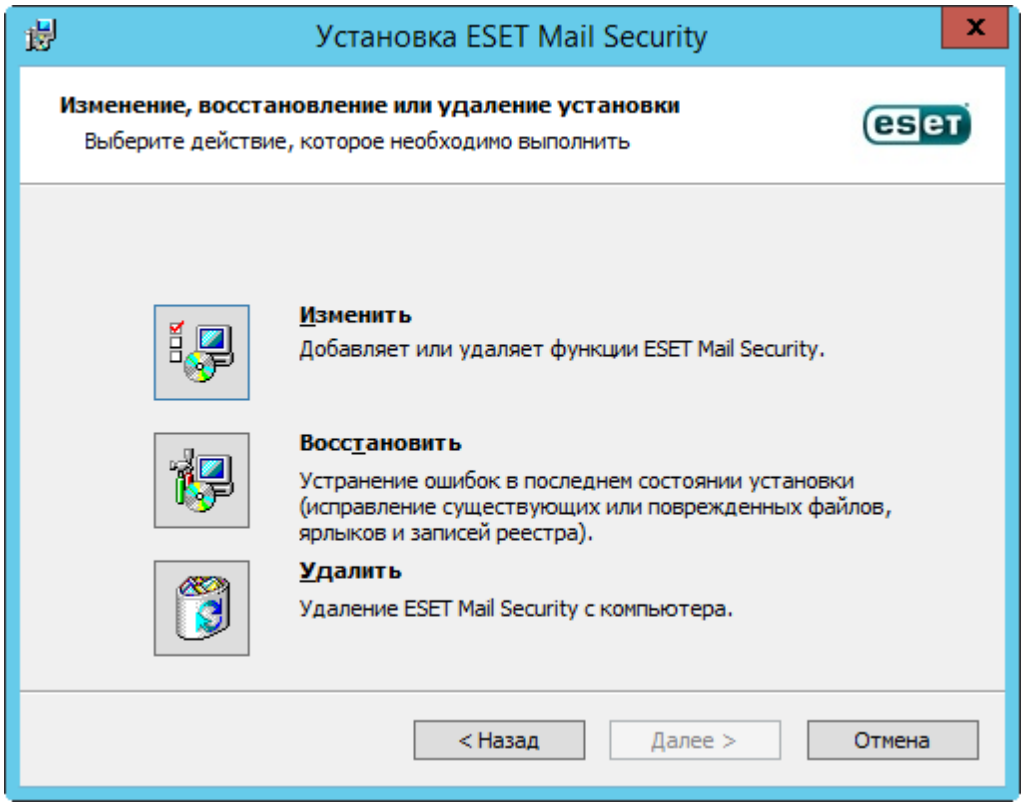
В этом типе можно выбрать, какие функции необходимо установить. Эта возможность полезна, если необходимо установить только те компоненты программы ESET Mail Security, которые нужны.



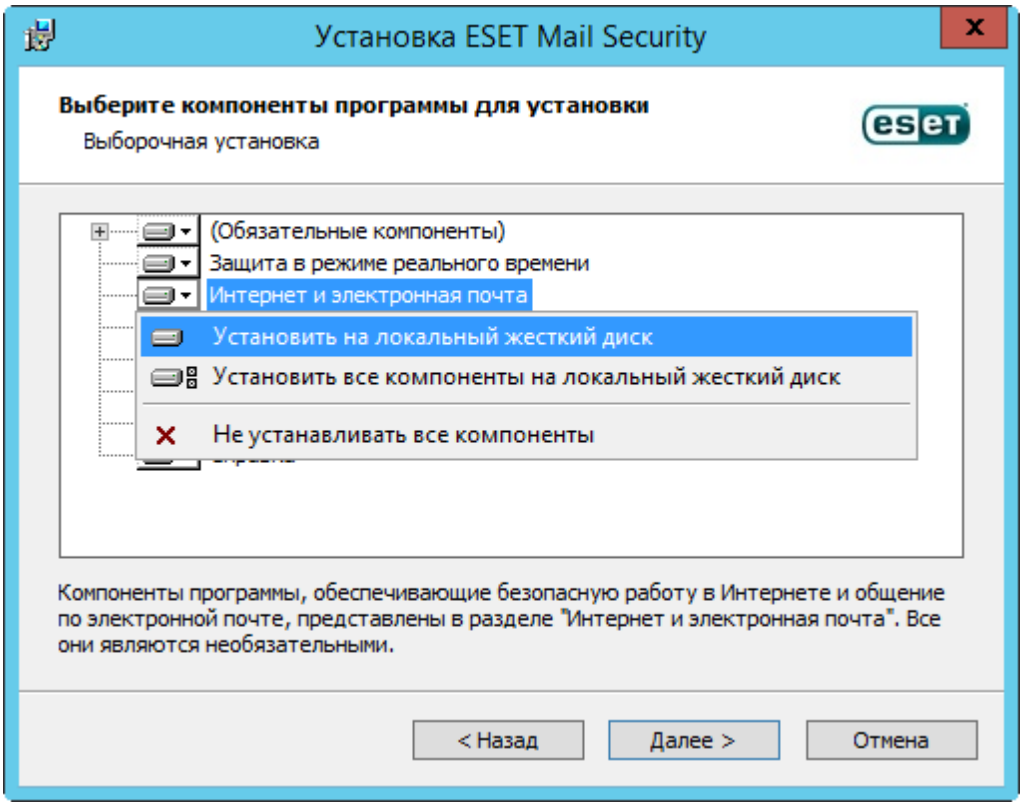
Можно добавлять и удалять компоненты программы. Для этого нужно запустить установочный файл с расширением .msi, который использовался при первой установке, или перейти в раздел **Программы и компоненты** (доступен на панели управления Windows), щелкнуть ESET Mail Security правой кнопкой мыши и выбрать **Изменить**. Чтобы добавлять или удалять компоненты, выполняйте описанные далее действия.

Изменение компонентов (добавление или удаление), восстановление и удаление

Доступны три перечисленных ниже варианта. Можно **изменить** установленные компоненты, **восстановить** установленную программу ESET Mail Security или **удалить** ее полностью.



При выборе команды **Изменить** отобразится список 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. Изменять установленные компоненты можно в любое время. Для этого нужно запустить установщик. Для изменения большинства компонентов перезапуск сервера не требуется. Будет выполнен перезапуск графического интерфейса пользователя, после чего отобразятся только те компоненты, которые были указаны для установки. Если для некоторых компонентов требуется перезагрузка сервера, установщик Windows отобразит соответствующий запрос. Новые компоненты станут доступны, когда сервер снова появится в сети.

3.1.1 Установка из командной строки

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

Поддерживаемые параметры:

APPDIR=<путь>
- Путь — действительный путь к каталогу.
- Каталог установки приложения.
- Например, `emsx_nt64_ENU.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

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

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

ADDLOCAL=<список>

- Установка компонентов — список необязательных функций, которые нужно установить локально.
- Использование с пакетами формата MSI компании ESET: `emsx_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 список (разделители — запятые) имен всех функций, которые нужно установить.
- При выборе функции, которую нужно установить, в список нужно добавить весь путь (указать все родительские функции).
- Чтобы все делать верно, см. дополнительные правила.

Наличие функции

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

Дерево функций выглядит следующим образом:

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

Дополнительные правила

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

нужно явным образом добавить в список невидимую функцию Почтовые модули**.**

Примеры

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

```
efsw_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,EmailClientProtection,Antispam,MailPlugins
```

Список свойств CFG_:

CFG_POTENTIALLYUNWANTED_ENABLED=1/0
• 0 — отключено, 1 — включено.
• ПНП.

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

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

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

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

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

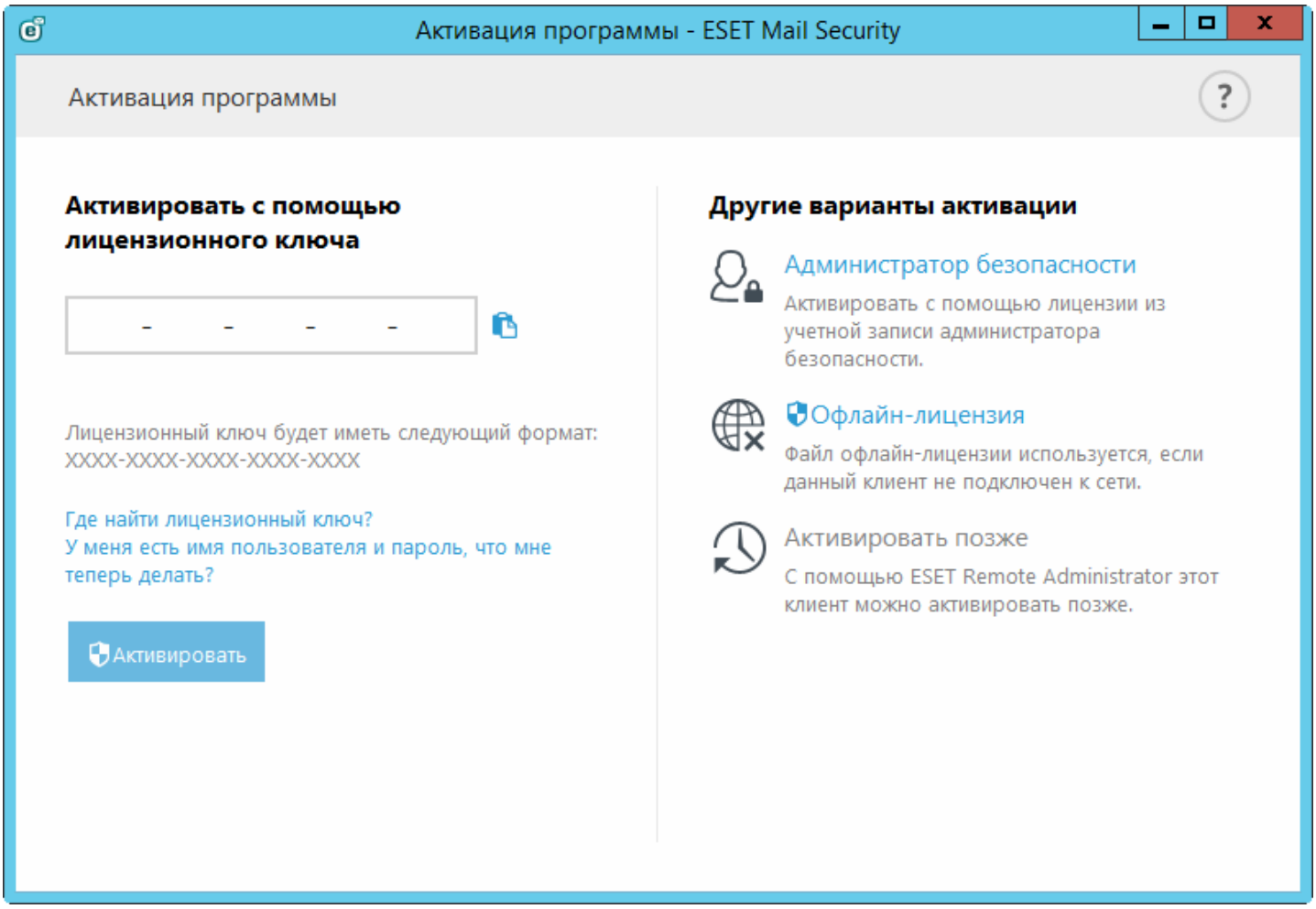
CFG_PROXY_PORT=<порт>
• Номер порта прокси-сервера.

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

CFG_PROXY_PASSWORD=<пароль>
• Пароль для проверки подлинности.

3.2 Активация программы

По завершении установки вам будет предложено активировать установленный продукт.



Выберите доступный метод активации ESET Mail Security. Дополнительные сведения см. в разделе Активация ESET Mail Security.

После активации ESET Mail Security на странице Мониторинг откроется главное окно программы, в котором отобразится ваше текущее состояние.

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, будут решены, состояние мониторинга станет зеленым, и для него отобразится значение «**Максимальная защита**».

3.3 Сервер терминалов

Если программное обеспечение ESET Mail Security устанавливается на сервере Windows Server, который выступает в качестве сервера терминалов, полезно будет отключить графический интерфейс пользователя ESET Mail 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.

3.4 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.

3.5 Обновление до новой версии

Новые версии ESET Mail Security выпускаются для реализации улучшений или исправления проблем, которые не могут быть устранены автоматическим обновлением модулей программы. Можно обновить старые версии программы ESET Mail Security (4.5 и более давние), несмотря на то что обновление приведет к кардинальному изменению архитектуры. Вы можете выполнить обновление до новой версии:

- Вручную путем загрузки и установки новой версии поверх используемой. Для этого необходимо просто запустить программу установки и выполнить установку привычным способом, при этом ESET Mail Security автоматически перенесет существующую конфигурацию с некоторыми исключениями (см. примечание ниже).

ВНИМАНИЕ! В процессе обновления имеются некоторые исключения: не все ваши параметры сохраняются, в частности, это касается правил. Это происходит, потому что в версии ESET Mail Security 6 функция правил полностью изменена и работает по-другому. Правила, которые использовались в предыдущих версиях ESET Mail Security, не совместимы с правилами, используемыми в версии ESET Mail Security 6. Рекомендуется настроить правила вручную — это будет полезно.

Далее перечислены параметры, которые сохраняются и переносятся из предыдущих версий ESET Mail Security.

- Общая конфигурация ESET Mail Security.
- Параметры защиты от спама:
  - все параметры, оставшиеся неизменными по сравнению с прошлыми версиями, а также любые новые параметры используют настройки по умолчанию;
  - белые и черные списки.

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

3.6 Роли сервера Exchange Server (пограничный сервер или сервер-концентратор)

Как на сервере пограничного транспорта, так и на транспортном сервере-концентраторе функции защиты от спама отключены по умолчанию. Именно такая конфигурация и нужна в организации Exchange с пограничным транспортным сервером. Рекомендуется, чтобы на пограничном транспортном сервере была запущена защита от спама ESET Mail Security для фильтрации сообщений перед их маршрутизацией в организацию Exchange.

Рекомендуется использовать пограничный сервер с целью сканирования на наличие спама, поскольку за счет этого программа ESET Mail Security может отклонять спам на раннем этапе процесса, не создавая лишней нагрузки на сетевые слои. Благодаря использованию этой конфигурации ESET Mail Security выполняет фильтрацию входящих сообщений на пограничном транспортном сервере, обеспечивая возможность для их безопасного перемещения на транспортный сервер-концентратор без дальнейшей фильтрации.

Если в вашей организации используется только транспортный сервер-концентратор без пограничного транспортного сервера, рекомендуется включить функции защиты от спама на транспортном сервере-концентраторе, который получает входящие сообщения из Интернета по протоколу SMTP.

3.7 Роли сервера Exchange Server 2013

Архитектура версии Exchange Server 2013 отличается от предыдущих версий Microsoft Exchange. В накопительном пакете обновления 4 для Exchange 2013 (который фактически является пакетом обновления 1 (SP1) для Exchange 2013) введена роль пограничного транспортного сервера.

Если вы планируете обеспечить защиту Microsoft Exchange 2013 с помощью программы ESET Mail Security, необходимо установить ESET Mail Security в системе, в которой сервер Microsoft Exchange 2013 имеет роль сервера почтовых ящиков или пограничного транспортного сервера.

Это не касается случаев, когда нужно установить ESET Mail Security на сервер Windows SBS (Small Business Server) или когда решение Microsoft Exchange 2013 имеет несколько ролей на одном сервере. В таких случаях все роли Exchange функционируют на одном и том же сервере, что позволяет программе ESET Mail Security обеспечить полную защиту, в том числе защиту почтовых серверов.

Если установить программу ESET Mail Security в системе, в которой активирована только роль сервера клиентского доступа (выделенный сервер клиентского доступа), самые важные функции ESET Mail Security, особенно функции почтового сервера, будут отключены. Функционировать будет только защита файловой системы в режиме реального времени и некоторые компоненты, относящиеся к защите компьютера. Почтовые серверы не будут защищены. Поэтому не рекомендуется устанавливать ESET Mail Security на сервере с ролью сервера клиентского доступа. Как указано выше, это не относится к Windows SBS (Small Business Server) и к решению Microsoft Exchange, имеющему несколько ролей на одном компьютере.

ПРИМЕЧАНИЕ.: Microsoft Exchange 2013 имеет некоторые технические ограничения, поэтому ESET Mail Security не поддерживает роль сервера клиентского доступа. Это не относится к решениям Windows SBS и Microsoft Exchange 2013, которые установлены на одном сервере со всеми серверными ролями. В этом случае ESET Mail Security с ролью сервера клиентского доступа можно запускать на сервере, так как почтовый сервер и пограничный транспортный сервер защищены.

3.8 Соединитель POP3 и защита от спама

Версии Microsoft Windows Small Business Server (SBS) содержат собственный встроенный соединитель POP3, который обеспечивает получение сервером сообщений электронной почты с внешних серверов POP3. В разных версиях SBS собственный соединитель Microsoft POP3 реализован по-разному.

ESET Mail Security поддерживает соединитель Microsoft SBS POP3, если он правильно настроен. Сообщения, загружаемые с помощью соединителя Microsoft POP3, сканируются на наличие спама. Для таких сообщений электронной почты защита от спама возможна, поскольку соединитель POP3 пересылает их из учетной записи POP3 на сервер Microsoft Exchange Server по протоколу SMTP.

Программа ESET Mail Security была протестирована с такими популярными почтовыми службами, как **Gmail.com**, **Outlook.com**, **Yahoo.com**, **Yandex.com** и **gmx.de**, в следующих системах SBS:

- Microsoft Windows Small Business Server 2003 R2
- Microsoft Windows Small Business Server 2008
- Microsoft Windows Small Business Server 2011

ВНИМАНИЕ! Если вы используете встроенный соединитель Microsoft SBS POP3 и все сообщения электронной почты сканируются на наличие спама, зайдите в раздел «Дополнительные настройки», последовательно выберите элементы **Сервер** > **Защита почтового транспорта** > Дополнительные параметры и для параметра **Сканировать также сообщения, полученные по проверенным или внутренним соединениям** выберите значение **Сканировать модулями защиты от вирусов и спама** из раскрывающегося списка. Это обеспечит защиту от спама для почтовых сообщений, полученных с учетных записей POP3.

Кроме того, можно использовать сторонние соединители POP3, например P3SS (вместо встроенного

соединителя Microsoft SBS POP3). Программа ESET Mail Security была протестирована в следующих системах (с использованием соединителя P3SS для получения сообщений из таких почтовых служб, как **Gmail.com**, **Outlook.com**, **Yahoo.com**, **Yandex.com** и **gmx.de**):

- Microsoft Windows Small Business Server 2003 R2
- Microsoft Windows Server 2008 с Exchange Server 2007
- Microsoft Windows Server 2008 R2 с Exchange Server 2010
- Microsoft Windows Server 2012 R2 с Exchange Server 2013

4. Руководство для начинающих

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

4.1 Интерфейс пользователя

Главное окно ESET Mail 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 Mail Security, действительности лицензии, последнем обновлении базы данных сигнатур вирусов, основные данные статистики 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. Также можно повторно запустить последнюю операцию сканирования.

Карантин почты: позволяет с легкостью управлять перемещенными на карантин сообщениями. Средство управления карантином почты используется для всех трех типов карантина: для локального карантина, карантина почтовых ящиков и карантина MS Exchange.

Обновление: отображение информации о базе данных сигнатур вирусов и оповещение о появлении доступных обновлений. Кроме того, в данном разделе можно выполнить активацию продукта.

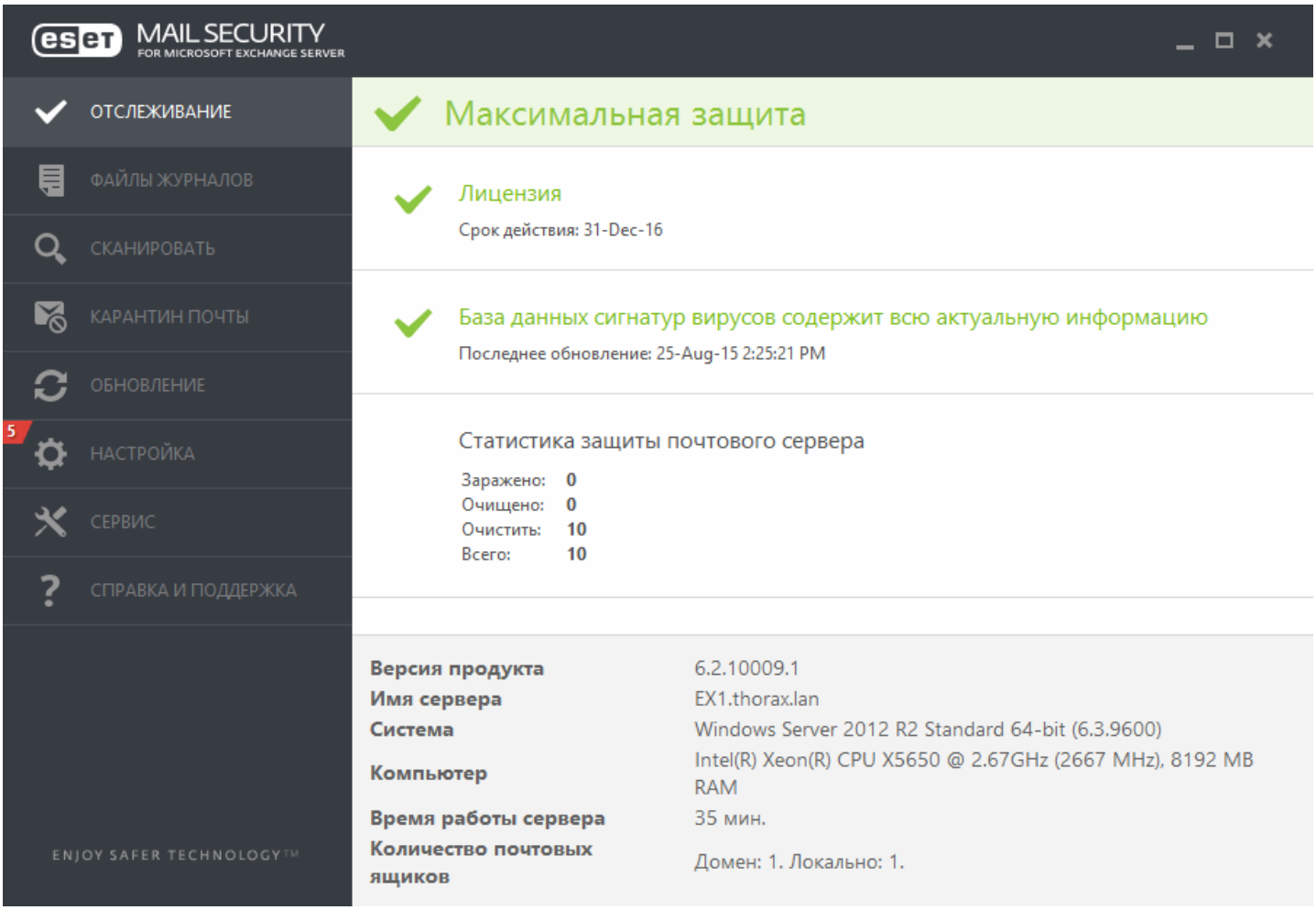
Настройки: этот параметр позволяет настроить параметры безопасности сервера и компьютера.

Сервис: дополнительная информация о компьютере и состоянии его защиты, а также сведения о программах, с помощью которых можно управлять безопасностью. Раздел «Сервис» содержит следующие подразделы: Запущенные процессы, Наблюдение, Сборщик журналов ESET, 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. Также доступны ссылки на форму запроса в службу поддержки клиентов и информацию об активации продукта.

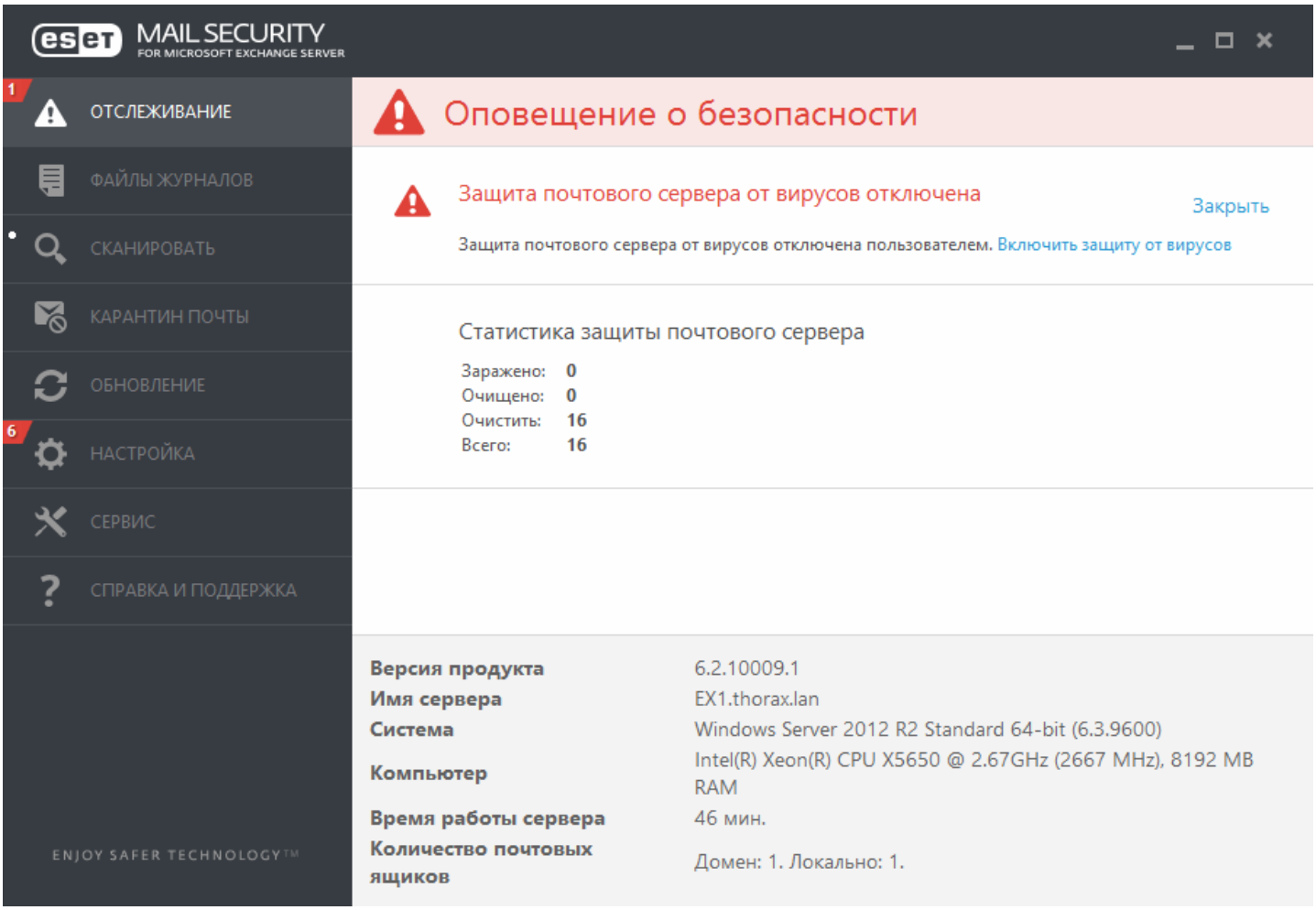
Окно **Состояние защиты** информирует пользователя о текущем уровне защиты компьютера. Зеленый значок **Максимальная защита** означает, что обеспечивается максимальная степень защиты.

В окне состояния также отображаются быстрые ссылки на часто используемые функции программы ESET Mail Security, а также информация о последнем обновлении.



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

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. Это состояние отображается в указанных ниже случаях.

- **Модули защиты от вирусов и шпионских программ отключены**: вы можете повторно включить защиту от вирусов и шпионских программ, выбрав команду **Включить защиту в режиме реального времени** на панели **Состояние защиты** или команду **Включить защиту от вирусов и шпионских программ** на панели**Настройки** в главном окне программы.
- Вы используете устаревшую базу данных сигнатур вирусов.
- Программный продукт не активирован.
- **Срок действия лицензии истек**: при возникновении этой проблемы значок состояния защиты становится красным. С этого момента программа больше не сможет выполнять обновления. Чтобы продлить лицензию, рекомендуется выполнить инструкции в окне предупреждения.

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

- **Защита доступа в Интернет отключена**: вы можете повторно включить защиту доступа в Интернет, щелкнув уведомление о защите и выбрав элемент **Включить защиту доступа в Интернет**.
- **Срок действия лицензии скоро закончится**: об этой проблеме свидетельствует появление восклицательного знака на значке состояния защиты. После окончания срока действия лицензии программа больше не сможет выполнять обновления, а значок состояния защиты станет красным.

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.

Чтобы просмотреть **Состояние защиты**, выберите верхний пункт в главном меню. В главном окне появится

сводная информация о работе ESET Mail Security и подменю с двумя пунктами: **Наблюдение** и **Статистика**. Для просмотра более подробных сведений о компьютере можно воспользоваться любым из этих пунктов.

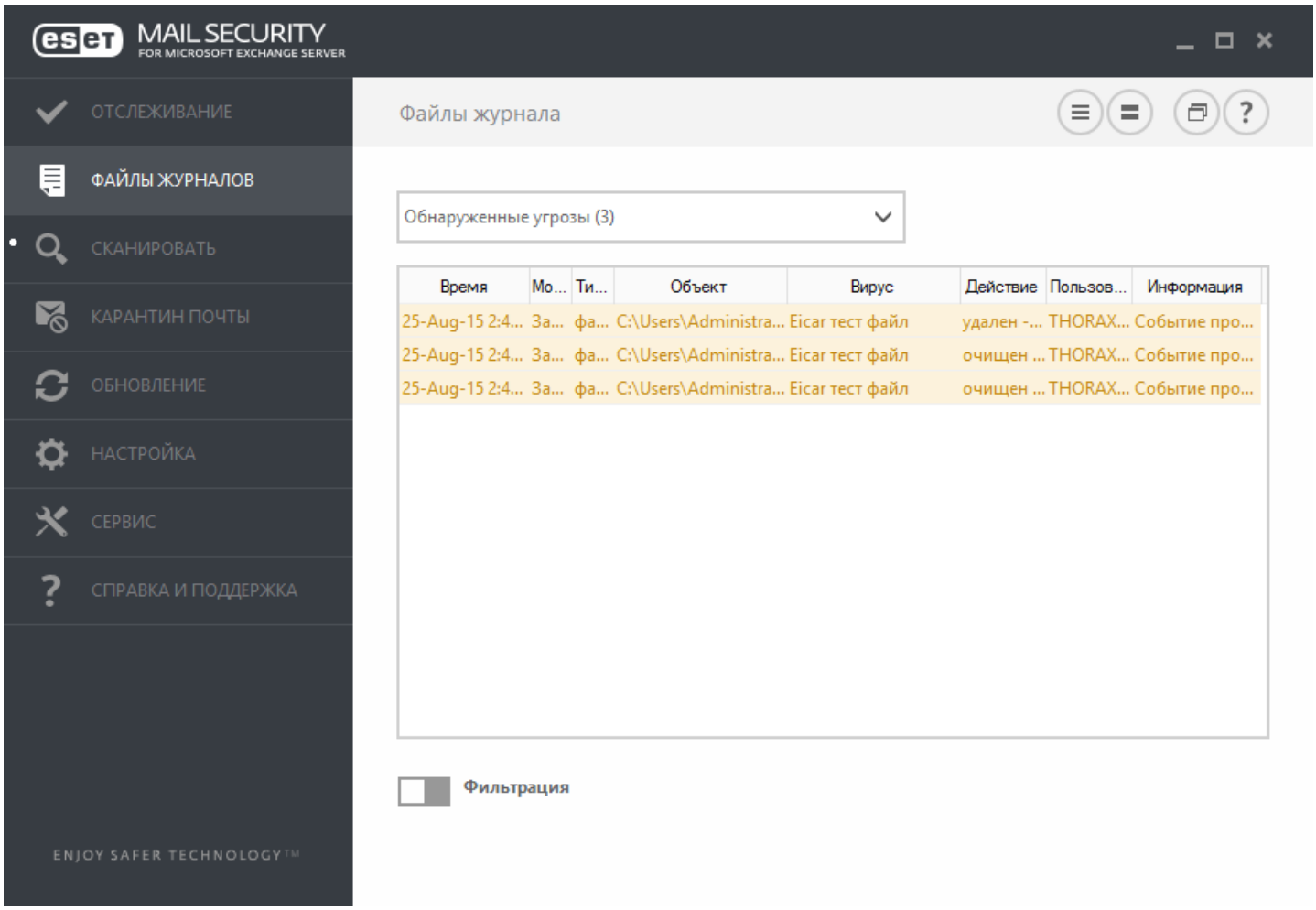
Когда функциональность ESET Mail Security используется полностью, **значок состояния защиты** обозначается зеленым цветом. Если требуется привлечь внимание пользователя, цвет значка меняется на оранжевый или красный.

Щелкните **Наблюдение**, чтобы просмотреть график действий файловой системы в режиме реального времени (горизонтальная ось). На вертикальной оси отображается объем считанных (синяя линия) и записанных (красная линия) данных.

В подменю **Статистика** содержатся сведения о количестве зараженных, очищенных и незараженных объектов по модулям. Доступные модули можно выбирать с помощью раскрывающегося списка.

4.2 Файлы журналов

Файлы журналов содержат информацию о важных программных событиях и сводные сведения об обнаруженных угрозах. Журналы являются важнейшим средством анализа системы, обнаружения угроз и устранения неполадок. Ведение журнала выполняется в фоновом режиме без вмешательства пользователя. Данные вносятся в журнал в соответствии с текущими параметрами его детализации. Просматривать текстовые сообщения и журналы можно непосредственно в среде ESET Mail Security или другом расположении, куда их нужно предварительно экспортировать.



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 Mail 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 Mail 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**: список 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 базы данных**: этот журнал содержит такие сведения, как версия базы данных сигнатур вирусов, дата, просканированное расположение, количество найденных угроз, количество совпадений по правилам, время завершения.
- **Защита почтового сервера**: все сообщения, классифицированные программой ESET Mail Security как спам или вероятный спам, регистрируются здесь. Эти журналы применяются для следующих типов защиты: защита от спама, правила и защита от вирусов.
- **Работа с «серыми» списками**: все сообщения, которые оценивались с применением метода работы с «серыми» списками, регистрируются в этом журнале.

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.

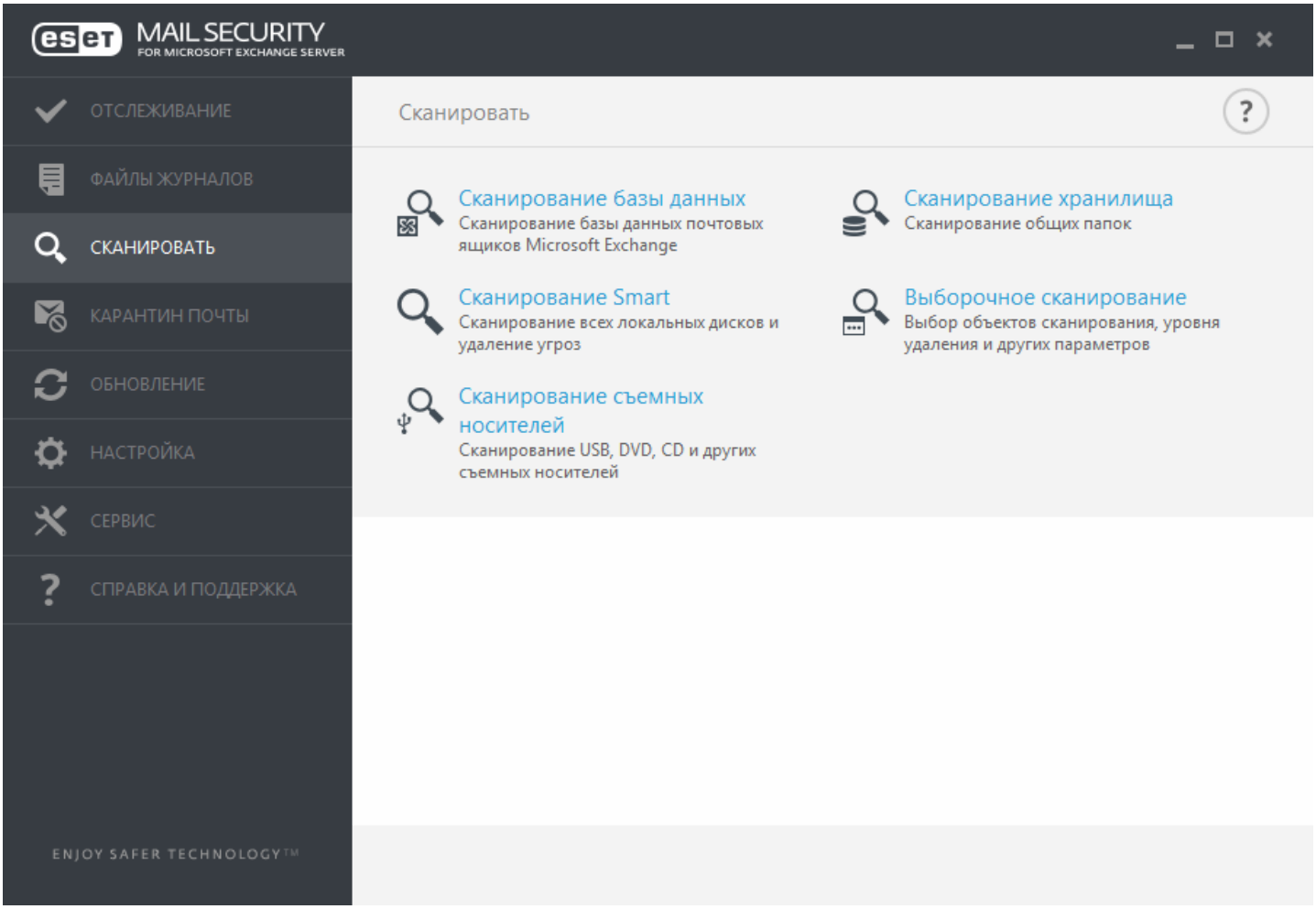
Щелкните переключатель  **Фильтрация**, чтобы открыть окно **Фильтрация журнала**, в котором можно задать критерии фильтрации.

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

- **Показать**: просмотр в новом окне более подробной информации о выбранном журнале (как и при двойном щелчке).
- **Фильтрация одинаковых записей**: активация фильтра журнала, который показывает только записи одного выбранного типа.
- **Фильтр...**: при выборе этого параметра на экран выводится окно Фильтрация журнала, в котором можно задать критерии фильтрации для определенных записей журнала.
- **Включить фильтр**: активация настроек фильтра. Критерии фильтрации нужно задать при первой фильтрации журналов. После настройки фильтров они остаются неизменными, если только не изменить их вручную.
- **Копировать**: копирование выделенных записей в буфер обмена.
- **Копировать все**: копирование 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 из выбранных записей в XML-файл.
- **Экспортировать все...** : экспорт всей информации в окне в XML-файл.
- **Найти...**: этот параметр открывает окно Поиск в журнале и позволяет определить критерии поиска. Используется для работы с уже отфильтрованным содержимым, чтобы сузить спектр результатов еще больше.
- **Найти далее**: поиск следующей записи, соответствующей предварительно заданным критериям (выше).
- **Найти ранее**: поиск предыдущей записи, соответствующей предварительно заданным критериям (выше).
- **Удалить диагностические записи**: удаление всех диагностических записей, отображенных в окне.
- **Прокрутить журнал**: установите этот флажок, чтобы выполнялась автоматическая прокрутка старых журналов, а на экран в окне **Файлы журналов** выводились активные журналы.

4.3 Сканирование

Модуль сканирования по требованию является важной частью ESET Mail Security. Он используется для сканирования файлов и папок на компьютере. С точки зрения обеспечения безопасности принципиально важно выполнять сканирование компьютера регулярно, а не только при возникновении подозрений. Рекомендуется выполнять регулярные (например, раз в месяц) операции детального сканирования системы на предмет обнаружения вирусов, которые не были обнаружены при помощи функции защиты файловой системы в реальном времени. Это может произойти, если в определенный момент защита файловой системы в реальном времени была отключена, база данных вирусов была устаревшей или при сохранении на диск файл не был распознан как вирус.



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 базы данных

Дает возможность выполнять сканирование базы данных по требованию. Вы можете выбрать для сканирования **общие папки, почтовые серверы и почтовые ящики**.

ПРИМЕЧАНИЕ. Если используется Microsoft Exchange Server 2007 или 2010, вы можете воспользоваться функциями Защита базы данных почтовых ящиков или Сканирование базы данных по требованию. При этом данные типы защиты не могут быть активными одновременно. Если выбрать сканирование базы данных по требованию, то в разделе Сервер дополнительных настроек необходимо отключить интеграцию защиты базы данных почтовых ящиков. В противном случае **сканирование базы данных по требованию** будет недоступно.

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 ESET Mail 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 тщательной 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**.

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

Выполнение любого последнего сканирования (сканирования хранилища, Smart, выборочного и т. д.) с такими же настройками.

ПРИМЕЧАНИЕ. Если используется сканирование базы данных по требованию, функция «Повторить последнее сканирование» недоступна.

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

4.3.1 Сканирование Hyper-V

Сканирование Hyper-V на наличие вирусов позволяет сканировать диски сервера Microsoft Hyper-V Server, то есть виртуальных машин (ВМ), без необходимости установки каких-либо агентов на соответствующих виртуальных машинах. Для установки модуля защиты от вирусов требуются права администратора сервера Hyper-V.

Сканирование Hyper-V выполняется на основе модуля сканирования компьютера по требованию, при этом некоторые функции не работают (сканирование загрузочного сектора (будет добавлено позже), сканирование оперативной памяти).

Поддерживаемые операционные системы сервера виртуальных машин

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

Требования к оборудованию

На сервере не должно возникать проблем с производительностью из-за работы виртуальных машин. В процессе сканирования задействованы в основном только ресурсы процессора.
В случае сканирования подключенной к Интернету виртуальной машины требуется наличие свободного места на диске. Объем свободного (доступного для использования) 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 динамически 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 Mail Security не поддерживает работу системы Hyper-V на сервере в кластере.
- Виртуальные машины на сервере 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 параметров ThreatSense.

ПРИМЕЧАНИЕ. Решение ESET Mail Security поддерживает сканирование основной загрузочной записи виртуального диска, однако это сканирование выполняется в режиме только для чтения. Сканирование основной загрузочной записи выполняется по умолчанию. 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

Решение ESET Mail Security использует управление Hyper-V для обнаружения виртуальных дисков виртуальных машин и для подключения к ним. Таким образом решение ESET Mail Security имеет доступ к содержимому виртуальных дисков в той же мере, что и к содержимому любого обычного диска.

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

Решение ESET Mail Security использует управление Hyper-V для обнаружения виртуальных дисков виртуальных машин. Подключение к этим дискам невозможно. Поэтому решение ESET Mail Security создает контрольную точку/моментальный снимок виртуальной машины, а затем подключается к ней. После сканирования контрольная точка или моментальный снимок удаляется. Это означает, что можно выполнить лишь сканирование только для чтения, так как находящаяся в сети виртуальная машина остается незатронутой. Этот параметр полезен, если нужен только обзор зараженных файлов на запущенных виртуальных машинах и сведения об этих заражениях (если они вообще есть).

Создание снимка/точки выполняется медленно, и на это может потребоваться от нескольких секунд до

минуты. Примите это к сведению, если планируете выполнить сканирование Hyper-V на многих виртуальных машинах.

Принципы именования

Модуль сканирования Hyper-V использует следующие принципы именования:
`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: если щелкнуть пункт «Сканирование Hyper-V» в меню ESET Mail Security, вы увидите список доступных виртуальных машин (если таковые имеются), подлежащих сканированию. Этот список имеет структуру дерева, в которой подлежащий сканированию объект самого нижнего уровня — это том. Это значит, что для сканирования невозможно выбрать каталог или файл. Данный вариант предполагает сканирование по крайней мере одного тома целиком.
  Чтобы отобразить список доступных томов, необходимо подключиться к конкретным виртуальным дискам, и это может занять несколько секунд. Поэтому будет быстрее, если отметить подлежащую сканированию виртуальную машину или ее диски.
  Отметив подлежащие сканированию виртуальные машины, диски или тома, нажмите кнопку «Сканировать».
- С помощью планировщика.
- С помощью ERA в качестве клиентской задачи под названием «Сканирование сервера». Элементом самого нижнего уровня, подлежащим сканированию, является диск виртуальной машины.

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

По завершении сканирования отобразится соответствующее оповещение, содержащее ссылку «Показать журнал», с помощью которой вы сможете просмотреть сведения о выполненном сканировании. Все журналы сканирования доступны в разделе «Файлы журналов» программы ESET Mail Security, но для просмотра соответствующих журналов необходимо в раскрывающемся меню выбрать пункт «Сканирование Hyper-V».

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, поскольку при просмотре журналов сканирования необходимо различать машины.

4.4 Карантин почты

Средство управления карантином почты позволяет работать со всеми тремя типами карантина:

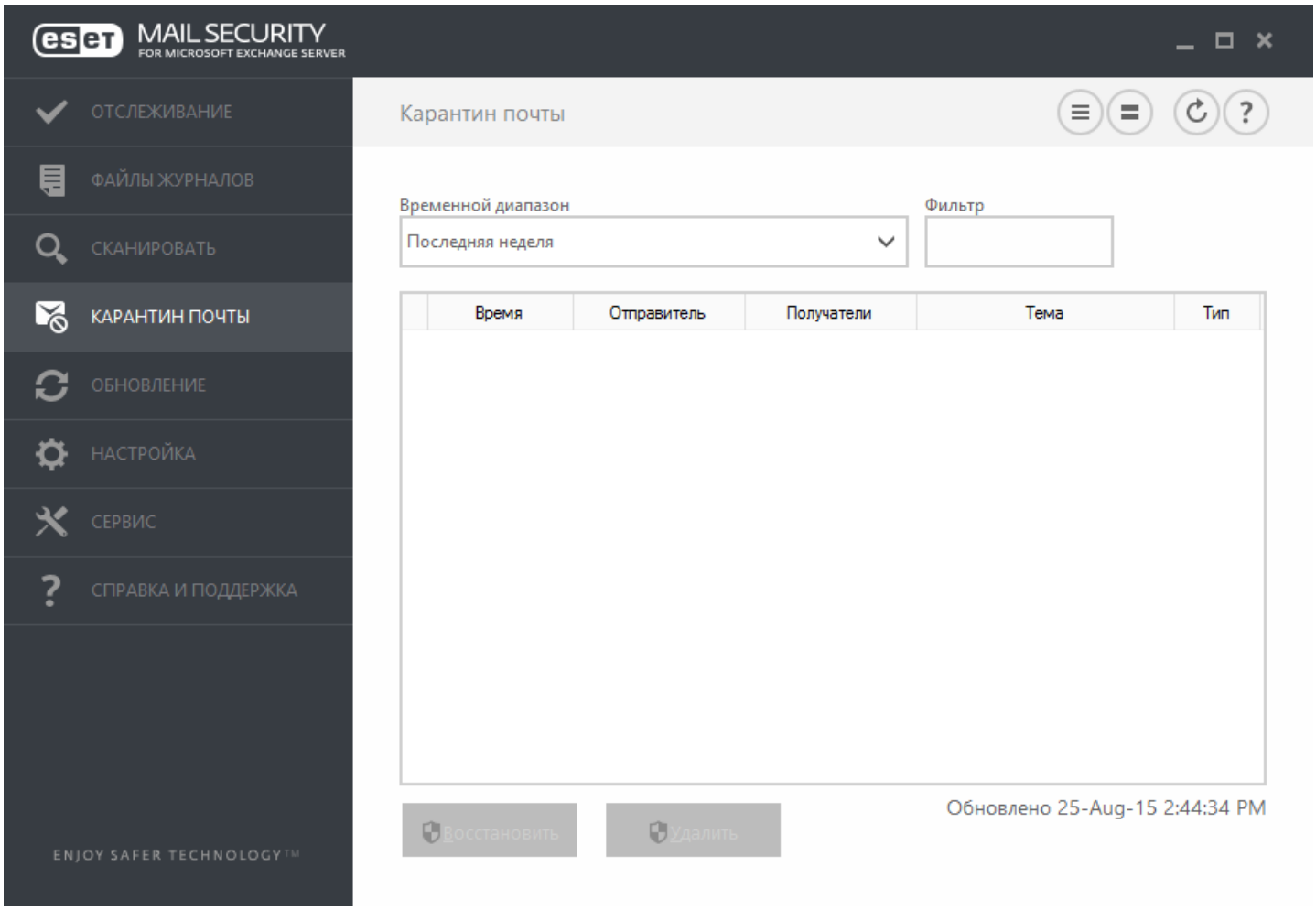
- локальный карантин,
- почтовый ящик карантина,
- карантин MS Exchange.

ПРИМЕЧАНИЕ. Веб-интерфейс карантина почты является альтернативой средству управления карантином почты, которая позволяет управлять объектами электронной почты, помещенными в карантин.

Фильтрация

- **Временной диапазон**: вы можете выбрать временной диапазон, к которому относятся отображаемые сообщения (по умолчанию одна неделя). Если изменить временной диапазон, элементы карантина почты автоматически перезагружаются.
- **Фильтр**: вы можете фильтровать отображаемые сообщения электронной почты с помощью текстового поля фильтрации (поиск выполняется по всем столбцам).

ПРИМЕЧАНИЕ. Данные средства управления карантином не обновляются автоматически. Чтобы в карантине почты отображались актуальные элементы, рекомендуется регулярно щелкать значок .



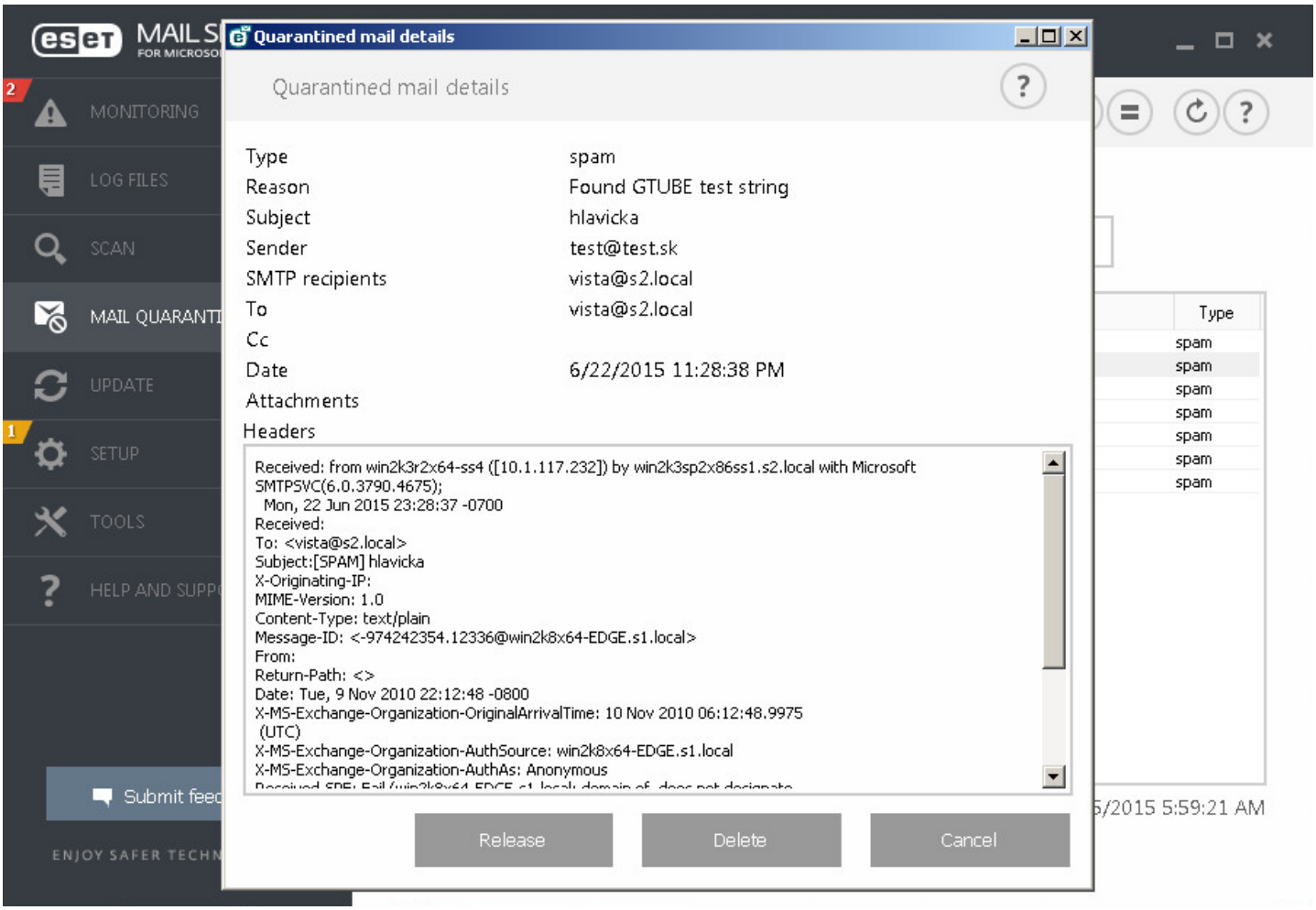
Действие

- **Восстановить**: это действие отправляет сообщение электронной почты обратно к отправителю, используя каталог преобразования, и удаляет его из карантина. Нажмите кнопку **Да** для подтверждения.
- **Удалить**: это действие удаляет сообщение из карантина. Нажмите кнопку **Да** для подтверждения.

Сведения о почте, перемещенной на карантин: дважды щелкните отправленное на карантин сообщение или щелкните его правой кнопкой мыши и выберите пункт **Подробности**, чтобы отобразить всплывающее окно с

подробными сведениями об отправленном на карантин сообщении электронной почты. Кроме того, некоторые дополнительные сведения о почтовом сообщении можно найти в заголовке почтового сообщения согласно RFC.

Действия можно вызывать также из контекстного меню. Если по отношению к перемещенному в карантин сообщению электронной почты нужно выполнить действие, выберите команду **Восстановить**, **Удалить** или **Удалить безвозвратно**. Нажмите кнопку **Да** для подтверждения. Если выбрать команду **Удалить безвозвратно**, сообщение будет удалено также из файловой системы, тогда как команда **Удалить** удаляет элемент только из представления, используемого средством управления карантином почты.



4.4.1 Сведения о почте, перемещенной на карантин

В этом окне содержится информация о перемещенном на карантин почтовом сообщении, например **Тип**, **Причина**, **Тема**, **Отправитель**, **Получатели SMTP**, **Получатель**, **Копия**, **Дата**, **Вложения** и **Заголовки**. В случае необходимости заголовки можно выделять, копировать и вставлять.

Чтобы выбрать действие для сообщения электронной почты, помещенного в карантин, используйте следующие кнопки:

- **Восстановить**: это действие отправляет сообщение электронной почты обратно к отправителю, используя каталог преобразования, и удаляет его из карантина. Нажмите кнопку **Да** для подтверждения.
- **Удалить**: это действие удаляет сообщение из карантина. Нажмите кнопку **Да** для подтверждения.

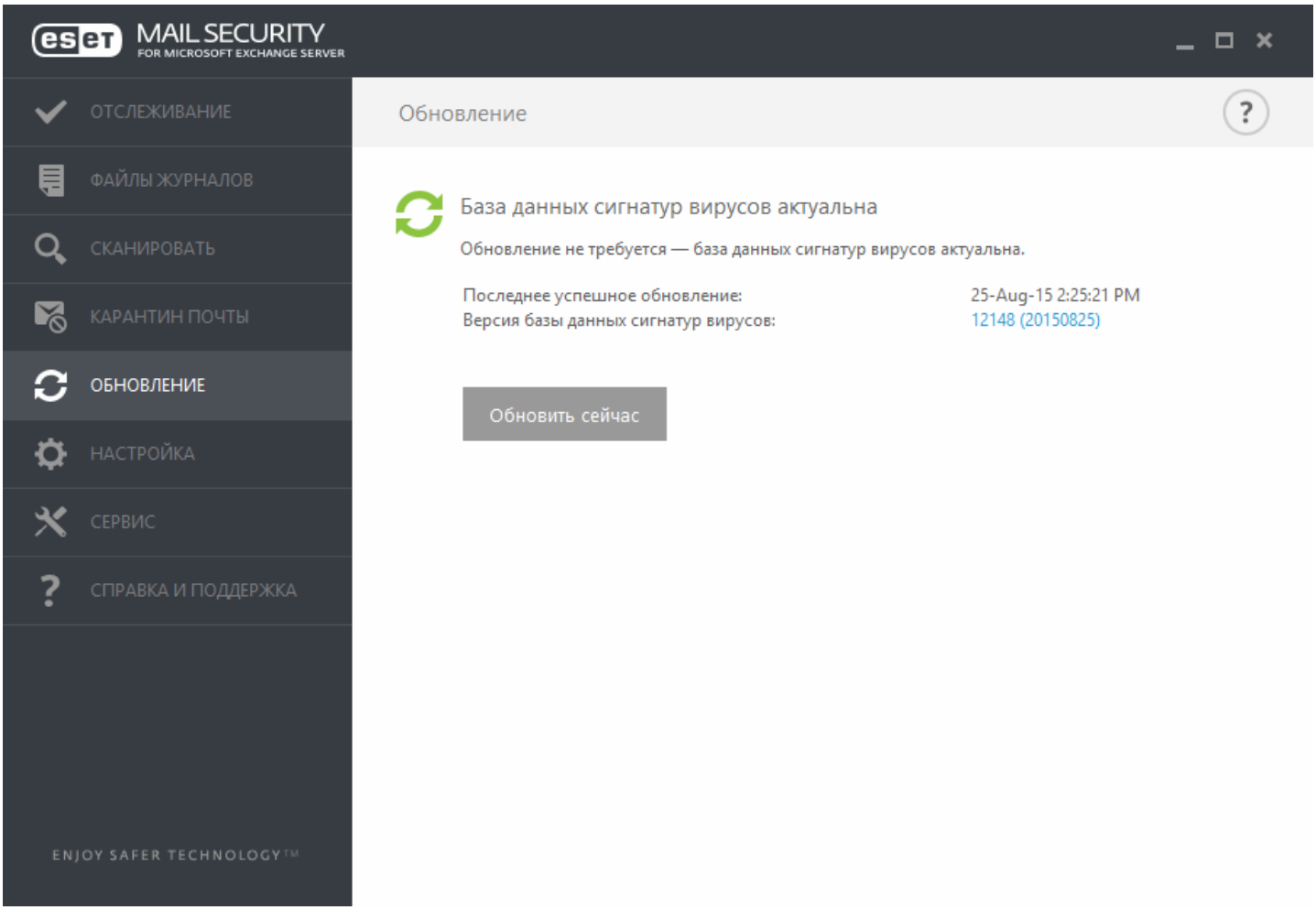
Нажатие кнопки **Отмена** закроет окно сведений о помещенных на карантин почтовых сообщениях.

4.5 Обновление

Регулярное обновление ESET Mail 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.

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

Чтобы начать процесс обновления, выберите команду **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**.

ВНИМАНИЕ! 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**).

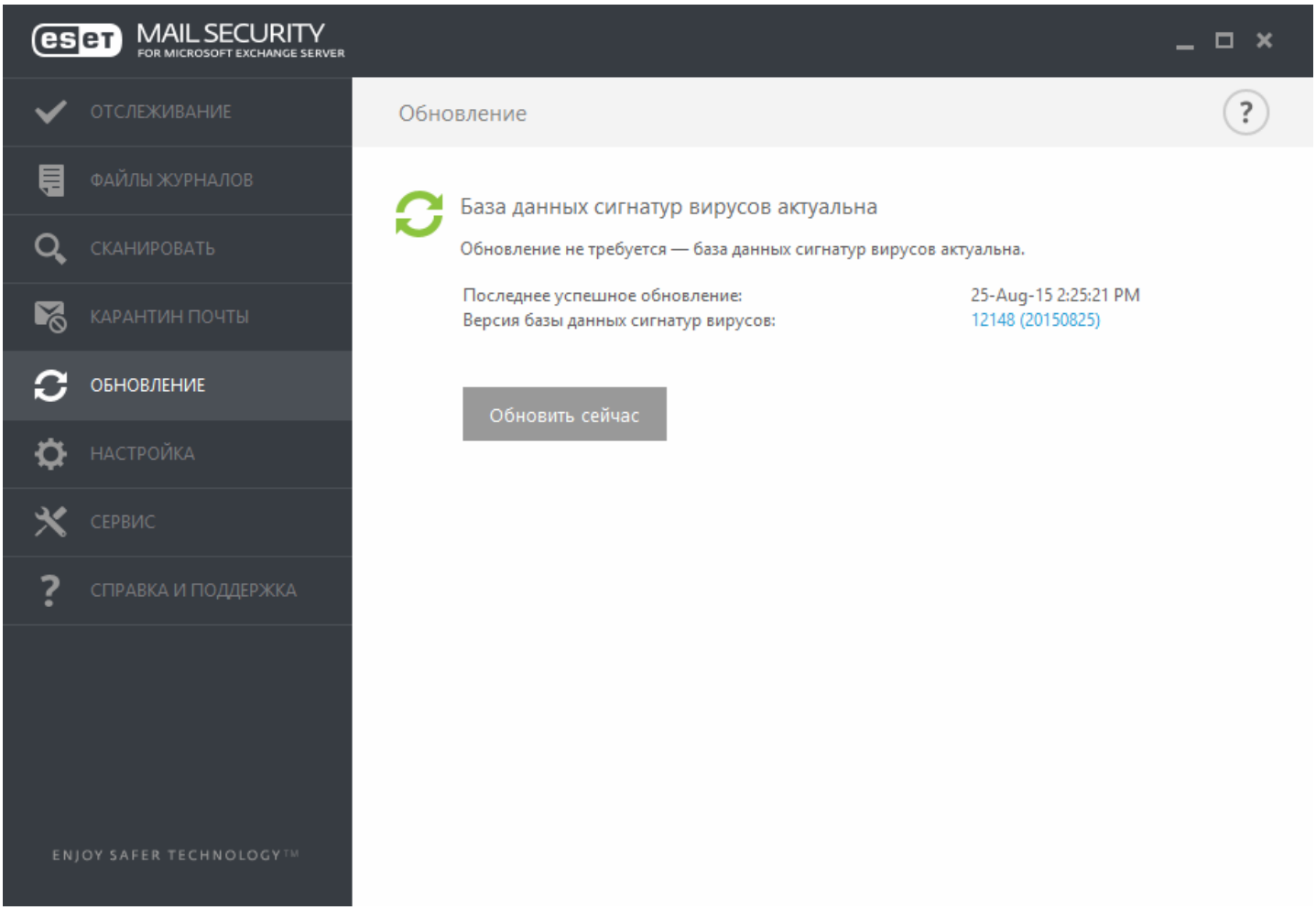
Недействительная лицензия: в разделе параметров обновления введен неправильный лицензионный ключ. Рекомендуется проверить данные аутентификации. В окне «Дополнительные настройки» (нажмите F5 на клавиатуре) содержатся расширенные параметры обновления. В главном меню последовательно щелкните элементы **Справка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

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

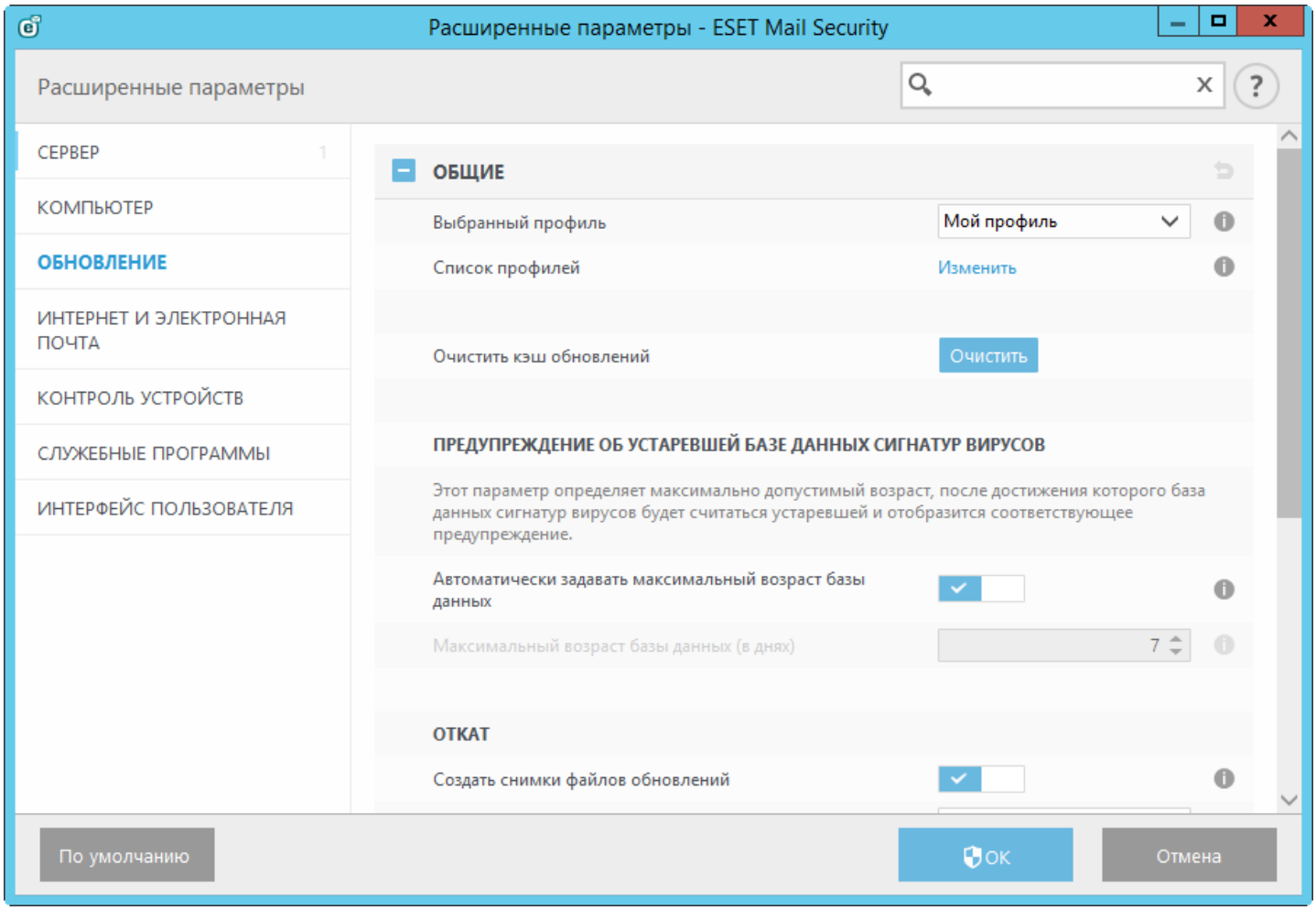
ПРИМЕЧАНИЕ. Дополнительные сведения можно найти в этой статье базы знаний ESET.

4.5.1 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). Чтобы сконфигурировать расширенные параметры обновлений, такие как режим обновления, доступ через прокси-сервер, подключение к локальной сети и создание копий сигнатур вирусов (зеркал), в левой части окна **Дополнительные настройки** щелкните элемент **Обновление**. При возникновении проблем с обновлением щелкните элемент **Очистить кэш**, чтобы удалить временные файлы обновлений. По умолчанию в меню **Сервер обновлений** выбран параметр **Автоматический выбор**. Параметр **Автоматический выбор** 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**.

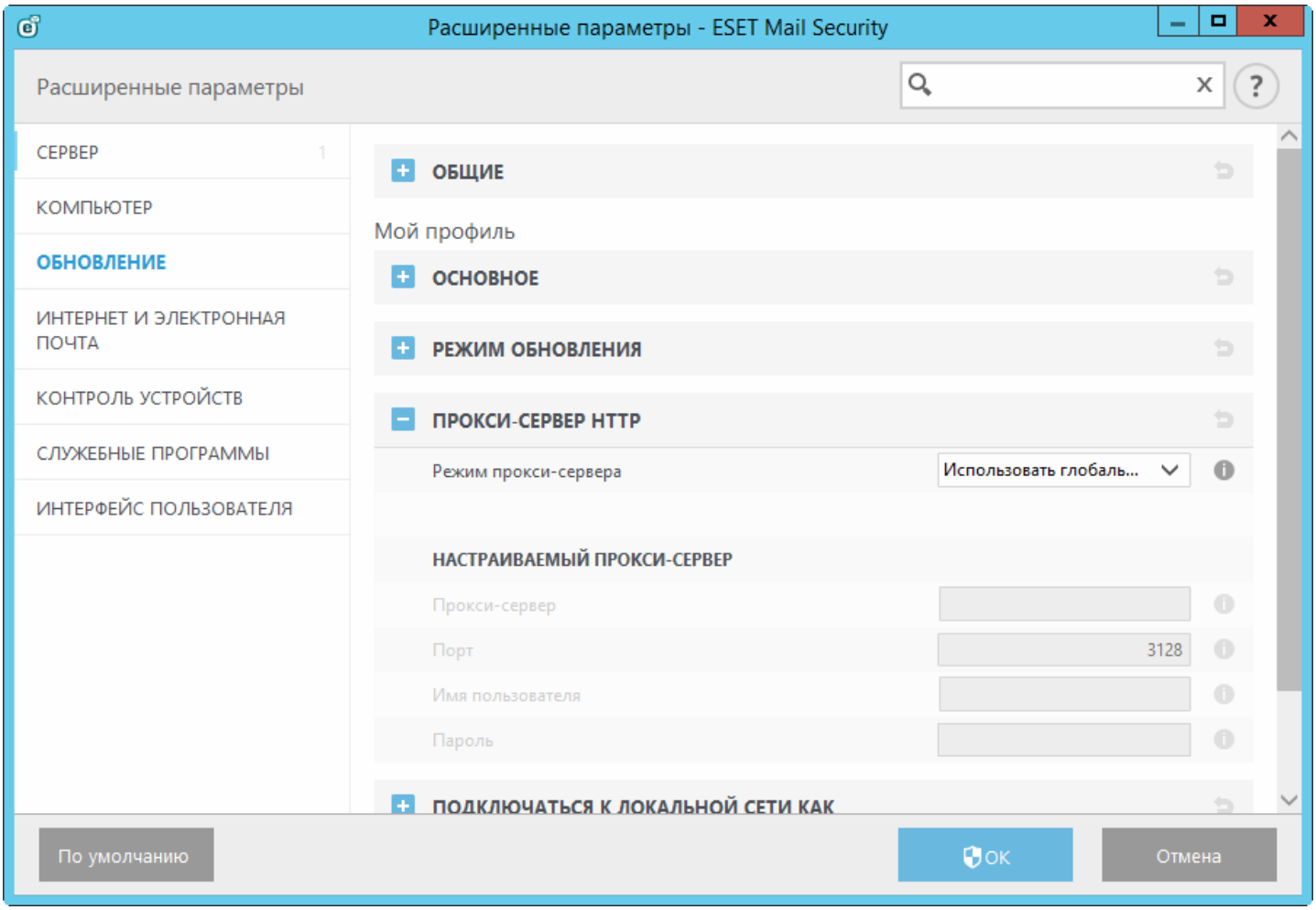


Чтобы использовать программу наилучшим образом, необходимо включить ее автоматическое обновление. Это возможно только в случае, если в разделе **Справка и поддержка** > **Активировать лицензию** введен правильный **Лицензионный ключ**.

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

4.5.2 Настройка обновлений на прокси-сервере

Если прокси-сервер используется для подключения к Интернету в системе, в которой установлено приложение ESET Mail Security, параметры прокси-сервера нужно настроить в разделе «Дополнительные настройки». Для доступа к окну конфигурирования прокси-сервера нажмите клавишу F5, чтобы открыть окно «Дополнительные настройки» и выберите пункты **Обновление** > **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, попробуйте автоматически обнаружить параметры прокси-сервера, выбрав в раскрывающемся меню пункт **Использовать общие параметры прокси-сервера**.

ПРИМЕЧАНИЕ. Параметры прокси-сервера для различных профилей обновления могут различаться. В этом случае следует настроить разные профили обновления в разделе «Дополнительные настройки», выбрав для этого пункт **Обновление** > **Профиль**.

4.6 Настройка

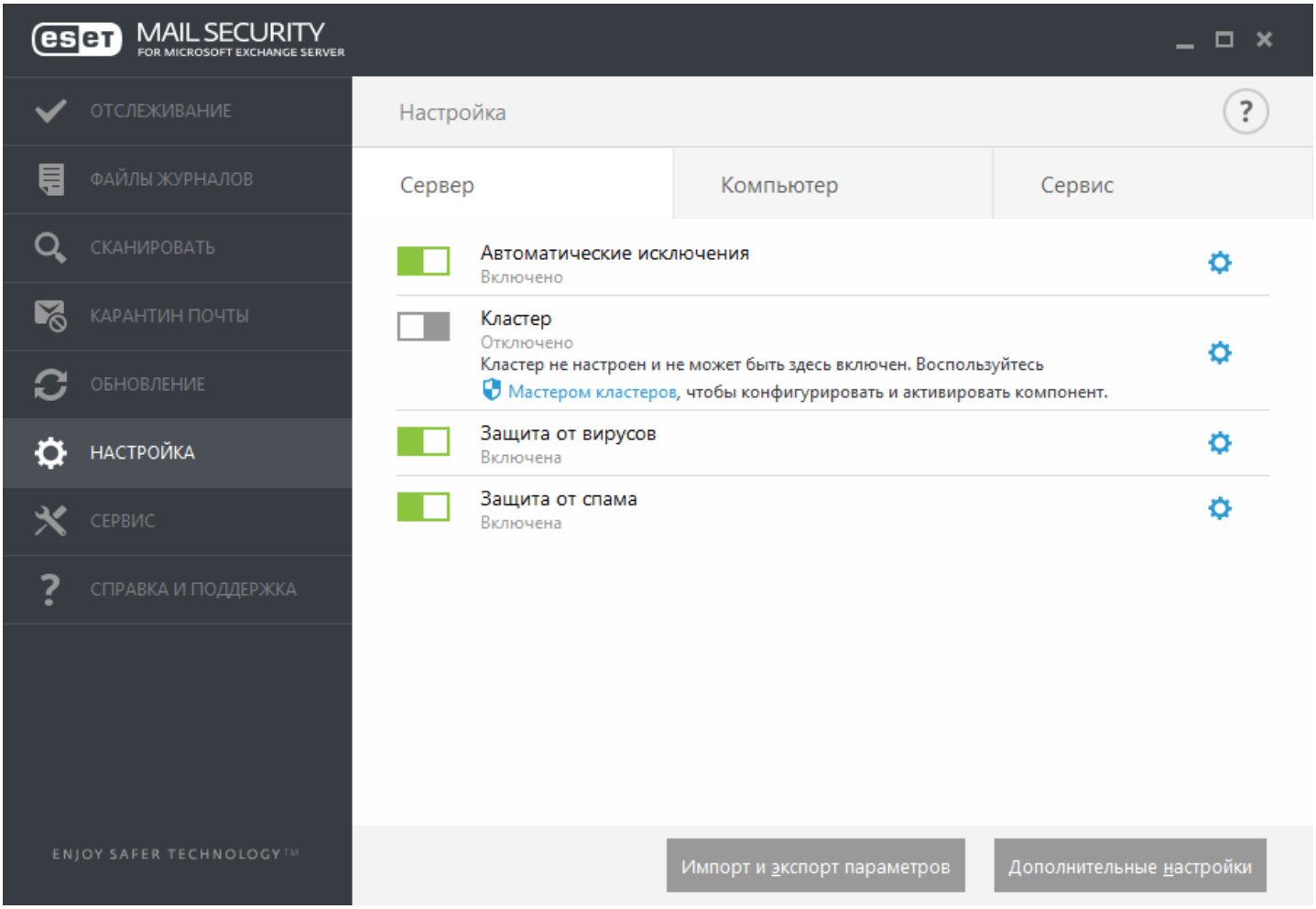
Меню настройки состоит из трех вкладок:

- Сервер
- Компьютер
- Сервис

4.6.1 Сервер

Программа ESET Mail Security обеспечивает защиту сервера за счет применения основных функций: защита от вирусов и шпионских программ, резидентная защита (защита в реальном времени), защита доступа в Интернет и защита почтового клиента. Дополнительные сведения о каждом из этих типов защиты см. в разделе «ESET Mail Security — Компьютер».

- 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.
- **Защита от вирусов** предотвращает вредоносные атаки на компьютер путем контроля файлов, электронной почты и связи через Интернет.
- Чтобы угрозы в электронной почте можно было обнаруживать максимально качественно, в **защите от спама** совмещается целый ряд технологий («черные» списки реального времени, «черные» списки серверов на основе DNS, технология создания цифровых отпечатков, проверка репутации, анализ содержимого, фильтр Байеса, правила, работа с «белыми» и «черными» списками вручную и т. д.).



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.

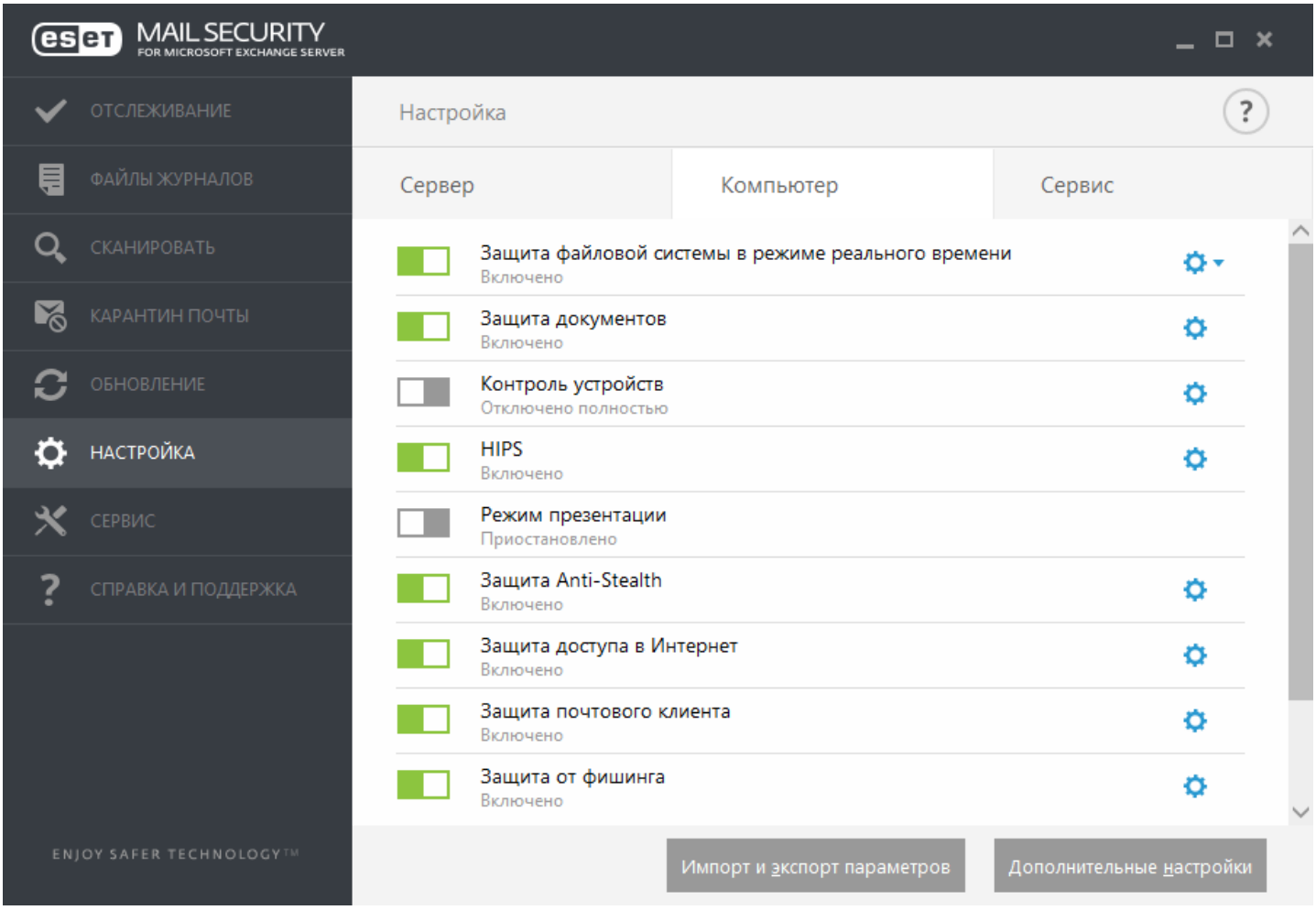
4.6.2 Компьютер

ESET Mail 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 откроется окно настройки Исключения и можно будет 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.
- **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 почтового клиента** — 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.

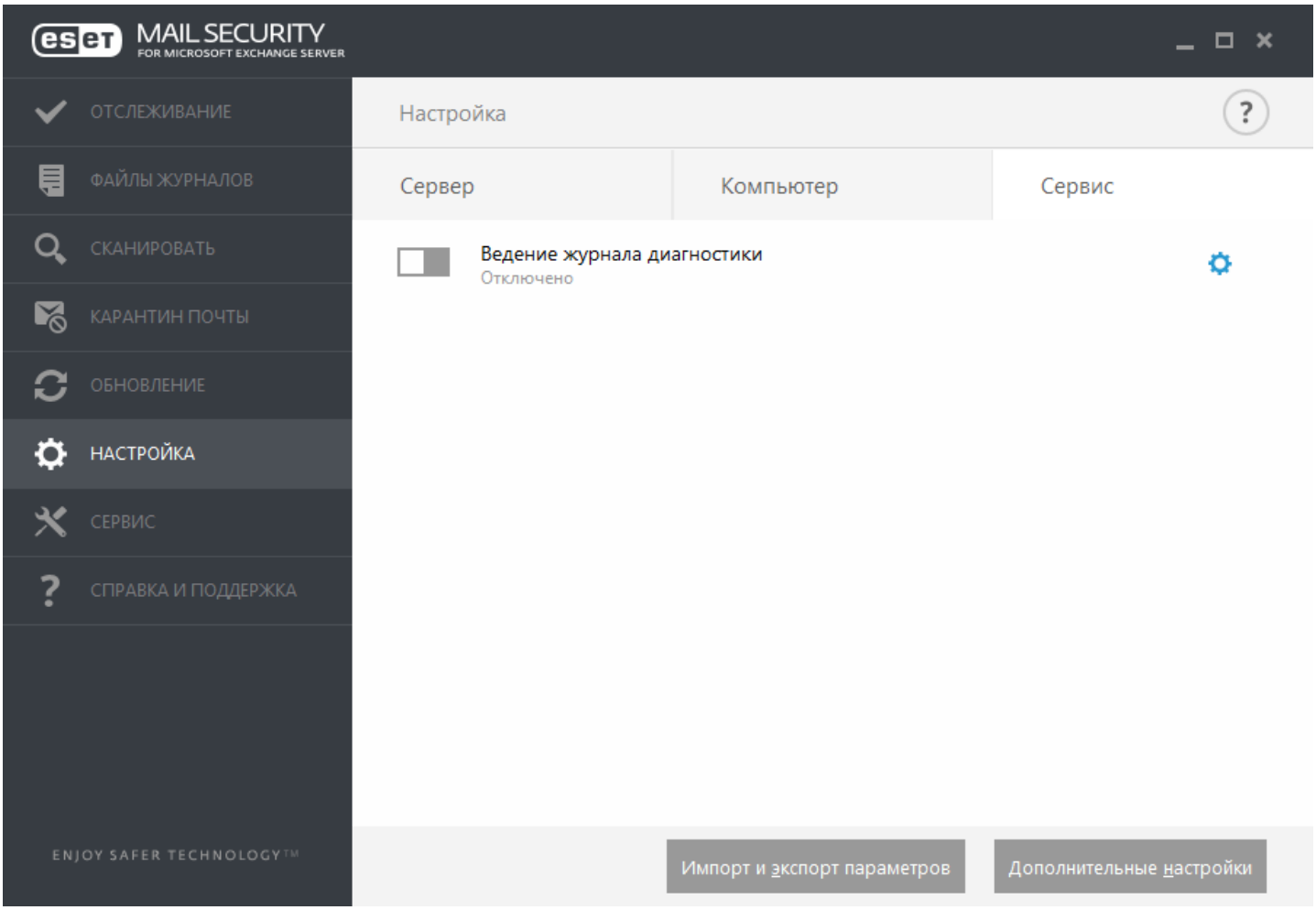
ПРИМЕЧАНИЕ. Защита документов отключена по умолчанию. Если необходимо, ее можно включить, щелкнув значок переключателя.

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.

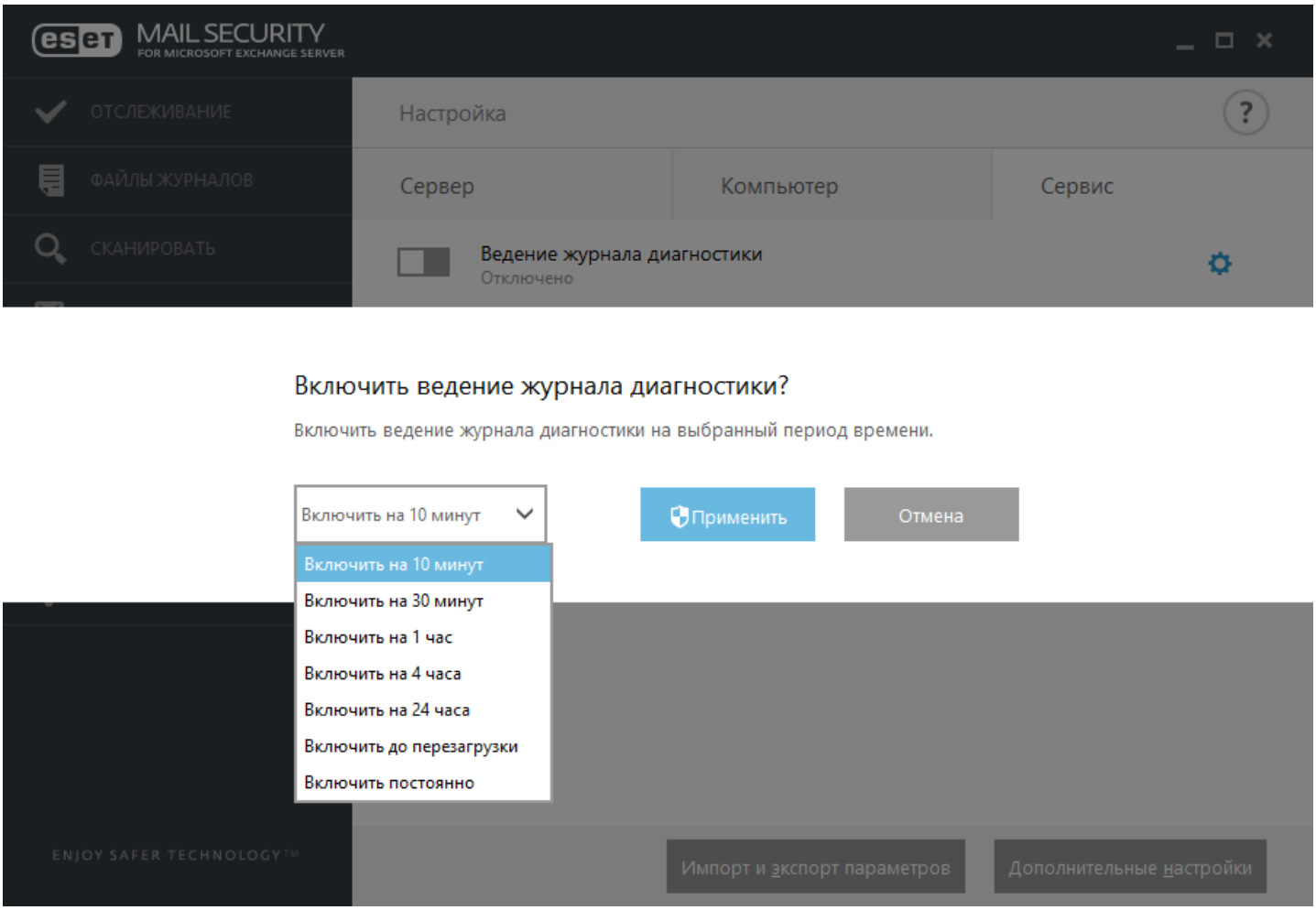
Чтобы получить доступ к более подробным настройкам, щелкните элемент **Дополнительные настройки** или нажмите клавишу **F5**.

4.6.3 Сервис

Ведение журнала диагностики: выбор компонентов, которые должны вести журналы диагностики, когда ведение таких журналов включено. 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). Компоненты, которые не отображаются на этой вкладке, всегда ведут журналы диагностики.



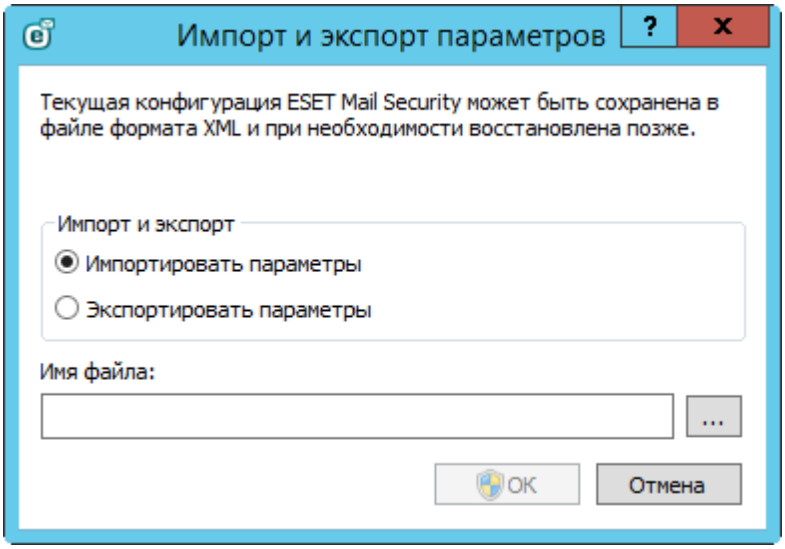
- **Включить** ведение журнала диагностики на выбранный период времени.



4.6.4 Импорт и экспорт параметров

Чтобы импортировать или экспортировать конфигурацию ESET Mail Security, в разделе **Настройки** нужно щелкнуть элемент **Импорт и экспорт параметров**.

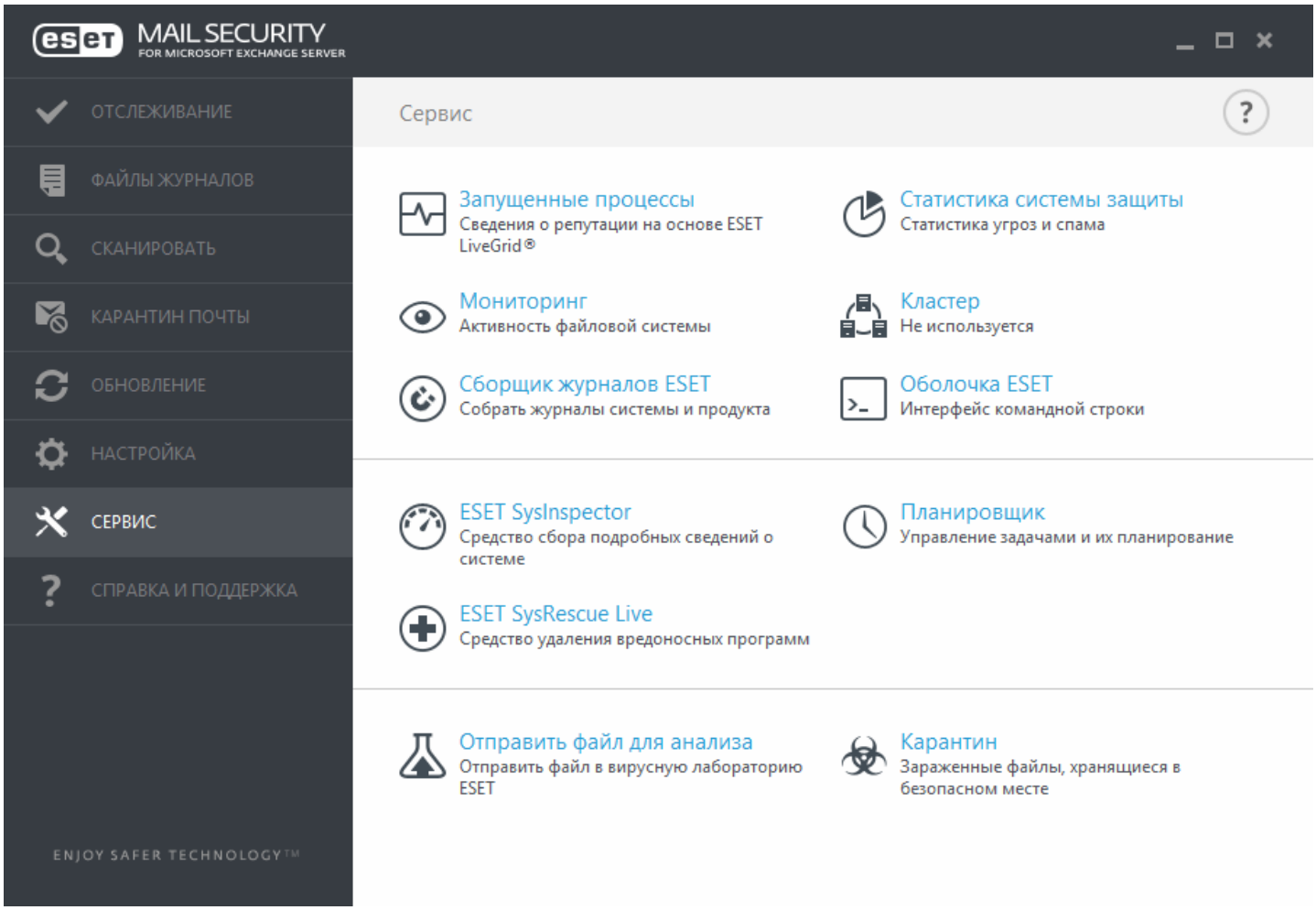
И для импорта, и для экспорта используются файлы в формате XML. Функции импорта и экспорта полезны, если нужно сделать резервную копию текущей конфигурации ESET Mail Security. С помощью этой резервной копии можно впоследствии применить те же параметры на других компьютерах.



4.7 Сервис

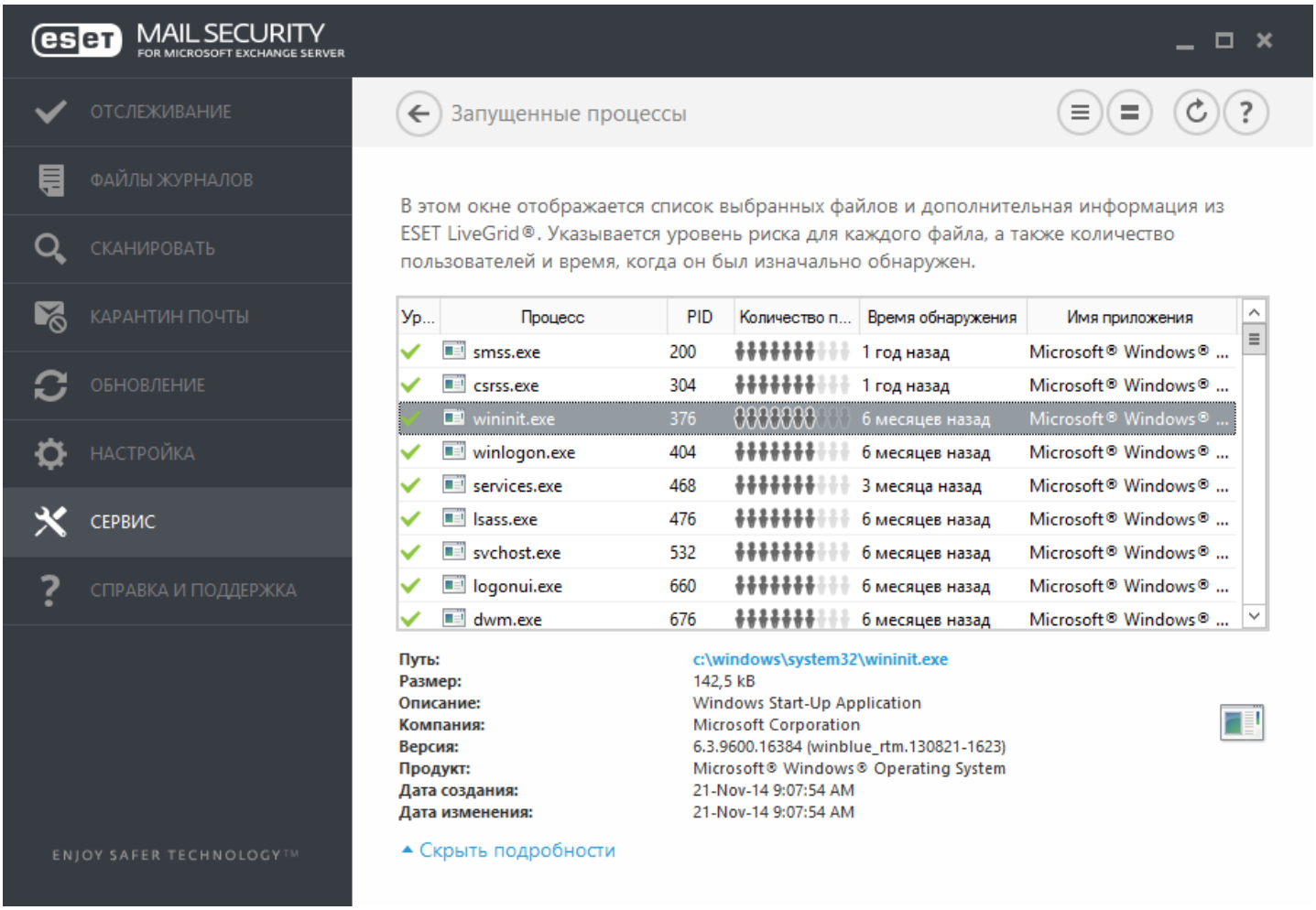
В меню «Сервис» доступны модули, которые позволяют упростить процесс администрирования программы и содержат дополнительные возможности. В этом меню представлены следующие служебные программы.

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



4.7.1 Запущенные процессы

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



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

Процесс: имя образа программы или процесса, запущенных в настоящий момент на компьютере. Для просмотра всех запущенных на компьютере процессов 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 при сканировании, благодаря чему ускоряется сканирование компьютера по требованию или защита файловой системы в реальном времени.

Количество пользователей: количество пользователей данного приложения. Эту информацию собирает технология ESET Live Grid.

Время обнаружения: время, прошедшее с момента, когда программу обнаружила технология ESET Live Grid.

ПРИМЕЧАНИЕ.Если для приложения выбран уровень безопасности Неизвестно (оранжевый), оно не обязательно является вредоносной программой. Обычно это просто новое приложение. Если вы не уверены в

безопасности файла, воспользуйтесь функцией отправки 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.

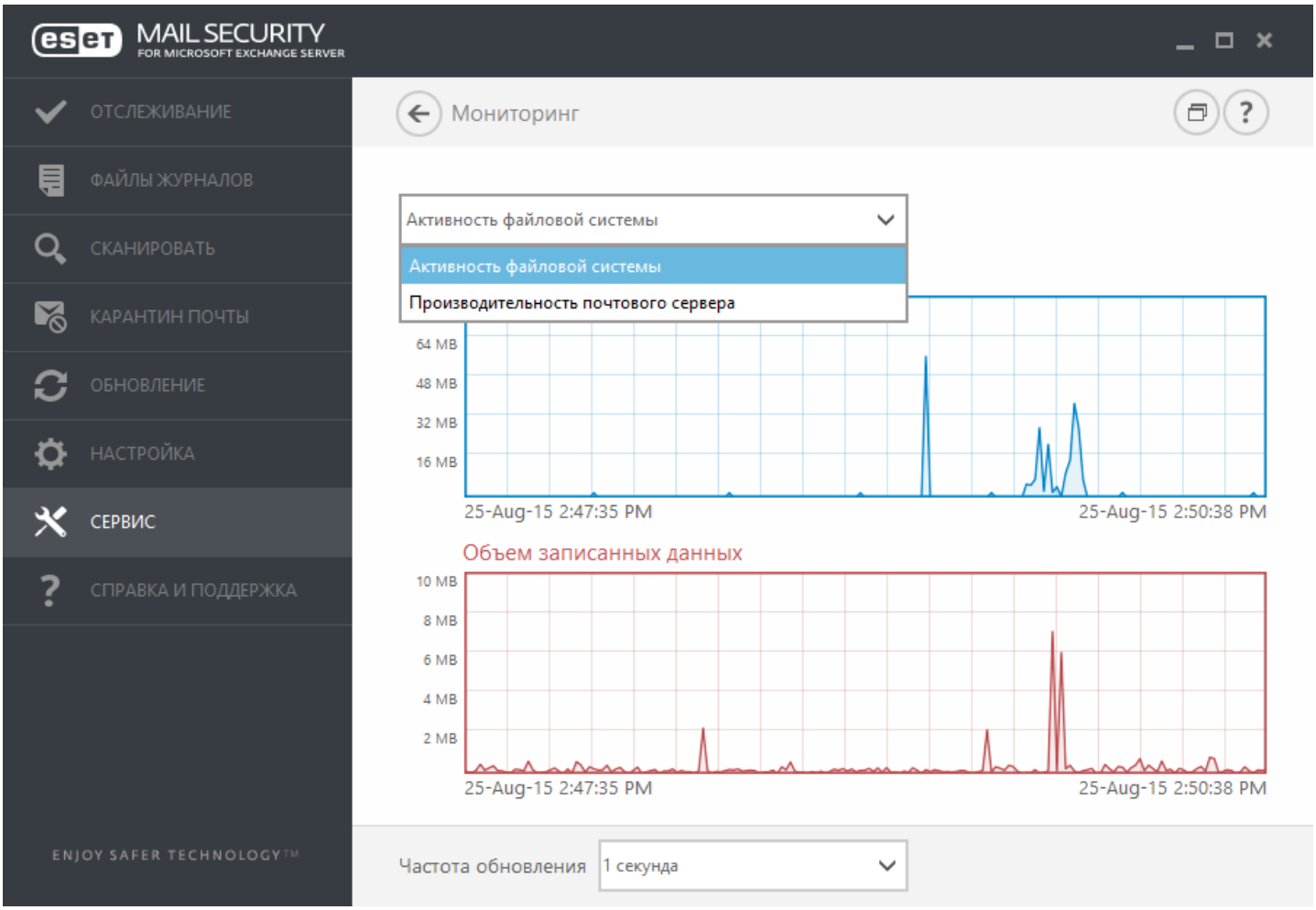
Если выбрать определенное приложение внизу, будет выведена указанная ниже информация.

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

4.7.2 Мониторинг

Чтобы отобразить текущие **активность файловой системы** и **производительность почтового сервера** в форме графика, щелкните **Сервис** > **Мониторинг**. В виде двух графиков показывает количество данных, которые были прочитаны и записаны в вашей системе. В нижней части диаграммы находится временная шкала, на которой отображается активность файловой системы в реальном времени за выбранный временной интервал. Чтобы изменить временной интервал, выберите необходимое значение в раскрывающемся 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.

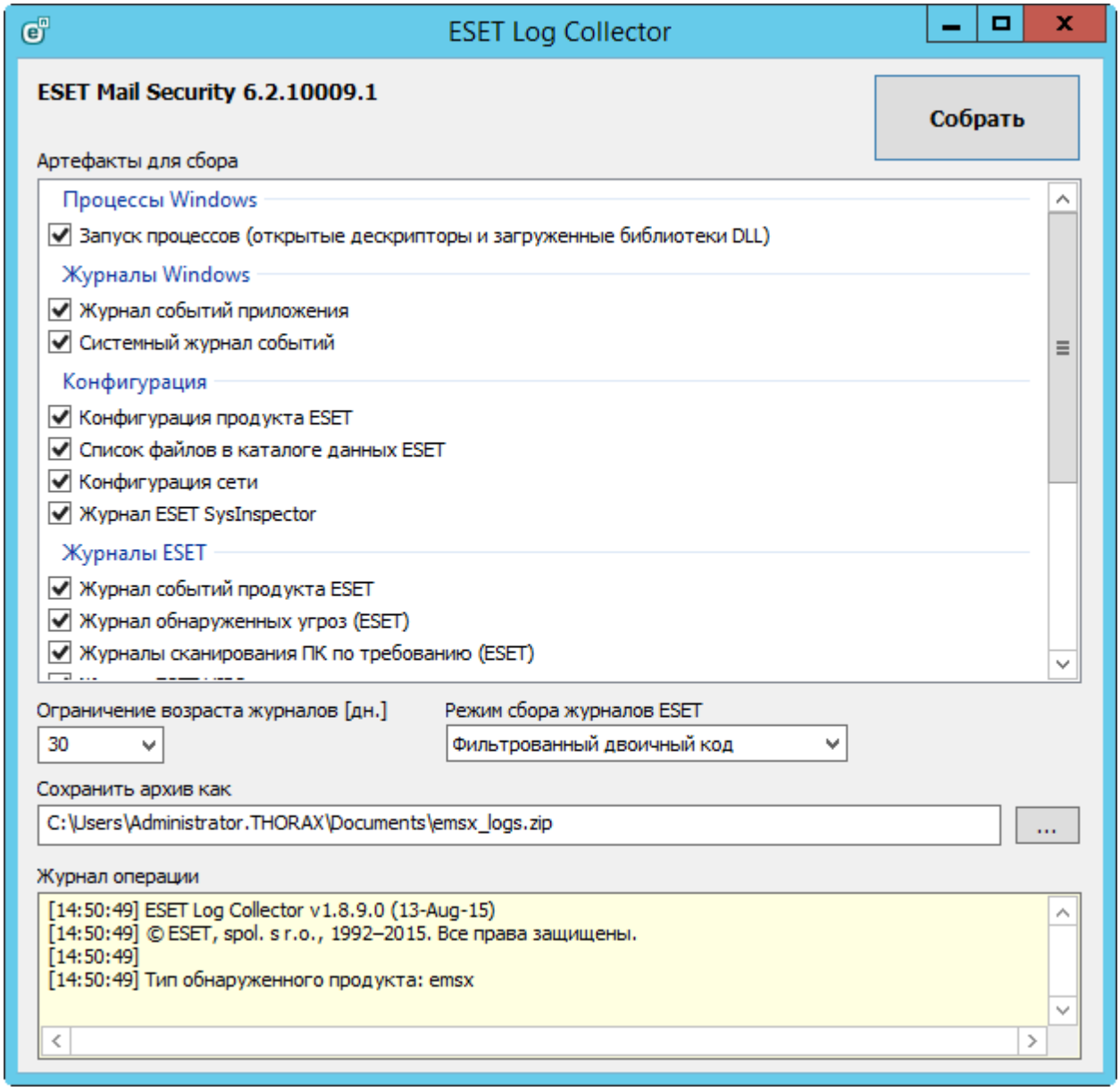
4.7.2.1 Выбор периода времени

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

4.7.3 ESET Log Collector

ESET Log Collector представляет собой приложение, которое автоматически собирает с сервера данные (например, конфигурацию и журналы) для ускорения решения проблем. Если в службе поддержки клиентов ESET рассматривается ваше обращение, вас могут попросить предоставить журналы, созданные на вашем компьютере. Сборщик журналов ESET облегчает сбор необходимой информации.

Получить доступ к приложению ESET Log Collector можно из главного меню, последовательно щелкнув элементы **Сервис** > **Сборщик журналов ESET**.



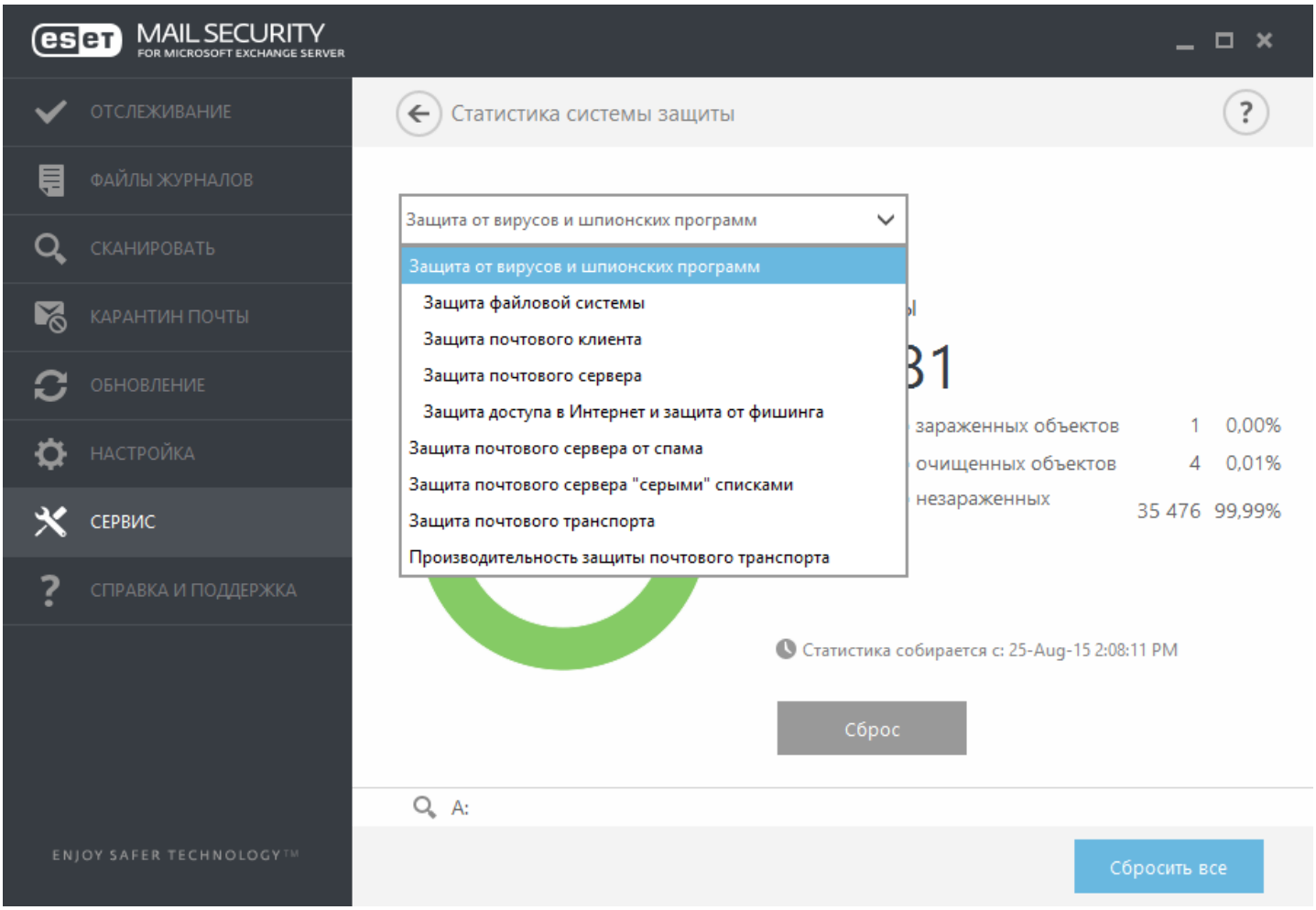
Выберите флажки рядом с журналами, которые необходимо собрать. Если вы не знаете, какие данные нужно собрать, оставьте все флажки выбранными (по умолчанию). Укажите каталог, куда необходимо сохранить заархивированные файлы, и нажмите кнопку **Сохранить**. Название файла архива является предварительно заданным. Нажмите кнопку **Собрать**.

Во время сбора информации можно просматривать сведения в окне журнала операции в нижней части окна. В нем отображается, какая операция выполняется в данный момент. Когда сбор сведений завершится, отобразятся все собранные и заархивированные файлы. Это означает, что сбор завершился успешно и файл архива (например, `emsx_logs.zip`) сохранен в указанный каталог.

Дополнительные сведения о приложении ESET Log Collector и о списке файлов, собираемых ESET Log Collector, см. в базе знаний ESET.

4.7.4 Статистика системы защиты

Чтобы в ESET Mail Security отобразить диаграмму статистических сведений о модулях защиты, нажмите **Сервис** > **Статистика системы защиты**. Выберите интересующий вас модуль защиты в раскрывающемся меню. На экран будет выведена соответствующая диаграмма и легенда. Подведите курсор мыши к элементу легенды, чтобы в диаграмме отобразились сведения об этом элементе.



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 почтового сервера**: на экран выводится статистика по защите почтового сервера от вирусов и шпионских программ.
- **Защита доступа в Интернет и защита от фишинга**: отображение только объектов, загруженных веб-браузерами.
- **Защита почтового сервера от спама**: отображение статистики защиты от спама с момента последнего запуска.
- **Защита почтового сервера «серыми» списками**: отображается также статистика защиты от спама, сформированная методом работы с «серыми» списками.
- **Защита почтового транспорта**: на экран выводятся объекты, которые были проверены, заблокированы или удалены почтовым сервером.
- **Производительность защиты почтового сервера**: на экран выводятся данные, обработанные интерфейсом VSAPI или агентом транспорта (в байтах в секунду).
- **Защита базы данных почтовых ящиков**: отображаются объекты, обработанные интерфейсом VSAPI (количество **проверенных**, **помещенных в карантин** и **удаленных объектов**).
- **Производительность защиты базы данных почтовых ящиков**: отображаются данные, обработанные интерфейсом VSAPI (количество разных средних значений за **сегодня**, **последние 7 дней** и **с момента последнего сброса**).

Возле графиков статистики отображается количество всех 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.

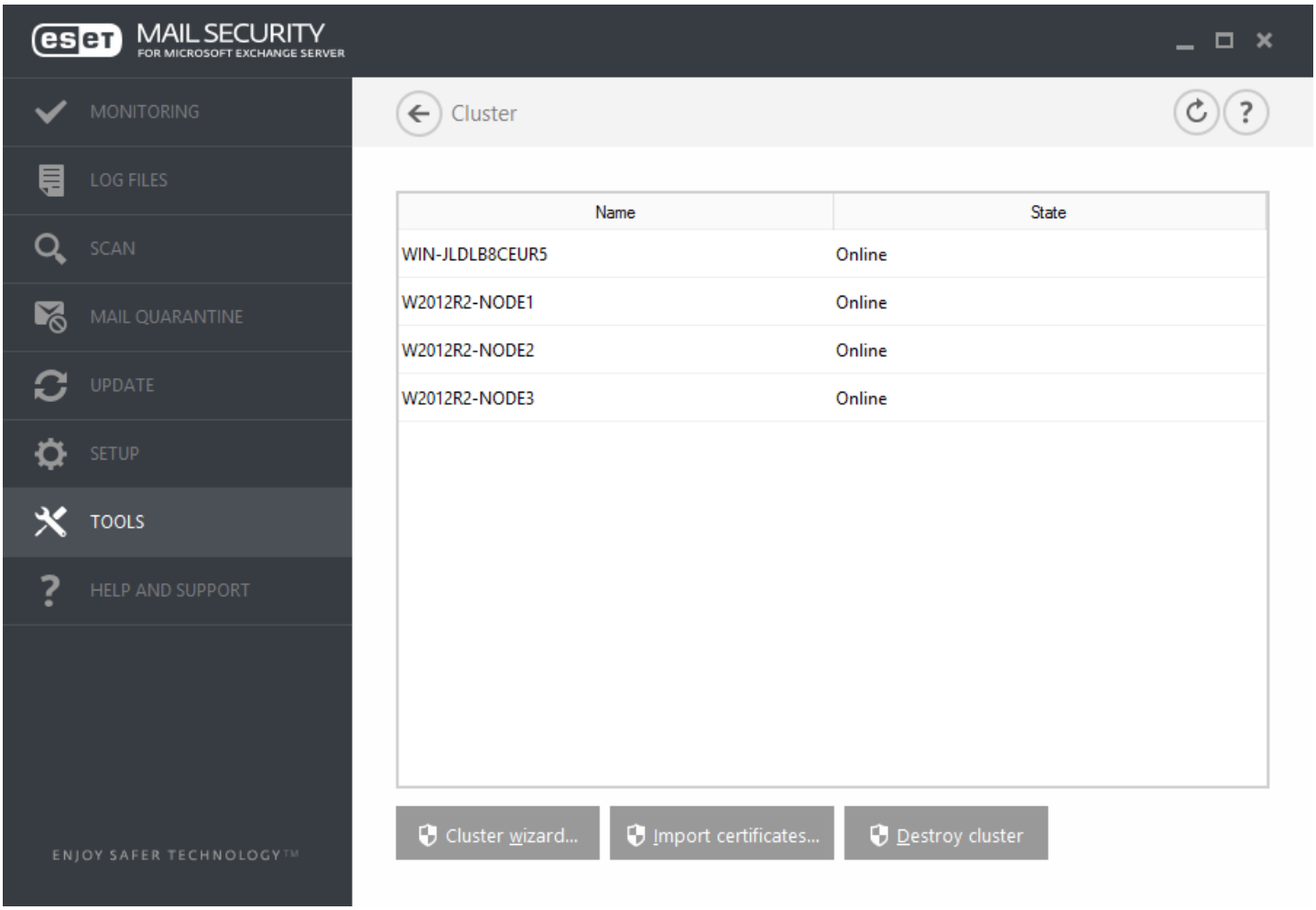
4.7.5 Кластер

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

Эта инфраструктура обеспечивает взаимодействие между серверными продуктами ESET и позволяет им обмениваться такими данными, как конфигурация и оповещения, а также выполнять синхронизацию данных, необходимых для надлежащей 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.

Автоопределение: автоматическое определение узлов, уже входящих в отказоустойчивый кластер Windows или кластер NLB, и добавление их в кластер ESET.
Обзор: узлы можно добавить вручную с помощью ввода имен 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 Mail Security на каждом их них. Это выполняется автоматически в процессе настройки кластера ESET.

Учетные данные, необходимые для удаленной установки программы ESET Mail 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 ESET Mail Security на узлы кластера ESET.

Если необходимо, кластер ESET можно с легкостью демонтировать, выбрав команду **Уничтожение кластера**. 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 Mail 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.

Дополнительную информацию о настройке кластера ESET см. в разделе Рабочий кластер.

4.7.6 Оболочка ESET

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

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 выполнить 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, введя `eshell` с соответствующими параметрами. 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 cmd, выбрав пункт **Запуск от имени администратора**. В противном случае выполнить некоторые команды будет невозможно, потому что, открывая cmd или eShell не от имени администратора, пользователь не получает все нужные разрешения.

ПРИМЕЧАНИЕ Чтобы выполнять команды eShell из командной строки Windows или запускать пакетные

файлы, нужно настроить некоторые параметры. Для получения дополнительных сведений о запуске пакетных файлов воспользуйтесь этой ссылкой.

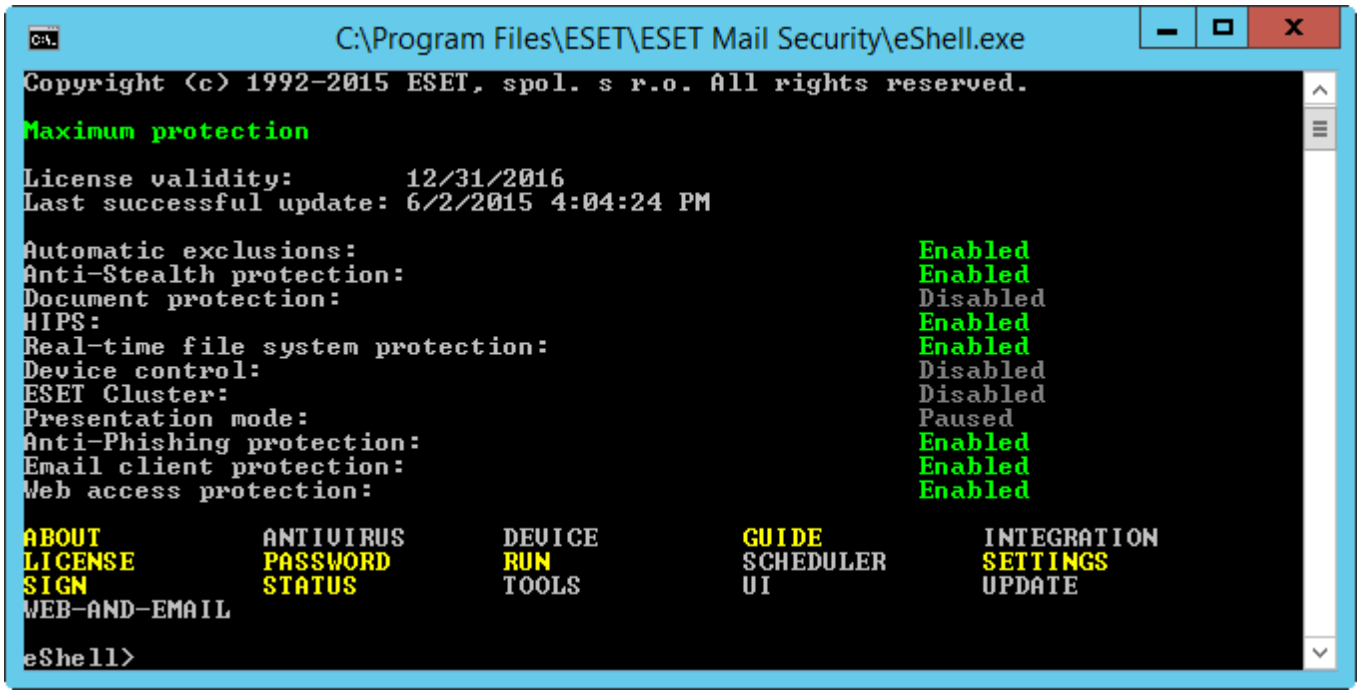
Для входа в интерактивный режим eShell можно использовать один из следующих двух способов.

- Через меню «Пуск» Windows: **Пуск** > **Все программы** > **ESET** > **ESET File Security** > **ESET shell**.
- Через командную строку Windows, введя `eshell` и нажав клавишу Enter.

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

ПРИМЕЧАНИЕ. Если в будущем нужно будет 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. По сути, это краткое руководство по eShell.

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, включить отображение скрытых команд и настроить прочие параметры.

4.7.6.1 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 ?` отобразит синтаксис для команды `STATUS` .

СИНТАКСИС

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

Видно, что конструкция `[get]` заключена в скобки. Это указывает на то, что префикс `get` используется по умолчанию для команды `status` . Это означает, что при выполнении команды `status` без указания какого-либо префикса будет использоваться префикс по умолчанию (в данном случае `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, но это не повлияет на выполнение команд.

Префикс/операция

Префикс — это операция. Префикс `GET` предоставляет сведения о том, как сконфигурирована определенная функция ESET Mail 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 того чтобы перейти на один уровень вверх, к

```
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, но 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.

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
Это новая функция, появившаяся в eShell с версии 2.0. Она 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 вводе команды выполнить автозаполнение или просмотреть доступные варианты, просто 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 по сути 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 Mail 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 всяком 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 на время этого сеанса).

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 историю 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`).

4.7.6.2 Команды

В этом разделе в качестве примера приведено несколько основных команд eShell с описаниями.

ПРИМЕЧАНИЕ. В командах не учитывается регистр: можно использовать как прописные, так и строчные буквы, но это не повлияет на выполнение команд.

Образцы команд (присутствующие в контексте ROOT)

ABOUT

На экран выводятся сведения о программе. Отображается название установленного программного продукта, номер версии, установленные компоненты (в том числе номер версии каждого компонента) и основная информация о сервере и операционной системе, на которых выполняется ESET Mail Security.

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 Mail 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. Это значит, что не придется вводить пароль каждый раз.

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.

Такой заданный пароль также очень удобен при выполнении пакетных файлов или сценариев. Ниже приведен пример такого пакетного файла.

```
eshell start batch "&" set password plain <вашпароль> "&" set status disabled
```

Такая объединенная команда запускает пакетный режим, задает пароль, который будет использоваться, и отключает защиту.

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, сконфигурирован 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 Mail 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.

4.7.6.3 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
```

Команды можно, а иногда и нужно, также связывать. Например, если нужно получить определенную запланированную задачу, введите следующие слова:

```
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».

По умолчанию для политики выполнения задано значение «Ограниченные сценарии». Это нужно из соображений безопасности. Поэтому вы можете использовать решение eShell как инструмент мониторинга, однако не можете изменять конфигурацию ESET Mail Security. При запуске команды, которая может нарушить безопасность, например команды отключения защиты, отобразится сообщение **В доступе отказано**. Для выполнения команд, которые изменяют конфигурацию, рекомендуется использовать подписанные пакетные файлы.

Если по какой-то причине нужно изменить конфигурацию путем ввода команды вручную в командную строку Windows, то 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 выберите элементы **Дополнительные настройки** > **Интерфейс пользователя** > Оболочка ESET в графическом интерфейсе.

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. И 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 параметров будет заканчиваться ошибкой. Это обусловлено тем, что 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`

4.7.7 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. Для этого также можно щелкнуть правой кнопкой мыши созданный журнал, а затем выбрать в контекстном меню команду **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*.

4.7.7.1 Создать снимок состояния компьютера

Введите краткий комментарий, описывающий создаваемый журнал, и нажмите кнопку **Добавить**. Дождитесь окончания создания журнала ESET SysInspector (состояние изменится на «Создан»). Длительность создания журнала зависит от конфигурации оборудования и системных данных.

4.7.7.2 ESET SysInspector

4.7.7.2.1 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 Mail 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.

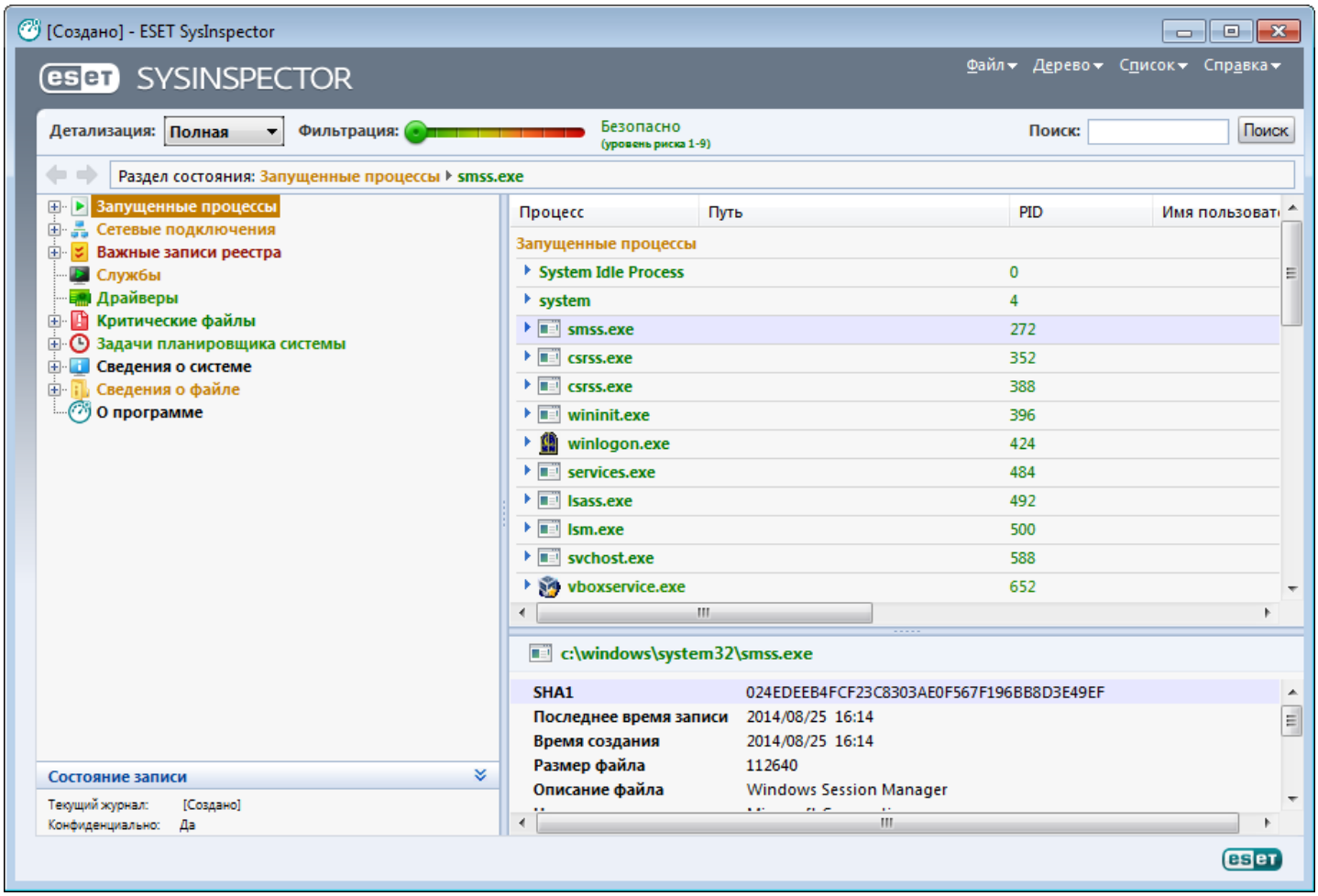
4.7.7.2.1.1 Запуск ESET SysInspector

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 Mail Security**).

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

4.7.7.2.2 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.).



4.7.7.2.2.1 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.

4.7.7.2.2.2 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

4.7.7.2.2.3 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.

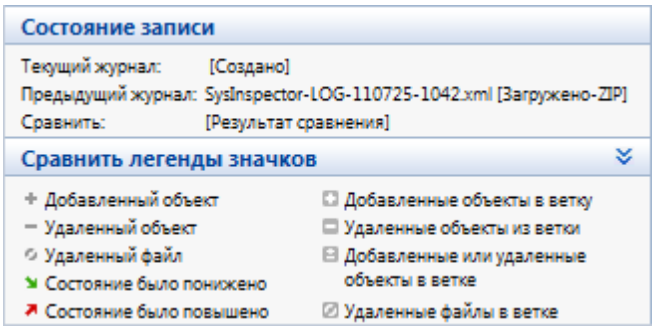
ПРИМЕЧАНИЕ. При сравнении двух файлов журнала в меню **Файл** выберите пункт **Сохранить журнал** и сохраните журнал как файл в формате ZIP. В результате будут сохранены оба файла. Если такой файл впоследствии открыть, содержащиеся в нем журналы сравниваются автоматически.

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

4.7.7.2.3 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.

4.7.7.2.4 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.

4.7.7.2.4.1 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.

4.7.7.2.4.2 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.

4.7.7.2.4.3 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.

4.7.7.2.5 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.

4.7.7.2.6 ESET SysInspector как часть ESET Mail Security

Для того чтобы открыть ESET SysInspector в ESET Mail 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).

4.7.8 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.

4.7.9 Планировщик

Планировщик управляет запланированными задачами и запускает их с предварительно заданными параметрами и свойствами. Параметры содержат информацию, такую как дата и время, а также профили обновления, которые следует использовать при выполнении задачи.

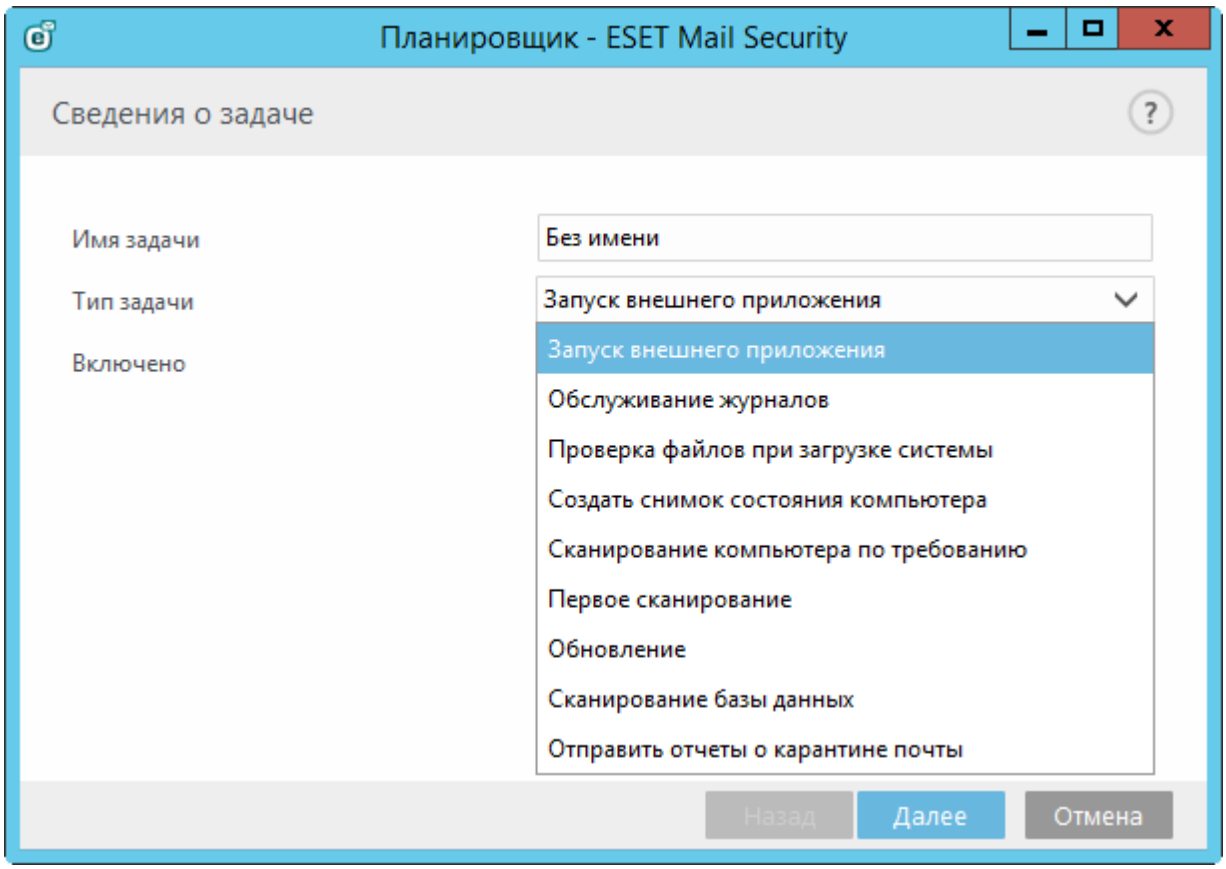
Перейти к планировщику можно из главного окна программы ESET Mail Security, последовательно щелкнув элементы **Сервис** > **Планировщик**. **Планировщик** содержит полный список всех запланированных задач и свойства конфигурации, такие как предварительно заданные дата, время и используемый профиль сканирования.

Планировщик предназначен для планирования следующих задач: обновление базы данных сигнатур вирусов, сканирование, проверка файлов, исполняемых при запуске системы, и обслуживание журнала. Добавлять и удалять задачи можно непосредственно в главном окне планировщика (нажмите кнопку **Добавить задачу** или **Удалить** в нижней части окна). С помощью контекстного меню окна планировщика можно выполнить следующие действия: отображение подробной информации, 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 журнала**
- **Регулярное автоматическое обновление**
- **Автоматическое обновление после коммутируемого соединения**
- **Автоматическое обновление после входа пользователя в систему**
- **Автоматическая проверка файлов при запуске системы** (после входа пользователя в систему)
- **Автоматическая проверка файлов при запуске системы** (после успешного обновления базы данных сигнатур вирусов)
- **Автоматическое первое сканирование**

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



Добавление новой задачи

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

3. Выберите нужную задачу в раскрывающемся меню.

- **Запуск внешнего приложения** - планирование выполнения внешнего приложения.
- **Обслуживание журнала**: в файлах журналов также содержатся остатки удаленных записей. Для эффективной работы эта задача регулярно оптимизирует записи в файлах журналов.
- **Проверка файлов, исполняемых при запуске 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 программные модули и база данных сигнатур вирусов.
- **Сканирование базы данных** — планируется сканирование базы данных, при этом объекты сканирования (общие папки, базы данных и почтовые ящики) можно выбрать так же, как и при настройке сканирования базы данных по требованию.
- **Отправить отчеты о карантине** — этот параметр применяется только к локальному карантину. Отправляются отчеты, содержащие сведения о состоянии карантина и хранящихся в нем объектах, а также ссылки на веб-интерфейс карантина почты, который позволяет быстро просматривать хранящиеся на карантине объекты электронной почты и управлять ими. Вы можете указать адрес электронной почты пользователя, который должен получать отчеты о карантине.

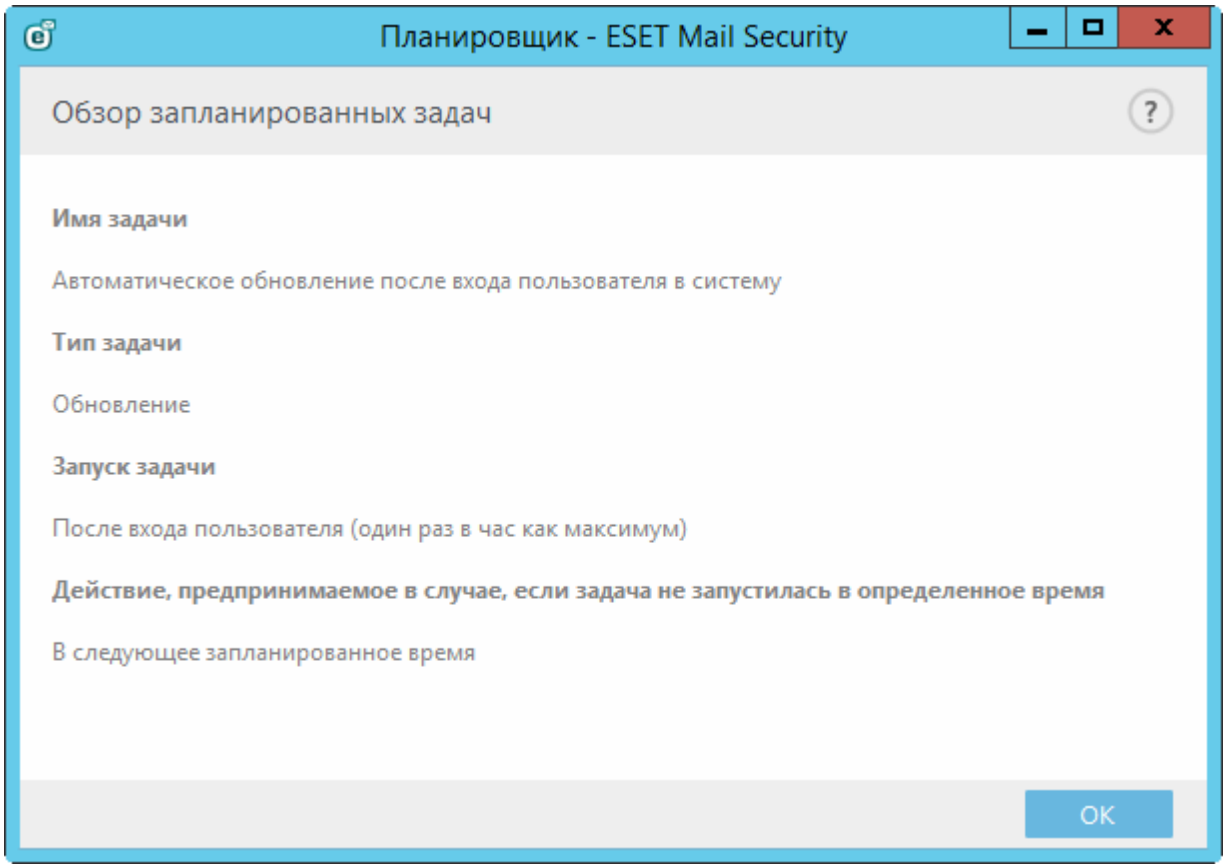
4. Щелкните переключатель **Включено**, если нужно активировать задачу (это можно сделать позже, установив/сняв флажок в списке запланированных задач), выберите элемент **Далее** и выберите один из указанных ниже режимов времени выполнения.

- **Однократно**: задача будет выполнена однократно в установленную дату и время.
- **Многократно**: задача будет выполняться регулярно через указанный промежуток времени.
- **Ежедневно**: задача будет многократно выполняться каждые сутки в указанное время.
- **Еженедельно**: задача будет выполняться в выбранный день недели в указанное время.
- **При определенных условиях**: задача будет выполнена при возникновении указанного события.

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

- **В следующее запланированное время**
- **Как можно скорее**
- **Незамедлительно, если с момента последнего запуска прошло больше времени, чем указано** (интервал можно указать с помощью ползунка полосы прокрутки **Время с момента последнего запуска**).

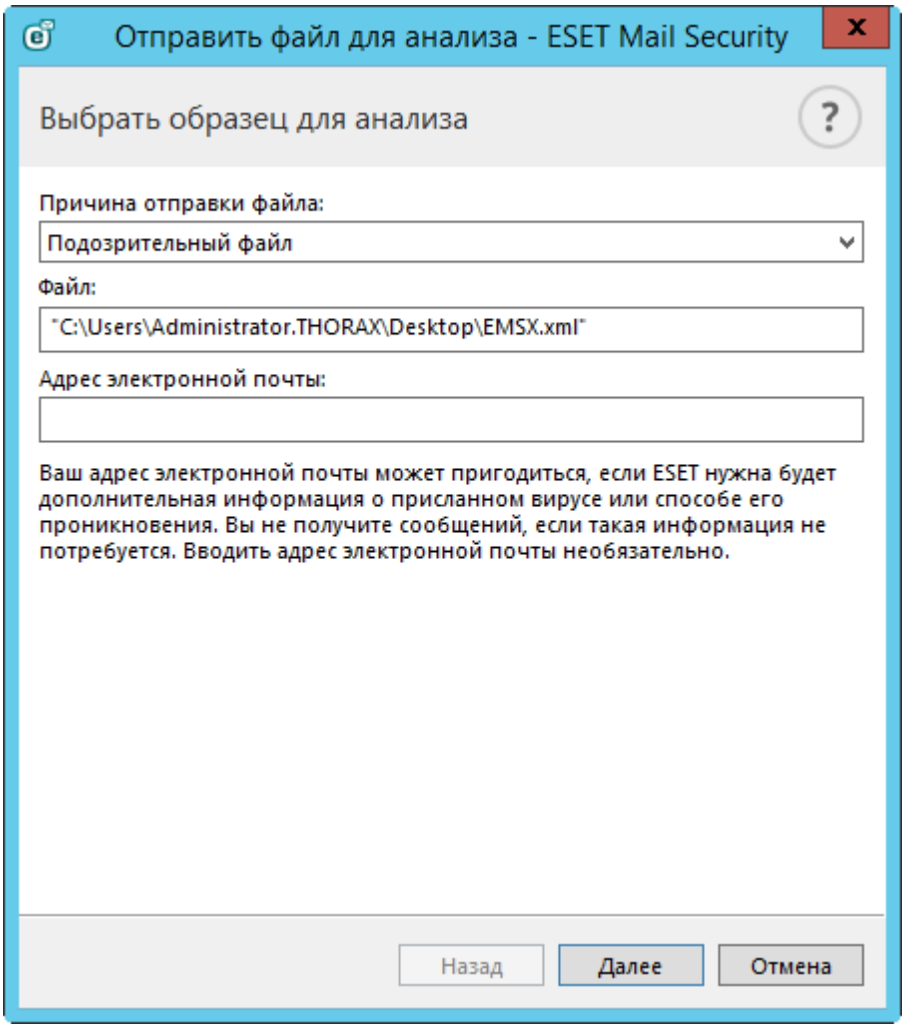
Щелкните задачу правой кнопкой мыши и, чтобы просмотреть сведения о ней, в контекстном меню выберите пункт **Показать информацию о задаче** .



4.7.10 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.

4.7.10.1 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.

4.7.10.2 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.

4.7.10.3 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.

4.7.10.4 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.

4.7.10.5 Другое

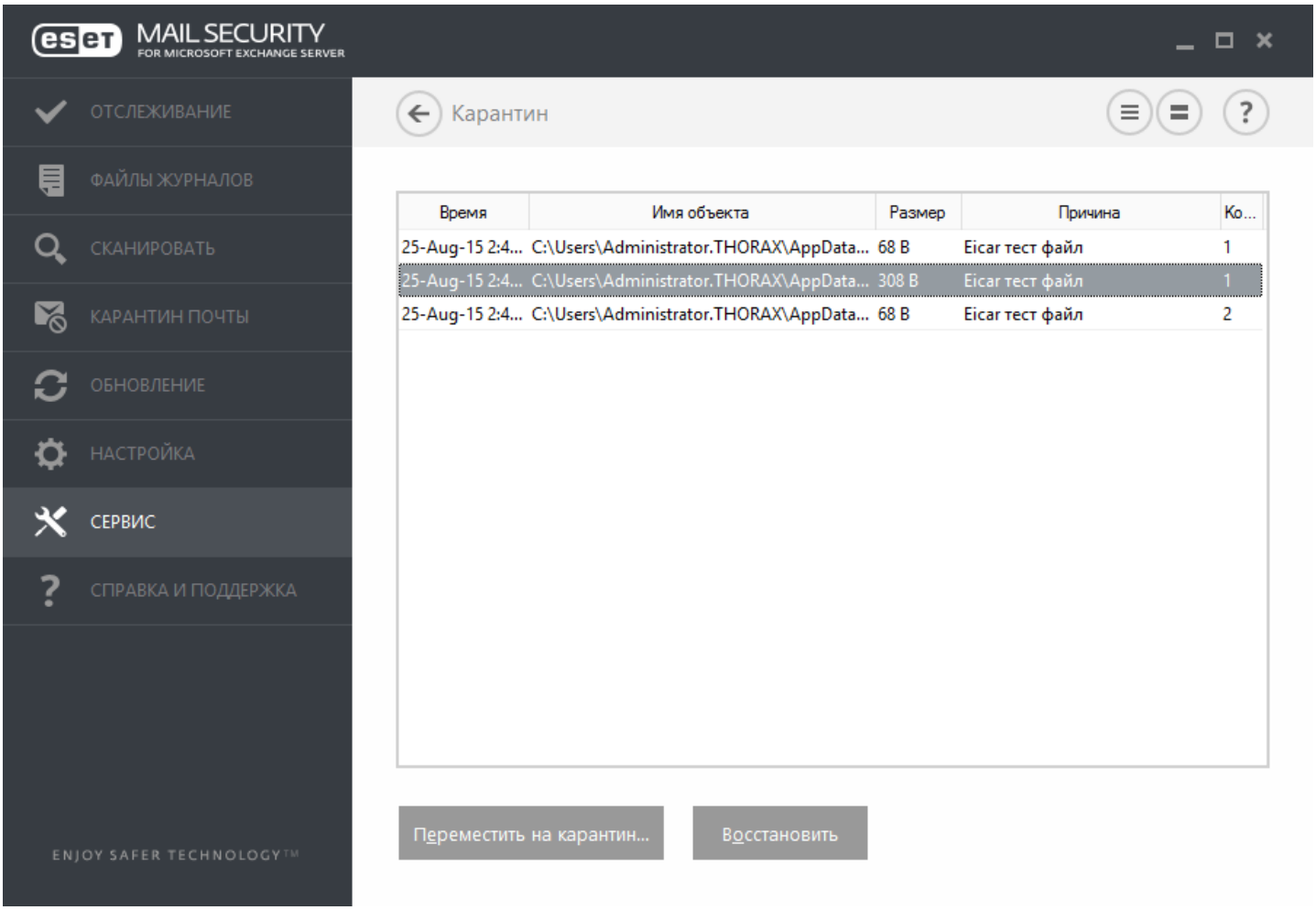
Эту форму следует использовать, если файл невозможно отнести к категории **Подозрительный файл** или **Ложное срабатывание**.

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

4.7.11 Карантин

Карантин предназначен в первую очередь для изоляции и безопасного хранения зараженных файлов. Файлы следует помещать на карантин, если их нельзя вылечить или безопасно удалить либо если они отнесены программой ESET Mail 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 Mail 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 помещения файлов на карантин можно воспользоваться также контекстным меню. Щелкните правой кнопкой мыши в окне **Карантин** и выберите 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 по нужному файлу 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) и изолирован, передайте файл в вирусную лабораторию ESET. Чтобы отправить файл из карантина, щелкните его правой кнопкой мыши и выберите пункт **Передать на анализ**.

4.8 Справка и поддержка

В ESET Mail Security есть средства для устранения проблем и сведения по поддержке, с помощью которых можно 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 Mail 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

- **Отправить запрос в службу поддержки клиентов**: если не удается найти ответ на вопрос, можно, воспользовавшись формой на веб-сайте компании ESET, обратиться в службу поддержки клиентов.

Средства поддержки

- **Энциклопедия угроз**: ссылка на энциклопедию угроз ESET, которая содержит информацию об опасностях и симптомах разных видов заражений.
- **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 Mail Security**: на экран выводится информация о вашей копии программы ESET Mail Security.
- Управление лицензией: щелкните, чтобы открыть окно активации продукта. Выберите доступный метод активации ESET Mail Security. Дополнительные сведения см. в разделе Активация ESET Mail Security.

4.8.1 Рекомендации

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

Выполнение обновления ESET Mail Security

Активация ESET Mail 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 Mail 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.

4.8.1.1 Выполнение обновления ESET Mail Security

Обновлять ESET Mail Security можно вручную или автоматически. Чтобы запустить обновление, нажмите кнопку **Обновление базы данных сигнатур вирусов**. 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).

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

Для активации ESET Mail 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.
- **Учетная запись администратора безопасности** - учетная запись, созданная на портале администраторов лицензий ESET с учетными данными (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.

Команда **Активировать позже** в ESET Remote Administrator используется в тех случаях, когда компьютер находится в управляемой сети и активацию продукта администратор выполняет удаленно через приложение ESET Remote Administrator. Эту команду можно использовать также тогда, когда активацию клиента требуется выполнить 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, на которого лицензия зарегистрирована в системе лицензирования, можно найти в разделе **О программе** (на панели задач щелкните значок правой кнопкой мыши).

ПРИМЕЧАНИЕ: Приложение ESET Remote Administrator может активировать клиентские компьютеры в автоматическом режиме, используя предоставленные администратором лицензии.

4.8.1.3 Механизм подсчета почтовых ящиков решением ESET Mail Security

Подробности см. в статье нашей базы знаний.

4.8.1.4 Создание задачи в планировщике

Чтобы создать новую задачу, последовательно выберите элементы **Сервис** > **Планировщик**, а затем нажмите кнопку **Добавить задачу** или щелкните правой кнопкой мыши и в контекстном меню выберите команду **Добавить**. Запланировать можно пять типов задач.

- **Запуск внешнего приложения** - планирование выполнения внешнего приложения.
- **Обслуживание журналов**: в файлах журналов содержатся также остатки удаленных записей. Для эффективной работы эта задача регулярно оптимизирует записи в файлах журналов.
- **Проверка файлов, исполняемых при запуске 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 программные модули и база данных сигнатур вирусов.

Поскольку **Обновление** — одна из самых часто используемых запланированных задач, ниже описан порядок добавления задачи обновления.

В раскрывающемся меню **Запланированная задача** выберите пункт **Обновление**. Введите имя задачи в поле **Имя задачи** и нажмите кнопку **Далее**. Выберите частоту выполнения задачи. Доступны указанные ниже варианты. **Однократно**, **Многократно**, **Ежедневно**, **Еженедельно** и **При определенных условиях.** Чтобы свести к минимуму потребление системных ресурсов, когда ноутбук работает от аккумулятора, установите флажок **Пропускать задачу, если устройство работает от аккумулятора**. Задача будет выполняться в день и время, указанные в полях области **Выполнение задачи**. Затем укажите, какое действие следует предпринимать, если задача не может быть выполнена в установленное время. Доступны указанные ниже варианты.

- **В следующее запланированное время**
- **Как можно скорее**
- **Незамедлительно, если с момента последнего запуска прошло больше времени, чем указано** (интервал можно указать, настроив с помощью ползунка полосы прокрутки параметр «Время с момента последнего запуска»).

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

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

4.8.1.5 Планирование задачи сканирования (каждые 24 часа)

Чтобы запланировать регулярную задачу, перейдите в раздел **ESET Mail Security** > **Сервис** > **Планировщик**. Ниже приведено краткое описание процедуры планирования задачи, которая будет сканировать локальные диски каждые 24 часа.

Чтобы запланировать задачу сканирования, выполните следующие действия:

1. В главном окне планировщика щелкните элемент **Добавить**.
2. В раскрывающемся меню выберите **Сканирование компьютера по требованию**.
3. Введите имя задачи и выберите вариант **Многократно**.
4. Укажите, что задача должна запускаться каждые 24 часа (1440 минут).
5. Выберите действие, которое будет выполняться, если по какой-либо причине не удается выполнить запланированную задачу.
6. Просмотрите сводную информацию о запланированной задаче и нажмите кнопку **Готово**.
7. В раскрывающемся меню **Объекты** выберите пункт «Жесткие диски».
8. Для применения задачи нажмите кнопку **Готово**.

4.8.1.6 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 Mail 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.

4.8.2 Отправка запроса в службу поддержки клиентов

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

При отправке веб-формы будут отправлены и данные о конфигурации системы. Установите флажок **Всегда отправлять эти сведения**, если для процесса нужно запомнить это действие. Чтобы отправить форму, не отправляя данные, щелкните элемент **Не отправлять данные**. В этом случае для обращения в службу поддержки ESET следует использовать соответствующую онлайн-форму.

Настроить этот параметр можно и по-другому: последовательно щелкните элементы **Дополнительные настройки** > **Сервис** > **Диагностика** > **Служба поддержки клиентов**.

ПРИМЕЧАНИЕ. Если вы решили отправить данные о системе, нужно заполнить и отправить веб-форму. В

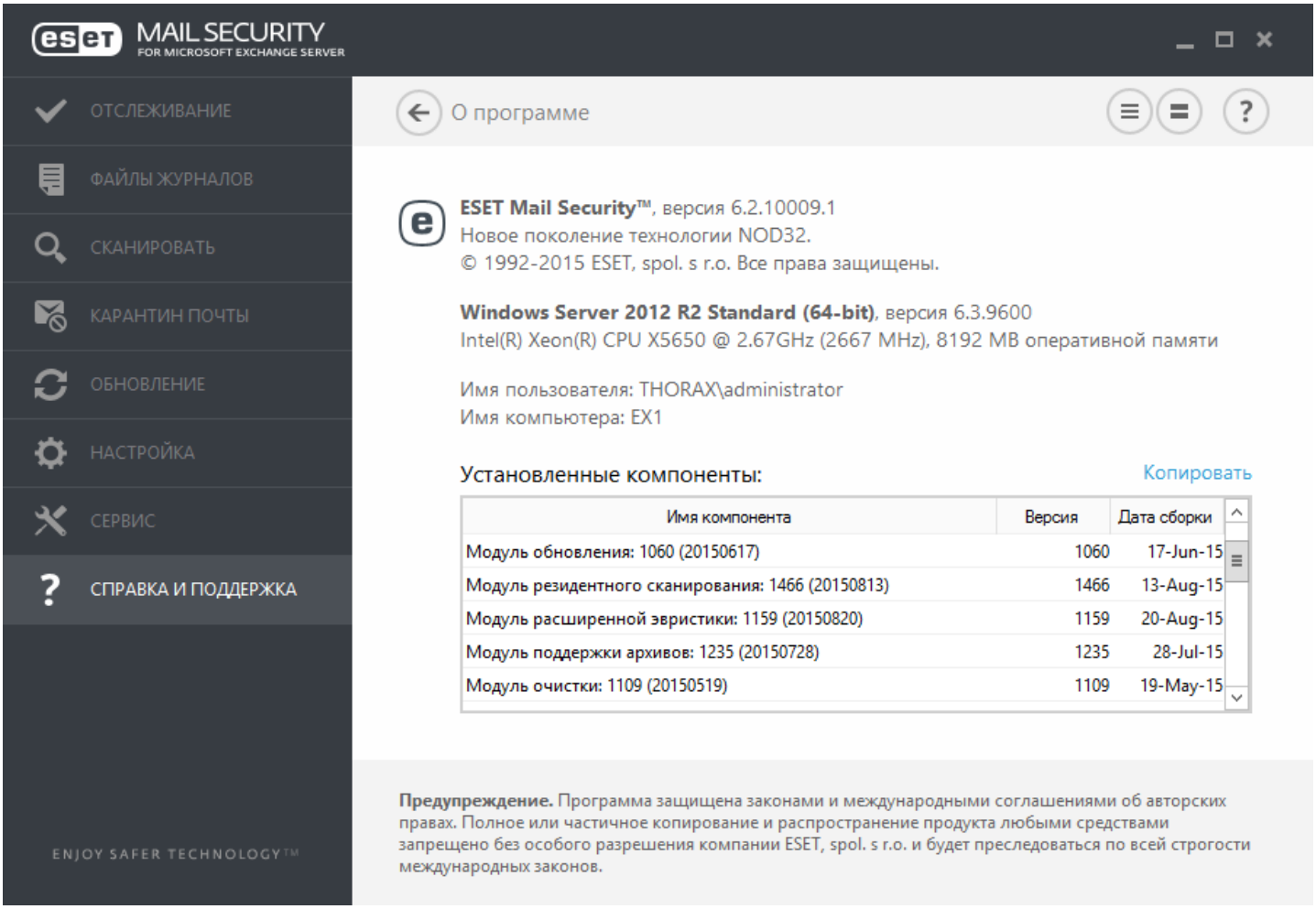
противном случае запрос создан не будет и данные о системе будут потеряны.

4.8.3 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.

4.8.4 О программе ESET Mail Security

В этом окне приводятся сведения об установленной версии ESET Mail Security и перечень установленных программных модулей. В верхней части окна содержится информация об операционной системе и системных ресурсах.



Чтобы скопировать информацию о модулях (**Установленные компоненты**) в буфер обмена, используйте команду **Копировать**. Это может быть полезно при устранении проблем или обращении в службу технической поддержки.

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

Для активации ESET Mail 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.
- **Учетная запись администратора безопасности** - учетная запись, созданная на портале администраторов лицензий ESET с учетными данными (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.

Команда **Активировать позже** в ESET Remote Administrator используется в тех случаях, когда компьютер находится в управляемой сети и активацию продукта администратор выполняет удаленно через приложение ESET Remote Administrator. Эту команду можно использовать также тогда, когда активацию клиента требуется выполнить 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, на которого лицензия зарегистрирована в системе лицензирования, можно найти в разделе **О программе** (на панели задач щелкните значок правой кнопкой мыши).

ПРИМЕЧАНИЕ: Приложение ESET Remote Administrator может активировать клиентские компьютеры в автоматическом режиме, используя предоставленные администратором лицензии.

4.8.5.1 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.

4.8.5.2 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.

4.8.5.3 Сбой активации

Не удалось выполнить активацию ESET Mail 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**.

4.8.5.4 Лицензия

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

4.8.5.5 Ход выполнения активации

Выполняется активация продукта ESET Mail Security. Пожалуйста, подождите. Эта процедура может занять некоторое время.

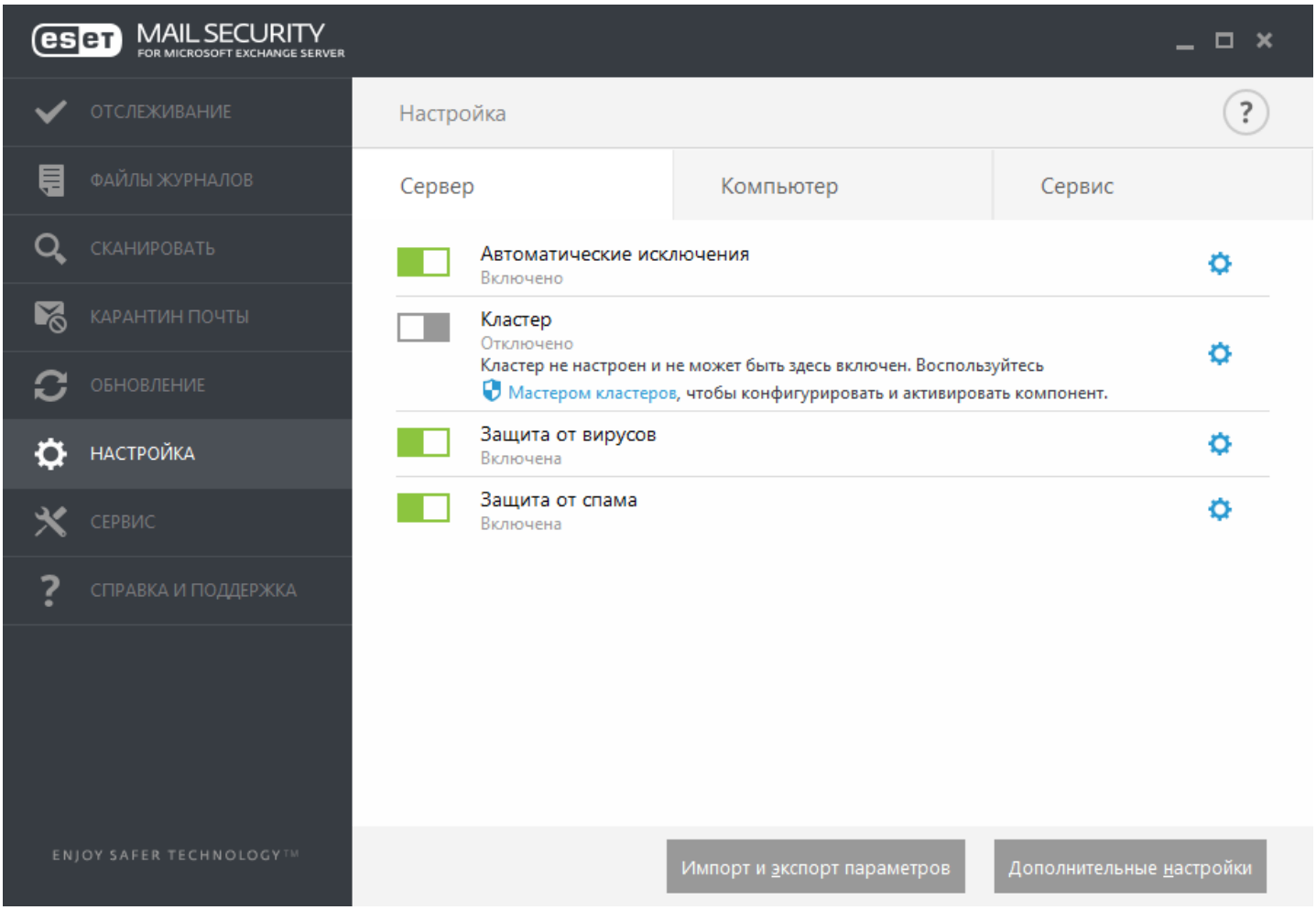
4.8.5.6 Активация выполнена

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

5. Работа с ESET Mail Security

Меню **Настройки** состоит из следующих разделов (между ними можно переключаться, используя вкладки):

- 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 подробные 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.

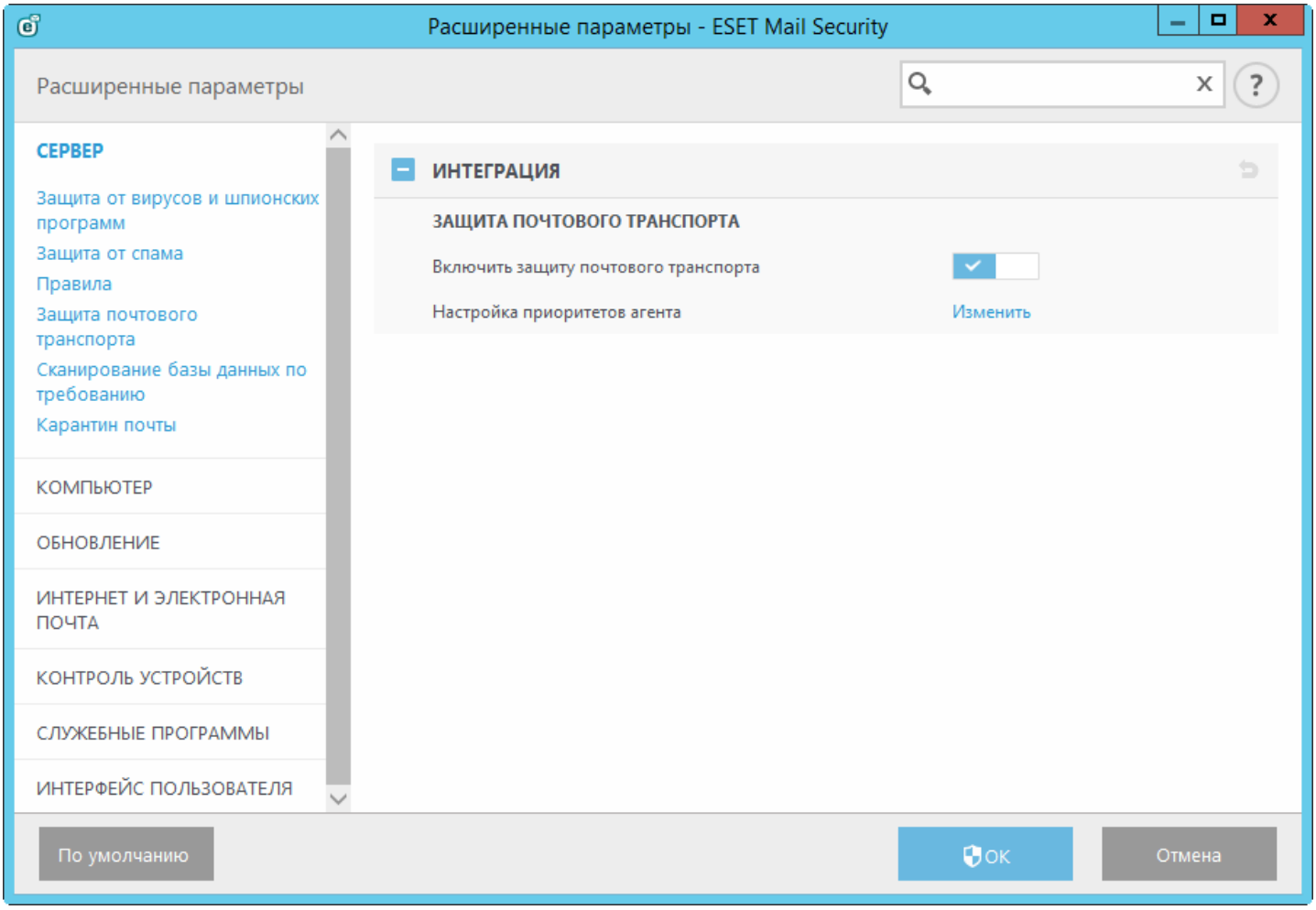
5.1 Сервер

ESET Mail Security обеспечивает значительный уровень защиты сервера Microsoft Exchange Server с помощью следующих функций:

- защита от вирусов и шпионских программ,
- защита от спама,
- правила,
- защита почтового транспорта (Exchange Server 2007, 2010, 2013),
- защита базы данных почтовых ящиков (Exchange Server 2003, 2007, 2010),
- сканирование базы данных по требованию (Exchange Server 2007, 2010, 2013),
- карантин (параметры типа карантина почты).

В разделе «Дополнительные настройки» можно включить или отключить интеграцию защиты базы данных почтовых ящиков и защиты почтового транспорта, а также изменить приоритет агентов.

ПРИМЕЧАНИЕ. Если вы работаете в системе Microsoft Exchange Server 2007 или 2010, вы можете воспользоваться защитой базы данных почтовых ящиков или сканированием базы данных по требованию. При этом данные типы защиты не могут быть активными одновременно. Если выбрать сканирование базы данных по требованию, то понадобится отключить интеграцию защиты базы данных почтовых ящиков. В противном случае сканирование базы данных по требованию будет недоступно.



5.1.1 Настройка приоритетов агента

В меню **Настройка приоритетов агента** вы можете задать приоритет, на основании которого после запуска сервера Microsoft Exchange Server будут активироваться агенты ESET Mail Security. Приоритет определяется числовым значением. Чем ниже значение, тем выше приоритет. Это относится к Microsoft Exchange 2003.

Нажмите кнопку **Изменить**, чтобы перейти к настройке приоритета агентов. Так вы можете задать приоритет, на основании которого после запуска Microsoft Exchange Server будут активироваться агенты ESET Mail Security.

- **Изменить**: ввод номера, определяющего приоритет выбранного агента, вручную.
- **Переместить вверх**: повышение приоритета выделенного агента путем перемещения его вверх в списке агентов.
- **Переместить вниз**: понижение приоритета выделенного агента путем перемещения его вниз в списке агентов.

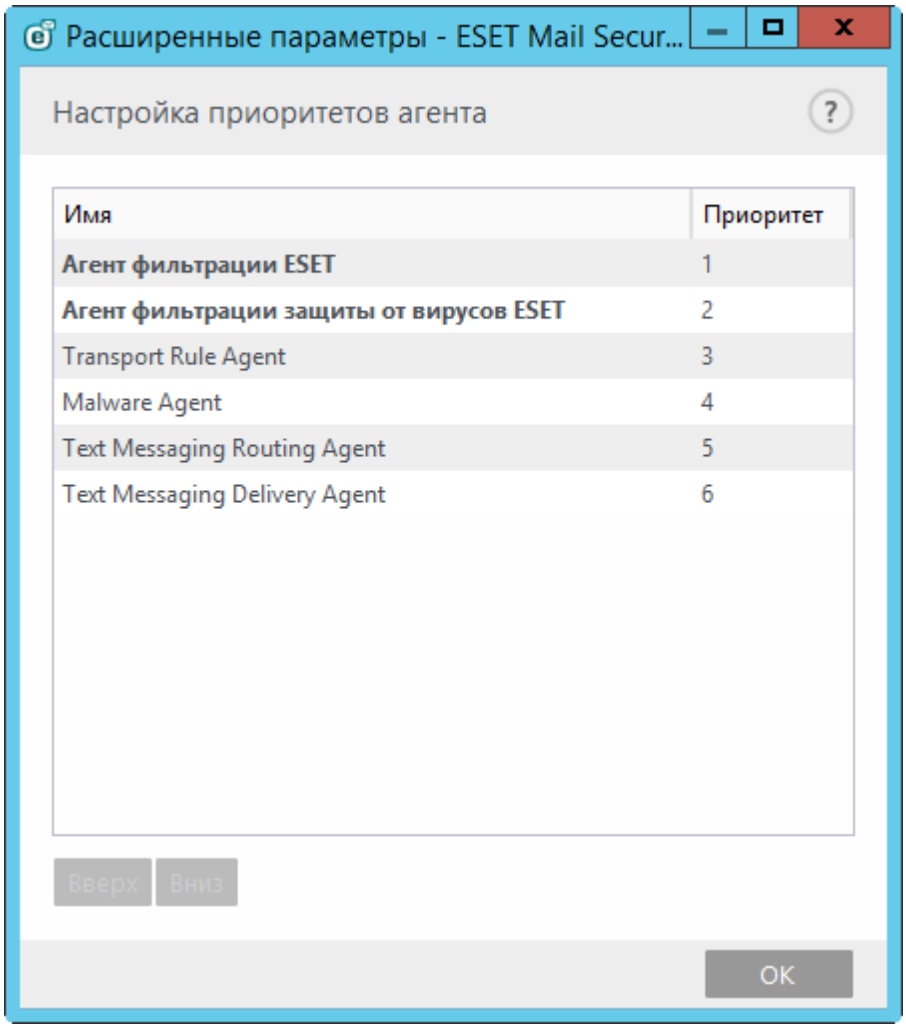
С помощью Microsoft Exchange Server 2003 вы можете задать приоритет агента по-другому, используя вкладки для указания конца данных (EOD) и получателя (RCPT).

5.1.1.1 Изменение приоритета

Если вы работаете с Microsoft Exchange Server 2003, вы можете задать число вручную, чтобы изменить **приоритет агента транспорта**. Чтобы изменить приоритет, измените число в текстовом поле или используйте стрелки вверх и вниз. Чем ниже значение, тем выше приоритет.

5.1.2 Настройка приоритетов агента

В меню **Настройка приоритетов агента** вы можете задать приоритет, на основании которого после запуска сервера Microsoft Exchange Server будут активироваться агенты ESET Mail Security. Это относится к Microsoft Exchange, начиная с версии 2007.



- **Переместить вверх**: повышение приоритета выделенного агента путем перемещения его вверх в списке агентов.
- **Переместить вниз**: понижение приоритета выделенного агента путем перемещения его вниз в списке агентов.

5.1.3 Защита от вирусов и шпионских программ

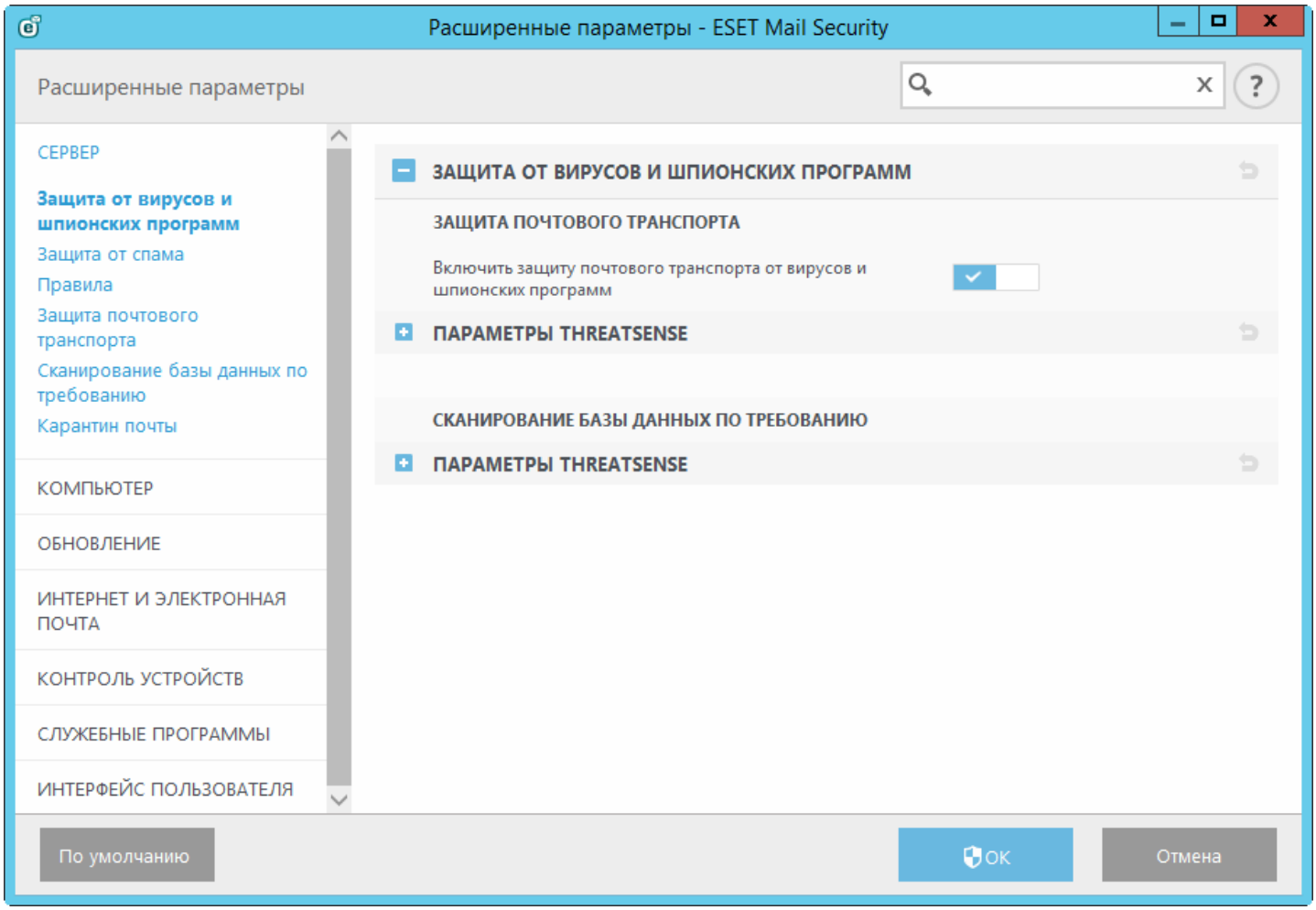
В этом разделе можно настроить параметры **защиты от вирусов и шпионских программ** для вашего почтового сервера.

ВНИМАНИЕ! Защиту почтового транспорта обеспечивает агент транспорта, и доступна эта функция только для Microsoft Exchange Server (начиная с версии 2007), при этом ваш сервер Exchange Server должен иметь роль пограничного транспортного сервера или транспортного сервера-концентратора. Сказанное относится также к одиночному серверу, на котором активированы несколько ролей Exchange Server и который установлен на одном компьютере (если среди этих ролей есть роль пограничного сервера или транспортного сервера-концентратора).

Защита почтового транспорта

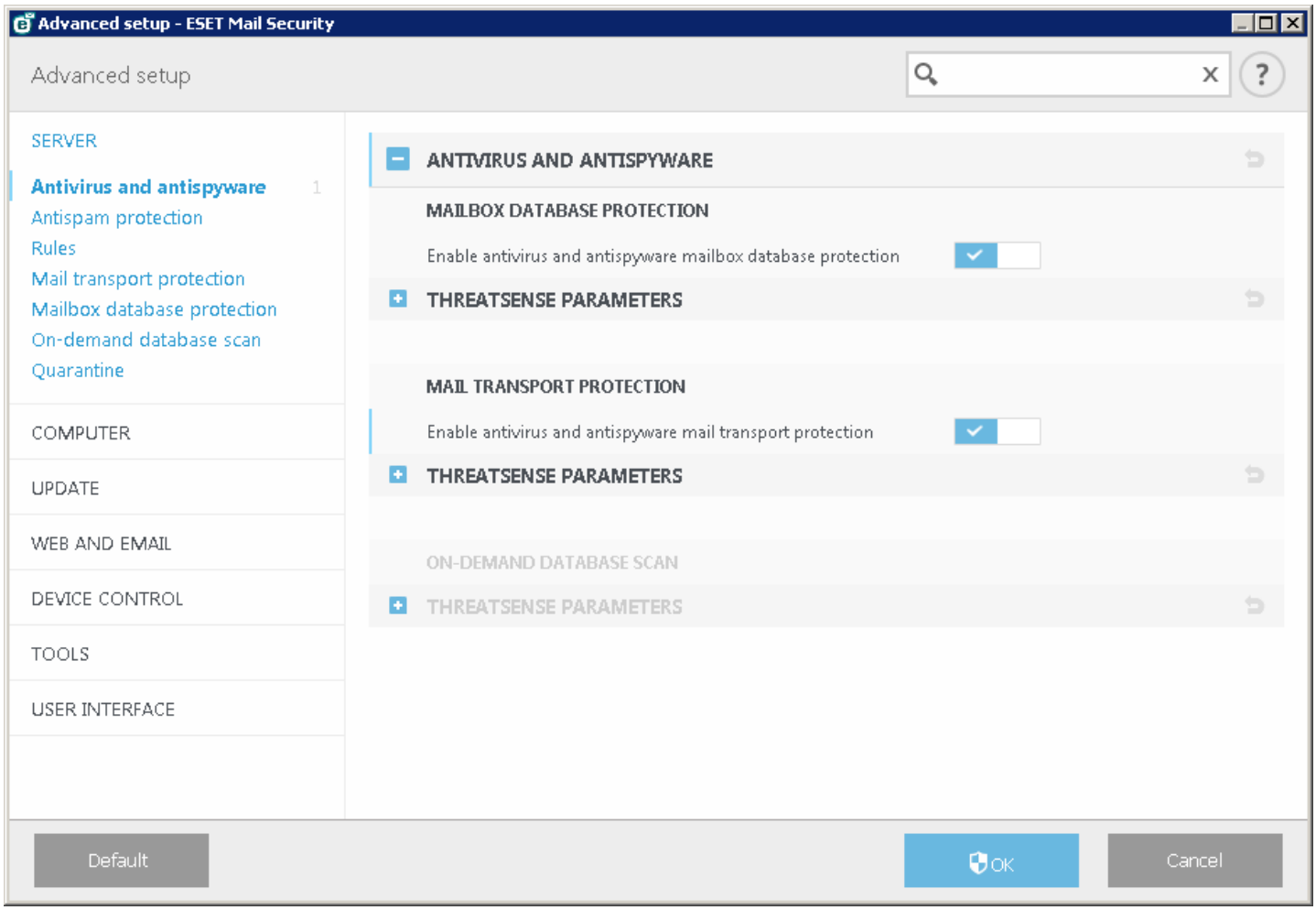
Если снять флажок **Включить защиту почтового транспорта от вирусов и шпионских программ**, подключаемый модуль ESET Mail Security для сервера Exchange не будет выгружен из процесса Microsoft Exchange Server. Он будет просто пропускать через себя сообщения, не сканируя их на наличие вирусов на транспортном уровне. Сообщения на уровне базы данных так и будут сканироваться на наличие вирусов и спама. Кроме того, будут

применяться правила.



Защита базы данных почтовых ящиков

Если снять флажок **Включить защиту базы данных почтовых ящиков от вирусов и шпионских программ**, подключаемый модуль ESET Mail Security для сервера Exchange не будет выгружен из процесса Microsoft Exchange Server. Он будет просто пропускать через себя сообщения, не сканируя их на наличие вирусов на уровне базы данных. Сообщения на уровне базы данных так и будут сканироваться на наличие вирусов и спама на транспортном уровне. Кроме того, к ним будут применяться правила.



5.1.4 Защита от спама

По умолчанию защита от спама для почтового сервера включена. Чтобы отключить ее, щелкните **Включить защиту от спама**.

Функция **Использовать «белые» списки с сервера Exchange Server для автоматического обхода защиты от спама** позволяет ESET Mail Security использовать определенные «белые» списки Exchange. Если эта функция включена, то принимаются во внимание следующие факторы.

- IP-адрес сервера находится в списке разрешенных IP-адресов сервера Exchange Server.
- В почтовом ящике получателя сообщения установлен флажок «Обойти защиту от спама».
- Адрес отправителя указан в списке «Надежные отправители» получателя сообщений (в среде сервера Exchange Server должна быть настроена синхронизация со списком надежных отправителей, включая объединение списков надежных отправителей).

Если какое-либо из вышеуказанных условий применяется ко входящему сообщению, проверка на наличие спама пропускается для этого сообщения и, следовательно, сообщение не оценивается как СПАМ и доставляется в почтовый ящик получателя.

Параметр **Принимать флажки обхода защиты от спама, установленные для сеанса SMTP** используется, когда выполнена проверка подлинности сеансов SMTP между серверами Exchange, на которых задан параметр обхода защиты от спама. Например, когда используется пограничный сервер и сервер-концентратор, нет потребности в сканировании трафика между этими двумя серверами на наличие спама. Параметр **Принимать флажки обхода защиты от спама, установленные для сеанса SMTP** включен по умолчанию и применяется, когда для сеанса SMTP на сервере Exchange Server установлен флажок обхода защиты от спама. Если отключить параметр **Принимать флажки обхода защиты от спама, установленные для сеанса SMTP**, решение ESET Mail Security сканирует сеанс SMTP на наличие спама вне зависимости от того, включен ли параметр обхода защиты от спама на сервере Exchange.

ПРИМЕЧАНИЕ.: Необходимо регулярное обновление базы данных модуля защиты от спама с целью

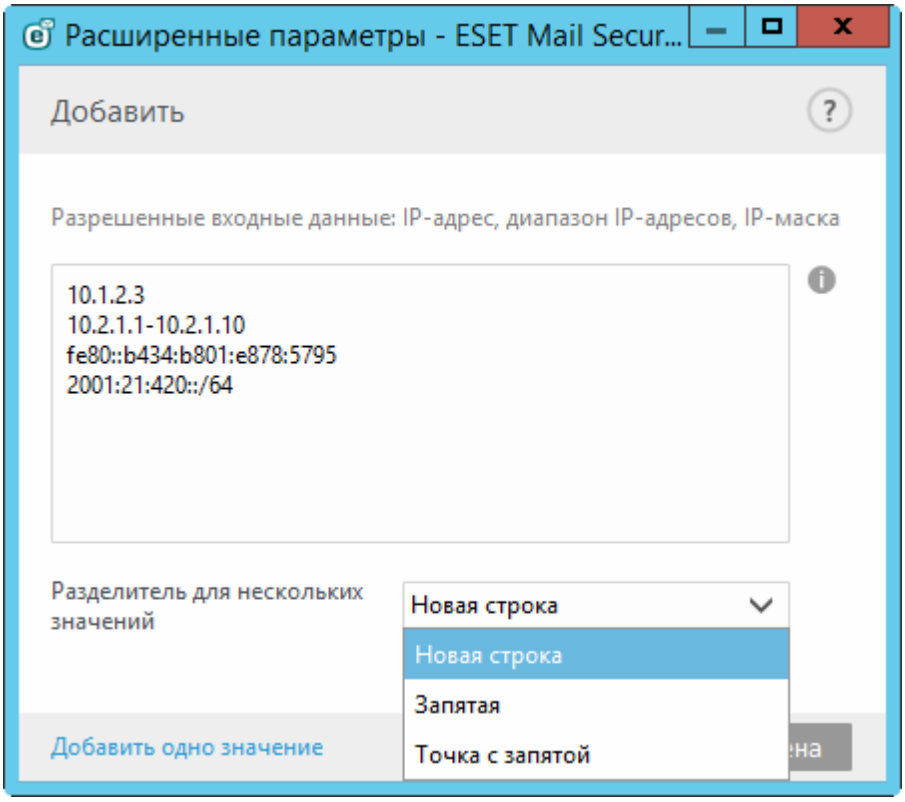
обеспечения оптимальной защиты от спама. Чтобы база данных защиты от спама обновлялась регулярно, обеспечьте для ESET Mail Security доступ к правильным IP-адресам на нужных портах. Дополнительные сведения о том, какие IP-адреса и порты следует включать для файервола сторонних разработчиков, см. в этой статье базы знаний.

5.1.4.1 Фильтрация и проверка

Вы можете настраивать списки **Разрешено**, **Заблокировано** и **Проигнорировано**, указывая такие критерии, как IP-адрес или диапазон, имя домена и т. д. Чтобы добавить, изменить или удалить критерий, щелкните элемент **Изменить**, относящийся к списку, которым вы хотите управлять.

- **Список разрешенных IP-адресов** — автоматическое добавление в «белый» список сообщений электронной почты, приходящих с указанных IP-адресов.
- **Список заблокированных IP-адресов** — автоматическая блокировка сообщений электронной почты, приходящих с указанных IP-адресов.
- **Список игнорируемых IP-адресов** — список IP-адресов, которые будут игнорироваться во время классификации.
- **Список блокируемых доменов в теле сообщения** — блокировка сообщений электронной почты, которые содержат указанный домен в теле сообщения.
- **Список игнорируемых доменов в теле сообщения** — указанные домены в теле сообщения будут игнорироваться во время классификации.
- **Список блокируемых IP-адресов в теле сообщения** — блокировка сообщений электронной почты, которые содержат указанный IP-адрес в теле сообщения.
- **Список игнорируемых IP-адресов в теле сообщения** — указанные IP-адреса в теле сообщения будут игнорироваться во время классификации.
- **Список разрешенных отправителей** — добавление в «белый» список сообщений электронной почты от указанного отправителя.
- **Список заблокированных отправителей** — блокировка сообщений электронной почты, приходящих от указанного отправителя.
- **Список утвержденных доменов и IP-адресов** — добавление в «белый» список сообщений электронной почты, приходящих с IP-адресов, которые получаются в результате разрешения указанных в списке доменов.
- **Список заблокированных доменов и IP-адресов** — блокировка сообщений электронной почты, приходящих с IP-адресов, которые получаются в результате разрешения указанных в списке доменов.
- **Список игнорируемых доменов и IP-адресов** — список доменов, в результате разрешения которых получаются IP-адреса, которые, в свою очередь, не будут проверяться во время классификации.
- **Список заблокированных кодировок** — блокировка сообщений электронной почты, созданных с применением указанных кодировок.
- **Список заблокированных стран** — блокировка сообщений электронной почты из указанных стран.

ПРИМЕЧАНИЕ.: Если нужно добавить несколько записей одновременно, щелкните **Добавить несколько значений** во всплывающем окне «Добавление» и выберите разделитель, который нужно использовать: **Новая строка**, **Запятая** или **Точка с запятой**. Например:



5.1.4.2 Дополнительные параметры

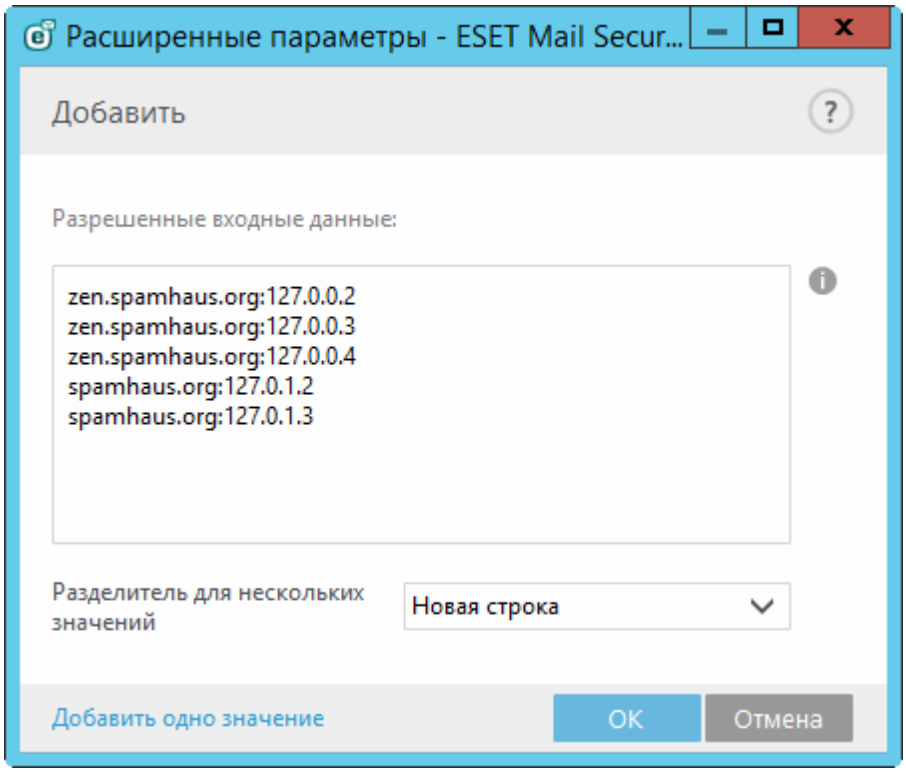
Эти параметры обеспечивают проверку сообщений внешними серверами (**RBL** — «черный» список реального времени, **DNSBL** — «черный» список на основе DNS) в соответствии с заданными критериями.

Максимальное количество проверенных адресов из заголовков «Получено». Вы можете ограничить количество IP-адресов, которые проверяет модуль защиты от спама. Это касается IP-адресов, включенных в заголовки `Received: from`. Значение по умолчанию — это 0. Оно означает, что ограничений нет.

Проверьте адрес отправителя по «черному» списку конечных пользователей. Электронные письма, отправленные не с почтовых серверов (то есть с компьютеров, которые не числятся почтовыми серверами), проверяются на предмет наличия их отправителя в черном списке. Этот параметр включен по умолчанию. Если необходимо, его можно выключить, при этом, однако, сообщения, отправленные не с почтовых серверов, не будут проверяться на предмет наличия их отправителя в черном списке.

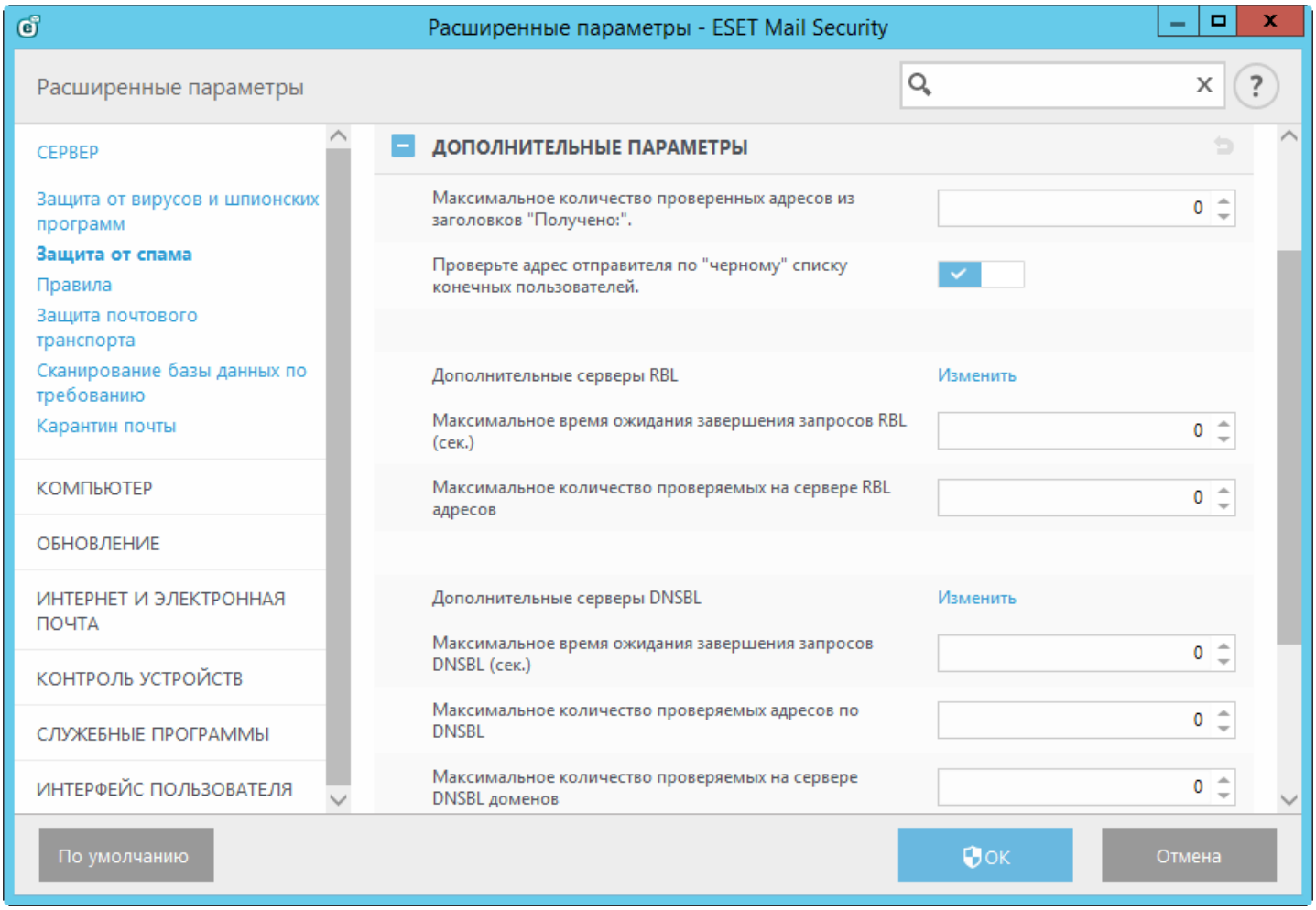
Дополнительные серверы RBL: это список серверов реального времени типа «черная дыра», которым отправляются запросы при анализе сообщений.

ПРИМЕЧАНИЕ.: При добавлении дополнительных серверов RBL введите имя домена сервера с кодом возврата в виде `сервер:ответ` (например, `zen.spamhaus.org:127.0.0.4`). Кроме того, добавлять каждое имя сервера и каждый код возврата нужно отдельно, чтобы образовался полный список. Щелкните **Добавить несколько значений** во всплывающем окне «Добавление», чтобы указать все имена сервера с их кодами возврата. Записи должны быть похожими на этот пример. Фактические имена узлов серверов RBL и коды возврата могут отличаться:



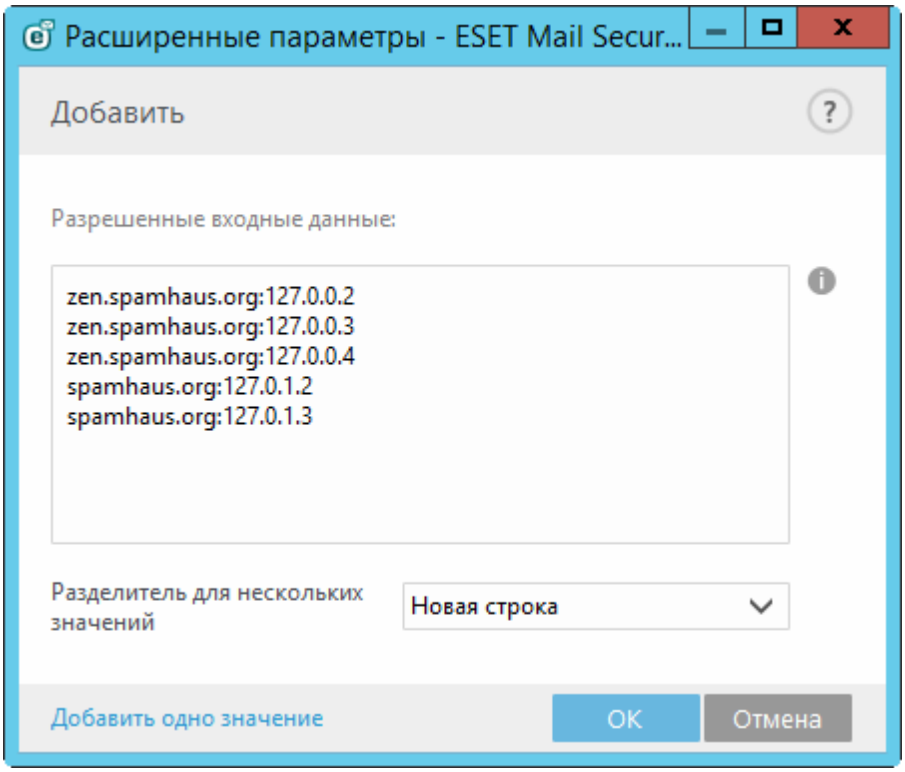
Максимальное время ожидания завершения запросов RBL (сек.): с помощью этого параметра можно указать максимальное время выполнения запроса RBL. Ответы RBL используются только от тех серверов RBL, которые ответили вовремя. Если задано значение «0», то время ожидания никогда не начинается.

Максимальное количество проверяемых на сервере RBL адресов: этот параметр позволяет ограничить количество IP-адресов, поиск которых выполняется на сервере RBL. Обратите внимание, что общее количество запросов RBL соответствует произведению числа IP-адресов в заголовках полученных сообщений (до максимального количества IP-адресов, указанных для проверки RBL), умноженному на количество серверов RBL, указанное в списке RBL. Если установлено значение «0», проверяется неограниченное количество полученных заголовков. Обратите внимание, что IP-адреса, которые присутствуют в списке пропускаемых IP-адресов, не учитываются при подсчете ограничения IP-адресов RBL.



Дополнительные серверы DNSBL: это серверы черного списка DNS, к которым отправляются запросы на домены и IP-адреса, извлеченные из тела сообщения.

ПРИМЕЧАНИЕ.: При добавлении дополнительных серверов DNSBL введите имя домена сервера с кодом возврата в виде `сервер:ответ` (например, `zen.spamhaus.org:127.0.0.4`). Кроме того, добавлять каждое имя сервера и каждый код возврата нужно отдельно, чтобы образовался полный список. Щелкните **Добавить несколько значений** во всплывающем окне «Добавление», чтобы указать все имена сервера с их кодами возврата. Записи должны быть похожими на этот пример. Фактические имена узлов серверов DNSBL и коды возврата могут отличаться:



Максимальное время ожидания завершения запросов DNSBL (сек.): позволяет задать максимальное время ожидания для всех запросов DNSBL.

Максимальное количество проверяемых адресов по DNSBL: этот параметр позволяет ограничить количество IP-адресов, поиск которых выполняется на сервере черного списка DNS.

Максимальное количество проверяемых на сервере DNSBL доменов: этот параметр позволяет ограничить количество IP-адресов, поиск которых выполняется на сервере черного списка DNS.

Включить ведение журнала диагностики для модуля: запись подробной информации о модуле защиты от спама в файлы журналов в целях диагностики.

Максимальный размер сканируемого сообщения (КБ): сообщения, размер которых превышает указанное здесь значение, не сканируются на наличие спама. Их не сканирует модуль защиты от спама. Поведение:

Если в качестве максимального размера сканируемого сообщения задать 0 = сканирование без ограничений.

Если в качестве максимального размера задать 1 - 12288 = 12288

Если в качестве максимального размера задать число больше 12 288 = заданное значение.

Рекомендуемое минимальное значение — 100 КБ.

5.1.4.3 Параметры работы с «серыми» списками

Параметр **Включить работу с «серыми» списками** активирует функцию, которая защищает пользователей от спама за счет следующего метода. Агент транспорта отправляет значение ответа «временное отклонение» по SMTP (по умолчанию 451/4.7.1) на каждое полученное от неизвестного отправителя сообщение. Нормальный сервер попробует повторить отправку сообщения через некоторое время. Как правило, рассылающие спам серверы не пытаются повторно отправить сообщения, так как они обычно обрабатывают тысячи адресов электронной почты и не тратят время на повторную отправку. Работа с «серыми» списками — это дополнительная мера защиты от спама, которая не влияет на возможности модуля защиты от спама по оценке нежелательности.

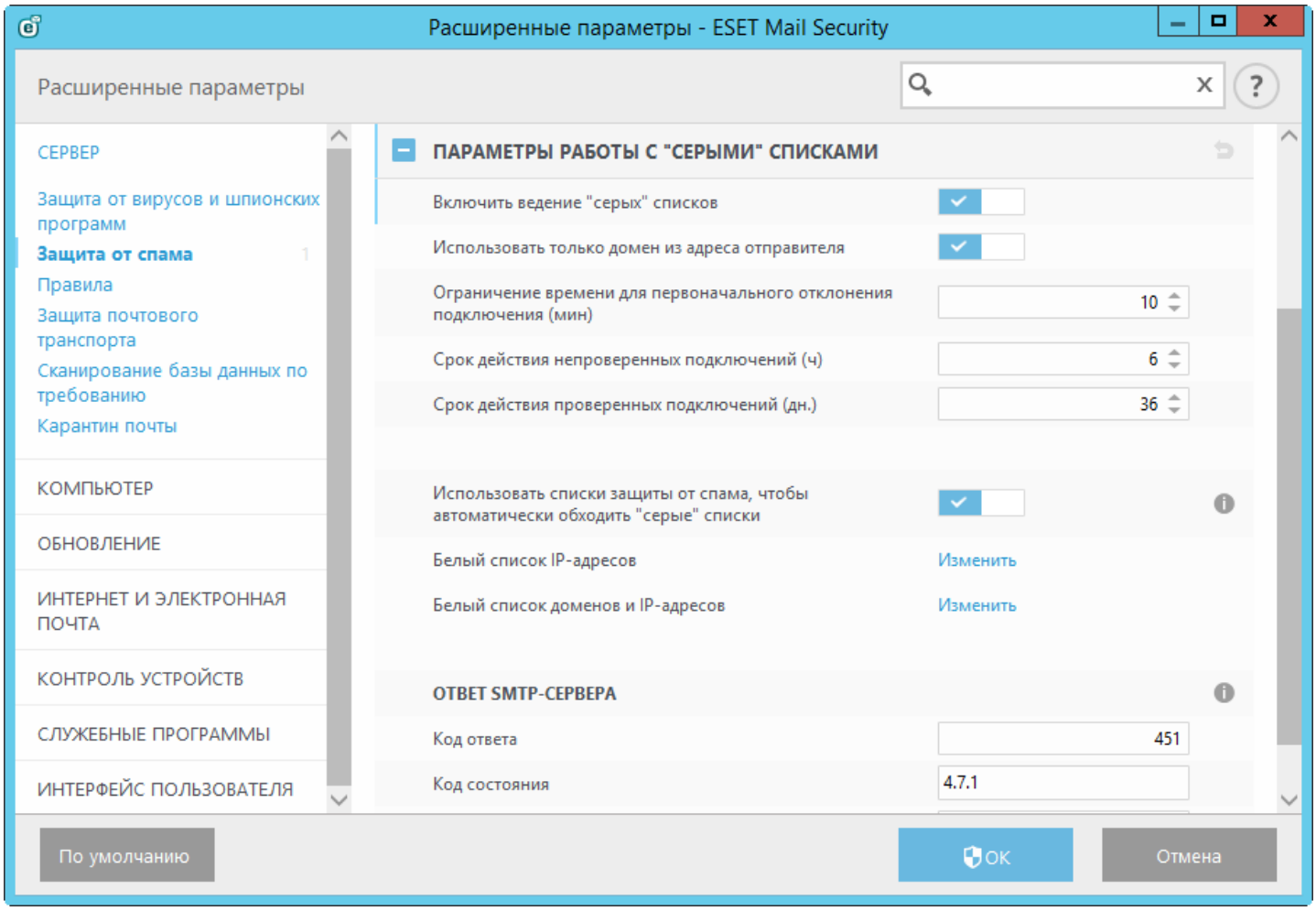
При оценке источника сообщения этим методом учитываются списки **Список разрешенных IP-адресов**, **Список игнорируемых IP-адресов**, **Надежные отправители** и **Разрешить IP** на сервере Exchange и параметры AntispamBypass для почтового ящика получателя. Сообщения электронной почты, поступающие с IP-адресов/от отправителей из этих списков, а также сообщения, доставляемые в почтовый ящик, у которого активирован параметр AntispamBypass, будут пропускаться методом обнаружения путем работы с «серыми» списками.

Использовать только домен из адреса отправителя: имя получателя в адресе электронной почты игнорируется, и учитывается только домен.

Ограничение времени для первоначального отклонения подключения (мин): когда сообщение доставляется впервые и временно отклоняется, этот параметр определяет период времени, в течение которого сообщение всегда будет отклоняться (с момента первого отклонения). По окончании заданного периода времени это сообщение будет успешно получено. Минимальное значение равняется 1 минуте.

Срок действия непроверенных подключений (ч):: этот параметр определяет минимальный период времени, в течение которого будут храниться данные трех параметров. Нормальный сервер должен повторить отправку нужного сообщения до окончания этого периода. Данное значение должно быть больше значения параметра **Ограничение времени для первоначального отклонения подключения**.

Срок действия проверенных подключений (дн.): минимальное количество дней, в течение которого хранится информация трех параметров. В течение этого времени электронная почта от конкретного отправителя будет получаться без какой-либо задержки. Это значение должно быть больше значения параметра **Срок действия непроверенных подключений**.



Ответ SMTP-сервера: вы можете (для временно отклоненных подключений) указать **код ответа**, **код состояния** и **сообщение с ответом**. Эти сведения определяют ответ о временном отклонении, отправляемый SMTP-серверу, если сообщение отклоняется.

Пример отправляемого по SMTP ответного сообщения об отклонении

Код ответа	Код состояния	Сообщение с ответом
451	4.7.1	Requested action aborted: (Запрошенное действие прервано:) local error in processing (локальная ошибка при обработке)

Предупреждение. Неверный синтаксис кодов ответа по SMTP может привести к некорректному функционированию защиты путем работы с «серыми» списками. В результате клиентам могут доставляться нежелательные сообщения или же сообщения могут не доставляться совсем.

ПРИМЕЧАНИЕ. Также можно использовать системные переменные при настройке ответа отклонения по SMTP.

5.1.5 Правила

Пункт меню **Правила** позволяет администраторам вручную задавать условия фильтрации электронной почты и действия, которые необходимо выполнить с отфильтрованными сообщениями.

Есть три независимых набора правил. То, какие правила доступны в вашей системе, зависит от того, какая версия Microsoft Exchange Server установлена на сервере с ESET Mail Security.

- Защита базы данных почтовых ящиков: защита этого типа доступна только для Microsoft Exchange Server 2010, 2007 и 2003 с ролью сервера почтовых ящиков (Microsoft Exchange 2010 и 2007) или тылового сервера (Microsoft Exchange 2003). Сканирование этого типа можно выполнить на одиночном сервере, на котором активированы несколько ролей Exchange Server и который установлен на одном компьютере (если среди этих ролей есть роль сервера почтовых ящиков или тылового сервера).
- Защита почтового транспорта: этот метод предоставляется транспортным агентом и доступен только для Microsoft Exchange Server (начиная с версии 2007) с ролью пограничного транспортного сервера или транспортного сервера-концентратора. Сканирование этого типа можно выполнить на одиночном сервере, на котором активированы несколько ролей Exchange Server и который установлен на одном компьютере (если среди этих ролей есть любая из упомянутых выше серверных ролей).
- Сканирование базы данных по требованию: функция, позволяющая выполнить или запланировать сканирование базы данных почтовых ящиков Exchange. Эта функция доступна только для сервера Microsoft Exchange Server (начиная с версии 2007), на котором активирована роль сервера почтовых ящиков или транспортного сервера-концентратора. Сказанное относится также к одиночному серверу, на котором активированы несколько ролей Exchange Server и который установлен на одном компьютере (если среди этих ролей есть любая из упомянутых выше серверных ролей). Дополнительные сведения о ролях в Exchange 2013 см. в разделе Роли Exchange Server 2013.

5.1.5.1 Список правил

Правило состоит из **условий** и **действий**. Когда сообщение электронной почты отвечает всем условиям, по отношению к нему выполняются действия. Иными словами, правила применяются в соответствии с набором условий. Если к правилу относится несколько условий, они сочетаются с помощью логического оператора AND и правило применяется, только если сообщение отвечает всем условиям.

Правила отображаются в окне списка **Правила**. Правила разделены на три категории. Оцениваются они в следующем порядке:

- **правила фильтрации (1);**
- **правила обработки вложений (2);**
- **правила обработки результатов (3).**

Правила одного уровня оцениваются в том порядке, в котором они отображаются в окне правил. Вы можете менять порядок только правил одного уровня. Например, если есть несколько правил фильтрации, то вы можете изменить порядок их применения. Но вы не можете для этого поместить правила обработки

вложений перед правилами фильтрации, и кнопки Вверх/вниз в таком случае будут недоступны. Иными словами, нельзя смешивать правила разных уровней.

Столбец Обращения содержит сведения о том, сколько раз правило успешно применялось. Если снять флажок (слева от имени правила), то соответствующее правило деактивируется до тех пор, пока вы не установите флажок снова.

- **Добавить...** : добавление нового правила.
- **Изменить** : изменение существующего правила.
- **Удалить**: удаление выбранного правила.
- **Переместить вверх**: перемещение выбранного правила вверх по списку.
- **Переместить вниз**: перемещение выбранного правила вниз по списку.
- **Сброс**: сброс счетчика, относящегося к выбранному правилу (столбец «Обращения»).

ПРИМЕЧАНИЕ. Если добавлено новое или изменено существующее правило, автоматически запускается повторное сканирование сообщений с применением новых или измененных правил.

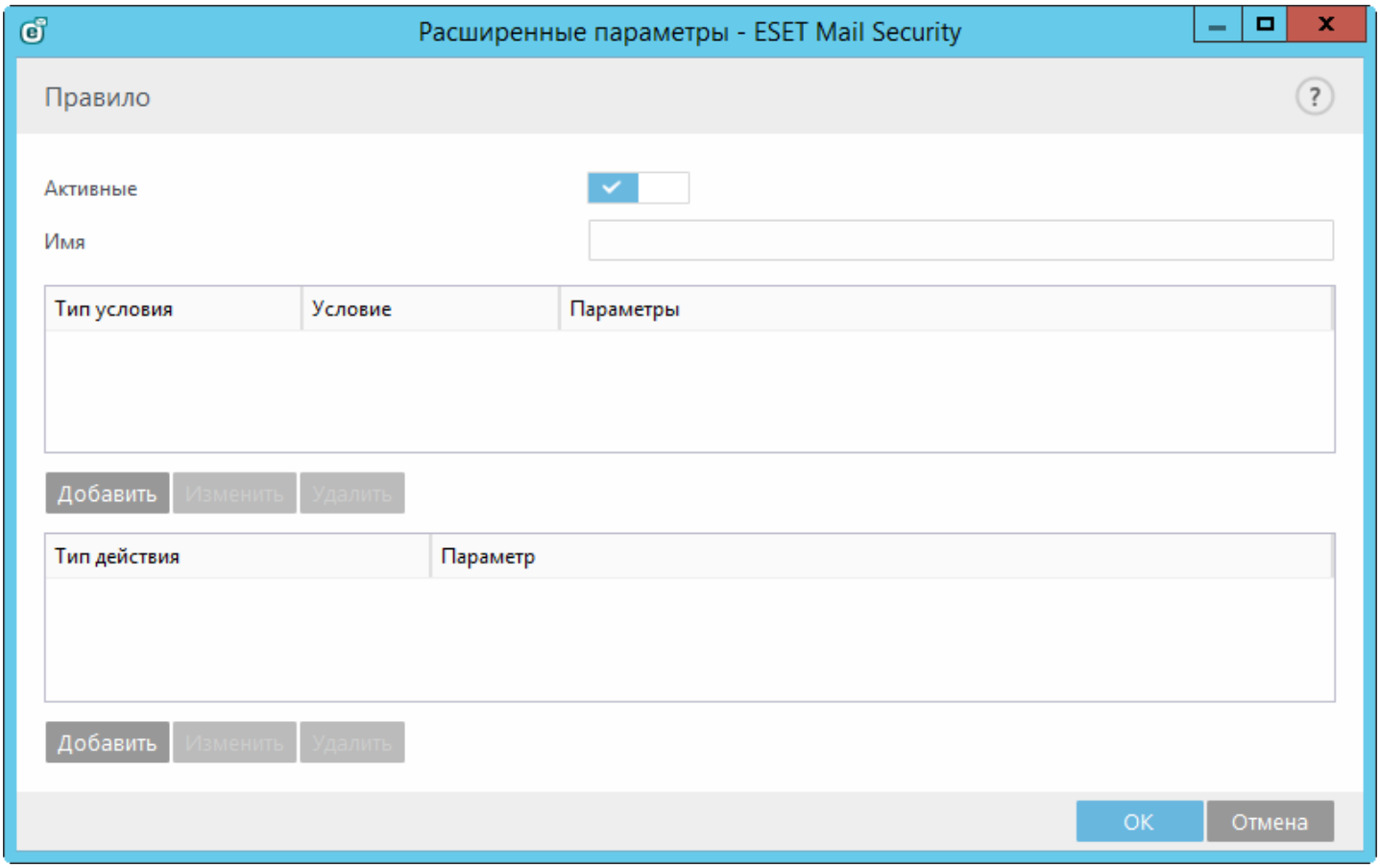
Сообщение проверяется на соответствие правилам, когда его обрабатывает агент транспорта или интерфейс VSAPI. Когда активирован и агент транспорта, и VSAPI, а сообщение отвечает условиям правила, счетчик может быть увеличен для правила на 2 и даже больше. Это связано с тем, что VSAPI обращается к телу сообщения и к вложению по отдельности, то есть правила последовательно применяются к каждой из частей. Правила применяются также во время фонового сканирования (например, когда продукт ESET Mail Security сканирует почтовый ящик после загрузки новой базы данных сигнатур вирусов), что может увеличивать значение счетчика.

5.1.5.1.1 Мастер создания правил

Задать **условия** и **действия** можно с помощью мастера создания **правил**. Сначала нужно задать условия, затем действия. Нажмите кнопку **Добавить**. Отобразится окно Условие правила, в котором можно выбрать тип условия, операцию и значение. Здесь можно задать также действие правила. Задав условия и действия, укажите **имя** правила (по которому вы сможете его узнавать). Оно будет отображаться в списке правил. Если правило нужно только подготовить, а использовать его планируется позже, то, чтобы деактивировать правило, щелкните переключатель возле элемента **Активный**. Чтобы активировать правило, находящееся в списке правил, установите флажок возле него.

ПРИМЕЧАНИЕ. **Имя** — это обязательное поле, если оно выделено красным цветом. Чтобы создать правило, введите имя правила в текстовое поле и нажмите кнопку **ОК**. Красное выделение не исчезает даже в том случае, если вы ввели имя правила. Оно исчезает после нажатия кнопки **ОК**.

Некоторые **условия** и **действия**, относящиеся к правилам, могут варьироваться в зависимости от того, для чего эти правила используются: для **защиты почтового транспорта**, **защиты базы данных почтовых ящиков** или **сканирования базы данных по требованию**. Это обусловлено тем, что эти виды защиты обрабатывают сообщения немного по-разному (особенно **защита почтового транспорта**).



ПРИМЕЧАНИЕ. Если задать тип действия **Вести журнал событий** для защиты базы данных почтовых ящиков с помощью параметра %IPAddress%, в столбце **Событие** в разделе Файлы журналов не будет отображаться ничего, что связано с этим определенным событием. Это обусловлено тем, что на уровне защиты базы данных почтовых ящиков нет IP-адреса. Некоторые параметры доступны только на некоторых уровнях защиты:

IP-адрес: игнорируется на уровнях **Сканирование базы данных по требованию** и **Защита базы данных почтовых ящиков**.
Почтовый ящик: игнорируется на уровне **Защита почтового транспорта**.

5.1.5.1.1.1 Условия правила

Этот мастер дает возможность добавлять условия для правила. В раскрывающемся списке выберите элементы **Тип** > **Операция** (то, какие операции содержит список, зависит от выбранного типа правил). Затем щелкните **Параметр**. Поля параметра варьируются в зависимости от типа правил и операции.

Например, последовательно выберите **Размер вложения** > **превышает**, а под элементом **Параметр** укажите 10 МБ. Если так настроить параметры, то любое сообщение, в котором есть вложение размером более 10 МБ, обрабатывается с помощью указанного вами действия правила. Поэтому, если при настройке параметров правила вы не указали действие, которое нужно выполнять при срабатывании правила, то вам нужно это сделать.

ПРИМЕЧАНИЕ. Для одного правила возможно добавить несколько условий. Если вы добавляете несколько условий, то условия, отменяющие друг друга, не отображаются.

Список доступных **условий** для **защиты почтового транспорта** (в зависимости от ранее выбранных условий некоторые параметры могут не отображаться):

- **Тема**: применяется к сообщениям, если в поле темы они содержат или не содержат указанную вами строку

(или регулярное выражение).

- **Отправитель**: применяется к сообщениям, которые отправил определенный отправитель.
- **Получатель**: применяется к сообщениям, которые отправлены определенному получателю.
- **Имя вложения**: применяется к сообщениям, которые содержат вложения с определенным именем.
- **Размер вложения**: применяется к сообщениям с вложением, размер которого меньше указанного, больше указанного или находится в пределах указанного диапазона размеров.
- **Тип вложения**: применяется к сообщениям, в которые вложен файл определенного типа. Типы файлов распределены по группам, чтобы их было легко выбирать. Вы можете выбрать несколько типов файлов или целые категории.
- **Размер сообщения**: применяется к сообщениям с вложением, размер которого меньше указанного, больше указанного или находится в пределах указанного диапазона размеров.
- **Результаты сканирования на наличие спама**: применяется к сообщениям в зависимости от того, помечены они как нормальная либо нежелательная почта или нет.
- **Результаты сканирования на наличие вирусов**: применяется к сообщениям на основании того, помечены они как вредоносные или невредоносные.
- **Внутреннее сообщение**: применяется в зависимости от того, является сообщение внутренним или внешним.
- **Время получения**: применяется к сообщениям, полученным перед указанной датой, после нее или в день, который входит в указанный диапазон дат.
- **Заголовки сообщений**: применяется к сообщениям, в заголовках которых есть указанные данные.
- **Содержит защищенный паролем архив**: применяется к сообщениям, в которые вложен архив, защищенный паролем.
- **Содержит поврежденный архив**: применяется к сообщениям, в которые вложен поврежденный архив (при этом его, скорее всего, невозможно открыть).
- **IP-адрес отправителя**: применяется к сообщениям, отправленным с указанного IP-адреса.
- **Домен отправителя**: применяется к сообщениям от отправителя, в адресе электронной почты которого указан определенный домен.
- **Подразделения получателя**: применяется к сообщениям, отправленным получателю, который входит в указанное подразделение.

Список доступных условий для защиты базы данных почтовых ящиков и сканирования базы данных по требованию (в зависимости от ранее выбранных условий некоторые параметры могут не отображаться):

- **Тема**: применяется к сообщениям, если в поле темы они содержат или не содержат указанную вами строку (или регулярное выражение).
- **Отправитель**: применяется к сообщениям, которые отправил определенный отправитель.
- **Получатель**: применяется к сообщениям, которые отправлены определенному получателю.
- **Почтовый ящик**: применяется к сообщениям, находящимся в указанном почтовом ящике.
- **Имя вложения**: применяется к сообщениям, которые содержат вложения с определенным именем.
- **Размер вложения**: применяется к сообщениям с вложением, размер которого меньше указанного, больше указанного или находится в пределах указанного диапазона размеров.
- **Тип вложения**: применяется к сообщениям, в которые вложен файл определенного типа. Типы файлов распределены по группам, чтобы их было легко выбирать. Вы можете выбрать несколько типов файлов или целые категории.

- **Результаты сканирования на наличие вирусов**: применяется к сообщениям на основании того, помечены они как вредоносные или невредоносные.
- **Время получения**: применяется к сообщениям, полученным перед указанной датой, после нее или в день, который входит в указанный диапазон дат.
- **Заголовки сообщений**: применяется к сообщениям, в заголовках которых есть указанные данные.
- **Содержит защищенный паролем архив**: применяется к сообщениям, в которые вложен архив, защищенный паролем.
- **Содержит поврежденный архив**: применяется к сообщениям, в которые вложен поврежденный архив (при этом его, скорее всего, невозможно открыть).
- **IP-адрес отправителя**: применяется к сообщениям, отправленным с указанного IP-адреса.
- **Домен отправителя**: применяется к сообщениям от отправителя, в адресе электронной почты которого указан определенный домен.

5.1.5.1.1.2 Действие правила

Вы можете добавлять действия, которые должны выполняться по отношению к сообщениям и/или вложениям, отвечающим условиям правила.

ПРИМЕЧАНИЕ. Для одного правила возможно добавить несколько условий. Если вы добавляете несколько условий, то условия, отменяющие друг друга, не отображаются.

Список доступных **действий** для **защиты почтового транспорта** (в зависимости от выбранных условий некоторые параметры могут не отображаться):

- **Переместить сообщение в карантин**: сообщение не доставляется получателю и перемещается в карантин почты.
- **Удалить вложение**: вложение удаляется, и сообщение доставляется получателю без него.
- **Отклонить сообщение**: сообщение не доставляется, и отправителю отправляется отчет о недоставке.
- **Автоматически удалить сообщение**: сообщение удаляется, при этом не отправляется отчет о недоставке.
- **Задать значение вероятности нежелательной почты**: это значение изменяется или задается.
- **Отправить оповещение по электронной почте**: позволяет отправить оповещение по электронной почте.
- **Пропустить сканирование на наличие спама**: сообщение сканируется модулем защиты от спама.
- **Пропустить сканирование на наличие вирусов**: сообщение сканируется модулем защиты от вирусов.
- **Обработать другие правила**: позволяет оценить также и другие правила, что дает пользователю возможность задать несколько наборов условий и разные применяемые действия в зависимости от условий.
- **Вносить в журнал событий**: информация о применяемом правиле регистрируется в журнале программы.
- **Добавить поле заголовка**: в заголовок сообщения добавляется настраиваемая строка.

Список доступных **действий** для **защиты базы данных почтовых ящиков** и **сканирования базы данных по требованию** (в зависимости от выбранных условий некоторые параметры могут не отображаться):

- **Удалить вложение**: вложение удаляется, и сообщение доставляется получателю без него.
- **Поместить вложение на карантин**: вложение перемещается в карантин почты, и сообщение доставляется получателю без вложения.
- **Заменить вложение сведениями о действии**: вложение удаляется, а информация об этом действии добавляется в тело сообщения.

- **Удалить сообщение**: сообщение удаляется.
- **Отправить оповещение по электронной почте**: позволяет отправить оповещение по электронной почте.
- **Пропустить сканирование на наличие вирусов**: сообщение сканируется модулем защиты от вирусов.
- **Обработать другие правила**: позволяет оценить также и другие правила, что дает пользователю возможность задать несколько наборов условий и разные применяемые действия в зависимости от условий.
- **Вносить в журнал событий**: информация о применяемом правиле регистрируется в журнале программы.
- **Переместить сообщение в корзину** (доступно только для **сканирования базы данных по требованию**): сообщение перемещается в корзину почтового клиента.

5.1.6 Защита базы данных почтовых ящиков

Параметр **Защита базы данных почтовых ящиков** в разделе **Дополнительные параметры** > **Сервер** доступен в следующих системах:

- Microsoft Exchange Server 2003 (роль тылового сервера);
- Microsoft Exchange Server 2003 (единичный сервер с несколькими ролями);
- Microsoft Exchange Server 2007 (роль сервера почтовых ящиков);
- Microsoft Exchange Server 2007 (единичный сервер с несколькими ролями);
- Microsoft Exchange Server 2010 (роль сервера почтовых ящиков);
- Microsoft Exchange Server 2010 (единичный сервер с несколькими ролями);
- Windows Small Business Server 2003;
- Windows Small Business Server 2008;
- Windows Small Business Server 2011.

ПРИМЕЧАНИЕ. Защита базы данных почтовых ящиков недоступна для Microsoft Exchange Server 2013.

Если снять флажок **Включить VSAPI 2.6 защиты от вирусов и шпионских программ**, подключаемый модуль ESET Mail Security для сервера Exchange не будет выгружен из процесса Microsoft Exchange Server. Он будет просто пропускать через себя сообщения, не сканируя их на наличие вирусов. Однако сообщения все же будут сканироваться на наличие спама, а также будут применяться правила.

Если активирован параметр **Проактивное сканирование**, новые входящие сообщения будут сканироваться в том же порядке, в котором они были получены. Если этот параметр активирован и пользователь открывает сообщение, которое еще не сканировалось, это сообщение будет просканировано до остальных сообщений в очереди.

Фоновое сканирование позволяет сканировать все сообщения в фоновом режиме (сканируется почтовый ящик и хранилище общих папок, например база данных Exchange). Microsoft Exchange Server принимает решение о том, будет ли выполняться фоновое сканирование, на основе различных факторов, таких как текущая нагрузка на систему, количество активных пользователей и т. д. Microsoft Exchange Server сохраняет записи о просканированных сообщениях и использованной версии базы данных сигнатур вирусов. Если открывается сообщение, которое не сканировалось с применением самой актуальной базы данных сигнатур вирусов, Microsoft Exchange Server отправляет это сообщение в ESET Mail Security для сканирования, прежде чем такое сообщение будет открыто в почтовом клиенте. Можно выбрать параметр **Сканировать только сообщения с вложениями** и фильтровать на основе времени получения, используя один из перечисленных далее вариантов параметра **Уровень сканирования**.

- **Все сообщения**
- **Сообщения, полученные за последний год**
- **Сообщения, полученные за последние 6 мес.**
- **Сообщения, полученные за последние 3 мес.**
- **Сообщения, полученные за последние месяцы**
- **Сообщения, полученные за последнюю неделю**

Поскольку фоновое сканирование может увеличить нагрузку на систему (сканирование выполняется после каждого обновления базы данных сигнатур вирусов), рекомендуется использовать сканирование по

расписанию, планируя его на нерабочие часы. Запланированное фоновое сканирование можно сконфигурировать с помощью особой задачи в планировщике. При планировании задачи фонового сканирования можно задать время запуска, количество повторений и другие параметры, которые доступны в планировщике. После планирования задача появляется в списке запланированных. Вы можете изменить ее параметры, удалить ее или временно отключить.

Установка флажка **Сканировать текст сообщений в формате RTF** активирует сканирование тела сообщений в формате RTF. В теле сообщений в формате RTF могут содержаться макровирусы.

ПРИМЕЧАНИЕ. Тело сообщений электронной почты в формате обычного текста не сканируется VSAPI.

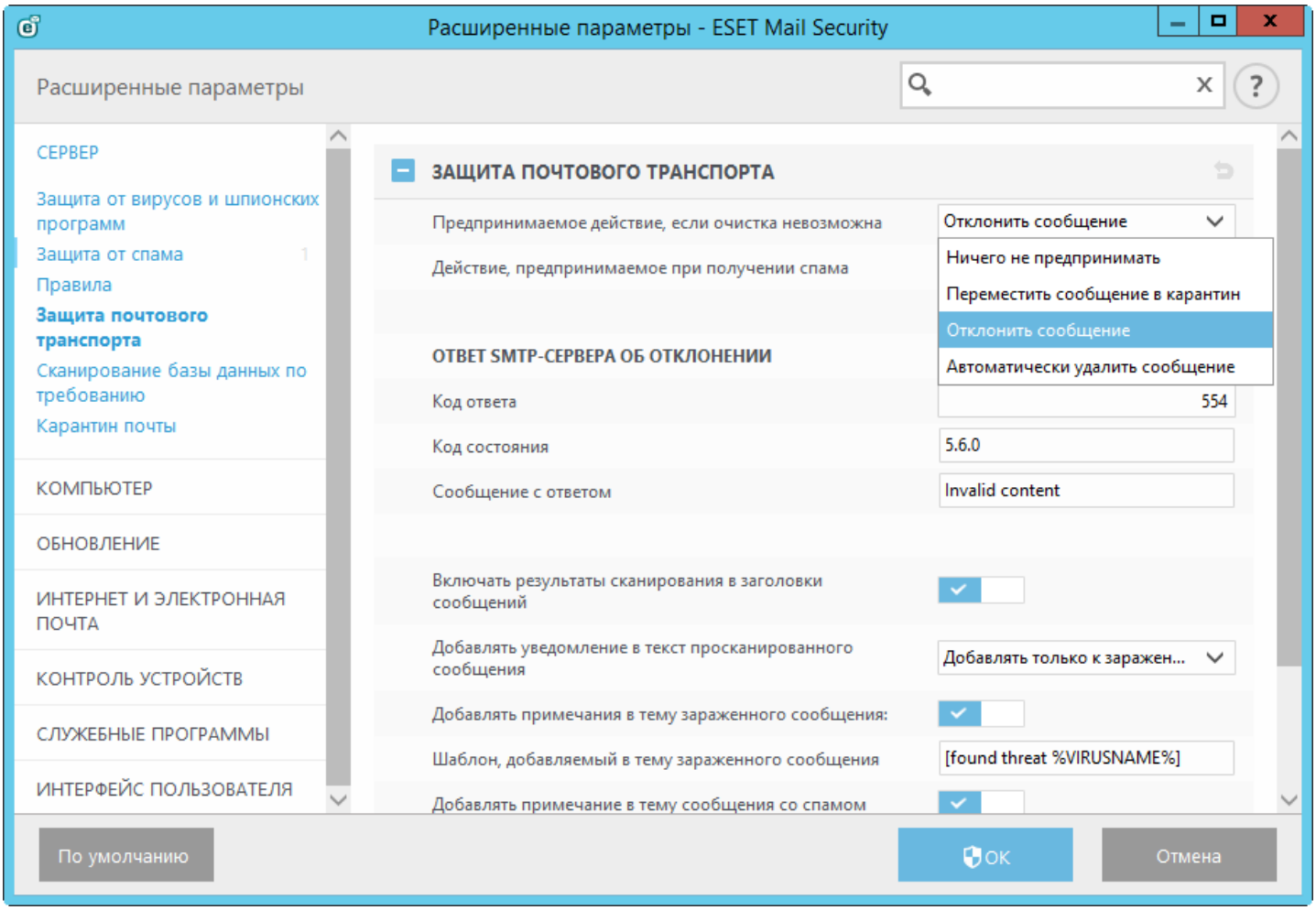
ПРИМЕЧАНИЕ: Действия по отношению к общим папкам и почтовым ящикам не отличаются. Это значит, что общие папки тоже сканируются.

5.1.7 Защита почтового транспорта

Параметр **Защита почтового транспорта** в разделе **Дополнительные параметры** > **Сервер** доступен в следующих операционных системах:

- Microsoft Exchange Server 2007 (пограничный транспортный сервер или транспортный сервер-концентратор);
- Microsoft Exchange Server 2007 (единичный сервер с несколькими ролями);
- Microsoft Exchange Server 2010 (пограничный транспортный сервер или транспортный сервер-концентратор);
- Microsoft Exchange Server 2010 (единичный сервер с несколькими ролями);
- Microsoft Exchange Server 2013 (роль пограничного транспортного сервера);
- Microsoft Exchange Server 2013 (единичный сервер с несколькими ролями);
- Windows Small Business Server 2008;
- Windows Small Business Server 2011.

Параметры защиты почтового транспорта:



Действия антивируса по отношению к транспортному уровню можно задать в параметре **Предпринимаемое действие, если очистка невозможна**:

- **Ничего не предпринимать**: зараженные сообщения, которые нельзя очистить, остаются в системе.
- **Переместить сообщение в карантин**: зараженное сообщение отправляется в почтовый ящик карантина.
- **Отклонить сообщение**: зараженное сообщение удаляется.
- **Автоматически удалить сообщение**: сообщение удаляется, при этом отчет о недоставке не отправляется.

Действие модуля защиты от спама на транспортном уровне можно задать в параметре **Действие, предпринимаемое при получении спама**:

- **Ничего не предпринимать**: сообщение сохраняется, даже если оно помечено как спам.
- **Переместить сообщение в карантин**: помеченное как спам сообщение отправляется в почтовый ящик карантина.
- **Отклонить сообщение**: отклонение сообщений, помеченных как спам.
- **Автоматически удалить сообщение**: сообщение удаляется, при этом отчет о недоставке не отправляется.

Ответ SMTP-сервера об отклонении: вы можете указать **код ответа**, **код состояния** и **сообщение с ответом**. Эти сведения определяют ответ о временном отклонении, отправляемый SMTP-серверу, если сообщение отклоняется. Можно ввести ответное сообщение в следующем формате.

Код ответа	Код состояния	Сообщение с ответом
250	2.5.0	Requested mail action okay, completed (Запрошенное действие с почтой в порядке, завершено)
451	4.5.1	Requested action aborted:local error in processing (Запрошенное действие прервано: обрабатывается локальная ошибка)
550	5.5.0	Requested action not taken: mailbox unavailable (Запрошенное действие не выполнено: почтовый ящик недоступен)
554	5.6.0	Invalid content (Недопустимое содержимое)

ПРИМЕЧАНИЕ.: Также можно использовать системные переменные при настройке ответа отклонения по SMTP.

Включать результаты сканирования в заголовки сообщений: когда этот параметр включен, результаты сканирования добавляются в заголовки сообщения. Эти заголовки сообщения начинаются с `X_ESET`, благодаря чему их легко распознавать (например, `X_EsetResult` или `X_ESET_Antispam`).

У параметра **Добавлять уведомление в текст просканированного сообщения** есть три значения:
- Не добавлять к сообщениям.
- Добавлять только к зараженным сообщениям.
- Добавлять ко всем просканированным сообщениям (это не касается внутренних сообщений).

Если выбрать вариант **Добавлять примечания в тему зараженного сообщения**, <%PN%> будет добавлять тег уведомления в тему сообщения. Значение такого тега задается в текстовом поле **Шаблон, добавляемый в тему зараженного сообщения** (по умолчанию `[found threat %VIRUSNAME%]`). С помощью этой функции можно автоматизировать фильтрацию зараженных сообщений, то есть фильтровать сообщения электронной почты по определенной теме. Для этого можно использовать, например, правила. Или же с помощью этой функции можно на стороне клиента (если это поддерживается почтовым клиентом) перемещать сообщения в отдельную папку.

Если выбрать вариант **Добавлять примечание в тему сообщения со спамом**, <%PN%> будет добавлять тег

уведомления в тему сообщения. Значение такого тега задается в текстовом поле **Шаблон, добавляемый в тему сообщения со спамом** (по умолчанию `[SPAM]`). С помощью этой функции можно автоматизировать фильтрацию спама, то есть фильтровать сообщения электронной почты по определенной теме. Для этого можно использовать, например, правила. Или же с помощью этой функции можно на стороне клиента (если это поддерживается почтовым клиентом) перемещать сообщения в отдельную папку.

ПРИМЕЧАНИЕ. Вы можете использовать системные переменные и тогда, когда изменяете текст, который будет добавлен в тему.

5.1.7.1 Дополнительные параметры

В этом разделе можно изменить дополнительные параметры, применяемые к агенту транспорта:

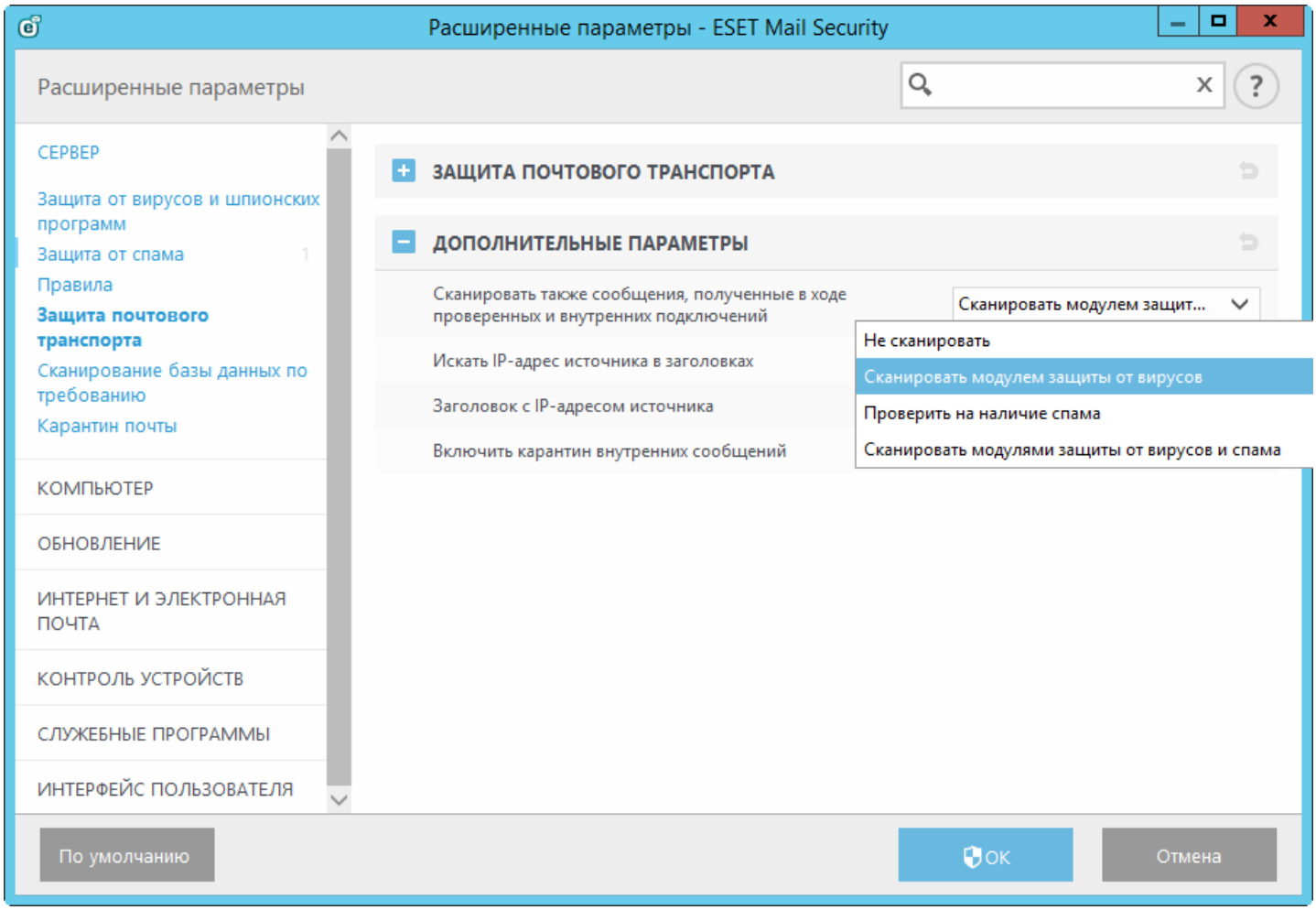
- **Сканировать также сообщения, полученные по проверенным или внутренним соединениям**: вы можете выбирать тип сканирования, который необходимо использовать для сообщений, получаемых из прошедших проверку подлинности источников или с локальных серверов. Рекомендуется выполнять сканирование таких сообщений, чтобы повысить уровень защиты, а если вы используете встроенный соединитель Microsoft SBS POP3 для получения почтовых сообщений с внешних серверов POP3 или из почтовых служб (например, **Gmail.com**, **Outlook.com**, **Yahoo.com**, **gmx.dem** и т. д.), такое сканирование является обязательным. Дополнительные сведения см. в разделе Соединитель POP3 и защита от спама.

ПРИМЕЧАНИЕ.: Внутрикорпоративные сообщения программы Outlook отправляются в формате TNEF (транспортном формате нейтральной инкапсуляции). Формат TNEF не поддерживается функцией защиты от спама. Поэтому внутренние электронные письма в формате TNEF не будут сканироваться на наличие спама, даже если выбрать **Проверить на наличие спама** или **Сканировать модулями защиты от вирусов и спама**.

- **Искать IP-адрес источника в заголовках**: если этот параметр включен, ESET Mail Security будет искать IP-адрес источника в заголовках сообщений, чтобы другие модули защиты (от спама и пр.) могли тоже использовать его. Если у вас организация Exchange отделена от Интернета прокси-сервером, шлюзом или пограничным транспортным сервером, почтовые сообщения выглядят, как пришедшие с одного IP-адреса (как правило, внутреннего). Распространенной является ситуация, когда на внешнем сервере (например, пограничном транспортном сервере в зоне DMZ) известен IP-адрес отправителя и этот IP-адрес записывается в заголовки получаемых почтовых сообщений. Значение, указанное в поле **Заголовок с IP-адресом источника** ниже, является заголовком, который программа ESET Mail Security ищет в заголовках сообщений.

- **Заголовок с IP-адресом источника** — это тот заголовок, который программа ESET Mail Security ищет среди заголовков сообщений. По умолчанию применяется значение **X-Originating-IP**, но если вы используете сторонние или специальные инструменты, применяющие другой заголовок, необходимо задать соответствующее значение.

- **Включить карантин внутренних сообщений**: если эта функция включена, внутренние сообщения будут отправляться на карантин. Обычно нет необходимости помещать в карантин внутренние сообщения. Тем не менее если требуется помещение в карантин, то соответствующую функцию можно включить.



5.1.8 Сканирование базы данных по требованию

Список систем, в которых доступен параметр **Сканирование базы данных по требованию**:

- Microsoft Exchange Server 2007 (сервер почтовых ящиков или транспортный сервер-концентратор);
- Microsoft Exchange Server 2007 (единичный сервер с несколькими ролями);
- Microsoft Exchange Server 2010 (сервер почтовых ящиков или транспортный сервер-концентратор);
- Microsoft Exchange Server 2010 (единичный сервер с несколькими ролями);
- Microsoft Exchange Server 2013 (роль сервера почтовых ящиков);
- Microsoft Exchange Server 2013 (единичный сервер с несколькими ролями);
- Windows Small Business Server 2008;
- Windows Small Business Server 2011.

ПРИМЕЧАНИЕ. Если вы работаете в системе Microsoft Exchange Server 2007 или 2010, вы можете воспользоваться защитой базы данных почтовых ящиков или сканированием базы данных по требованию. При этом данные типы защиты не могут быть активными одновременно. Если выбрать сканирование базы данных по требованию, то в разделе Сервер дополнительных настроек необходимо отключить интеграцию защиты базы данных почтовых ящиков. В противном случае сканирование базы данных по требованию будет недоступно.

Параметры сканирования базы данных по требованию

Адрес хоста: имя или IP-адрес сервера, на котором запущены веб-службы Exchange.

Имя пользователя: учетные данные пользователя, у которого есть доступ к веб-службам Exchange.

Пароль пользователя: щелкните **Задать** возле элемента **Пароль пользователя** и введите пароль для этой учетной записи пользователя.

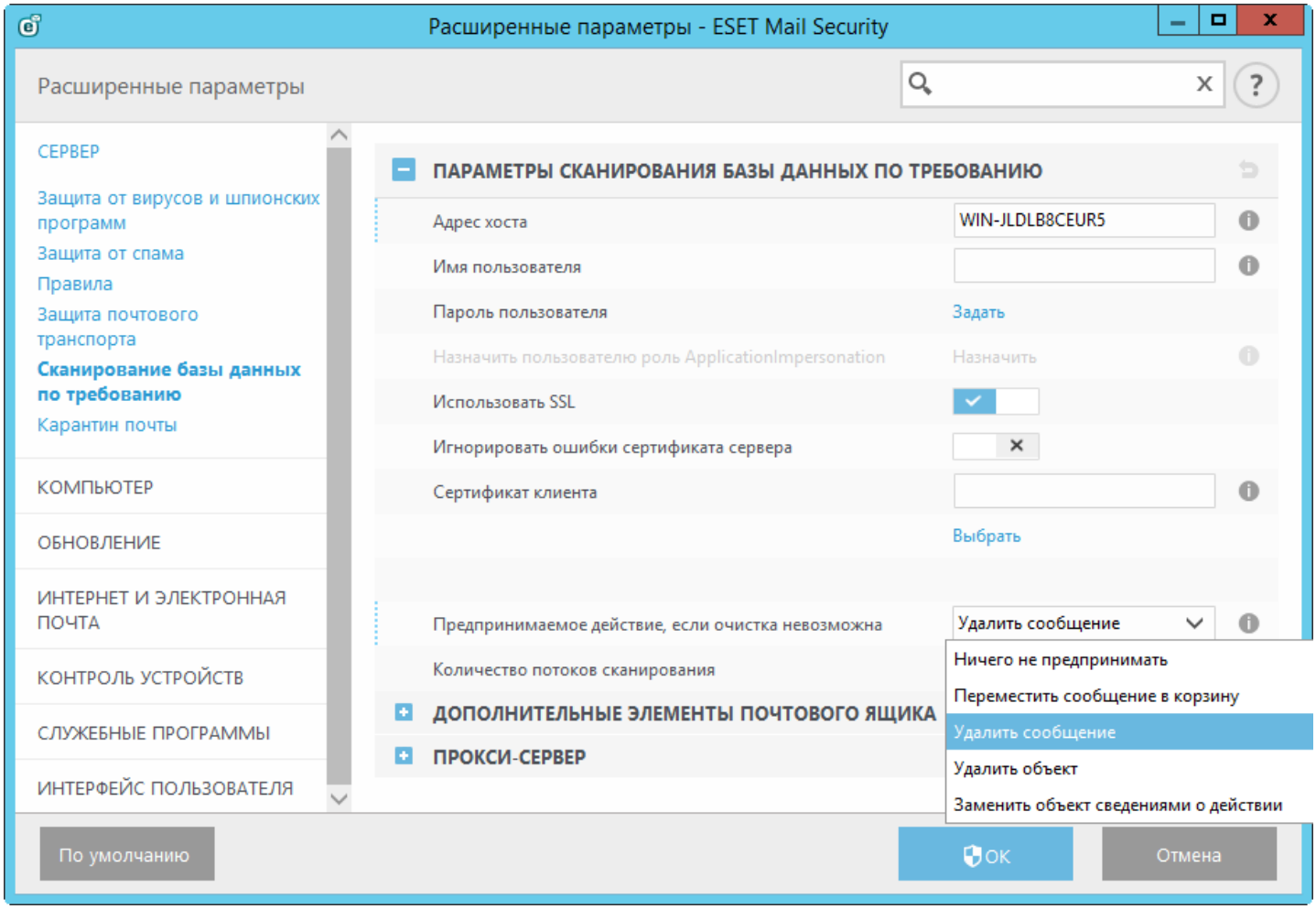
Назначить пользователю роль ApplicationImpersonation: если этот параметр неактивен, нужно сначала указать **имя пользователя**. Чтобы автоматически назначить роль ApplicationImpersonation выбранному пользователю,

щелкните **Назначить**. Или же вы можете назначить роль ApplicationImpersonation вручную учетной записи пользователя. Дополнительные сведения см. в разделе Сведения об учетной записи сканирования баз данных.

Использовать SSL: нужно включить, если в IIS для веб-служб Exchange задано значение **Требовать SSL**. Если протокол SSL включен, сертификат сервера Exchange Server нужно импортировать в систему с ESET Mail Security (если роли Exchange Server активированы на разных серверах). В IIS параметры веб-служб Exchange можно найти в расположении *Sites/Default web site/EWS/SSL Settings*.

ПРИМЕЧАНИЕ. Параметр **Использовать SSL** можно отключать, только если в IIS веб-службы Exchange настроены так, чтобы не требовать SSL.

Сертификат клиента нужно задавать только тогда, когда он требуется для веб-служб Exchange. Элемент **Выбрать** позволяет выбрать любой сертификат.



Предпринимаемое действие, если очистка невозможна: это поле действий позволяет **заблокировать** зараженное содержимое.

Ничего не предпринимать: не предпринимать никаких действий по отношению к зараженному содержимому сообщения.
Переместить сообщение в корзину: это параметр нельзя применить по отношению к файлам общей папки. Вместо него можно воспользоваться командой **Удалить объект**.
Удалить объект: удалить зараженное содержимое сообщения.
Удалить сообщение: удалить все сообщение вместе с зараженным содержимым.
Заменить объект сведениями о действии: объект удаляется, при этом остается информация о действии, выполненном по отношению к этому объекту.

5.1.8.1 Дополнительные элементы почтового ящика

Настраивая параметры в модуле сканирования базы данных по требованию, вы можете включить или отключить сканирование других типов элементов почтового ящика. Вы можете:

- сканировать календарь,
- сканировать задачи,
- сканировать контакты,
- сканировать журнал.

ПРИМЕЧАНИЕ. Если возникли проблемы с производительностью, сканирование этих элементов можно отключить. Если же оно не отключено, то сканирование занимает больше времени.

5.1.8.2 Прокси-сервер

Если вы используете прокси-сервер в качестве посредника между сервером Exchange Server с ролью сервера клиентского доступа и сервером Exchange Server, на котором установлен продукт ESET Mail Security, укажите параметры этого прокси-сервера. Это нужно потому, что программа ESET Mail Security соединяется с интерфейсом API веб-служб Exchange по протоколу HTTP или HTTPS. В противном случае сканирование базы данных по требованию не будет функционировать.

Прокси-сервер: введите IP-адрес или имя используемого вами прокси-сервера.

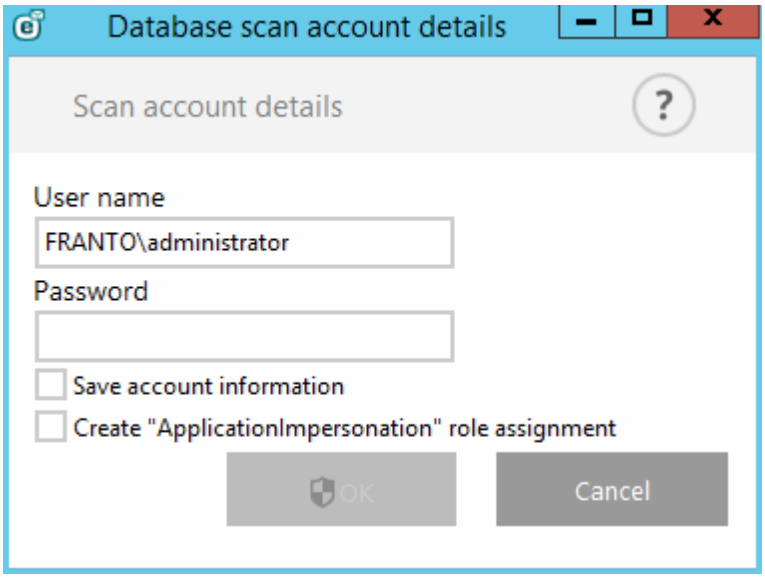
Порт: укажите номер порта прокси-сервера.

Имя пользователя, Пароль: введите учетные данные, если для вашего прокси-сервера нужна проверка подлинности.

5.1.8.3 Сведения об учетной записи сканирования баз данных

Это диалоговое окно отображается, если в разделе интерфейса **Дополнительные настройки** вы не указали имя пользователя и пароль для **сканирования базы данных**. Укажите в нем учетные данные пользователя, имеющего доступ к веб-службам Exchange, и нажмите кнопку **ОК**. Или же нажмите клавишу **F5**, чтобы перейти к разделу **Дополнительные настройки**, а затем последовательно щелкните **Сервер** > Сканирование базы данных по требованию. Укажите **имя пользователя**, щелкните **Задать**, введите пароль для этой учетной записи пользователя и нажмите кнопку ОК.

- Чтобы сохранить настройки параметров учетной записи, вы можете щелкнуть **Сохранить сведения об учетной записи**. После этого вам не придется вводить эти сведения всякий раз, когда запускается сканирование базы данных по требованию.
- Если учетная запись пользователя не имеет надлежащего доступа к веб-службам Exchange, вы можете выбрать **Создать назначение роли «ApplicationImpersonation»**, чтобы назначить учетной записи эту роль. Или же вы можете назначить роль ApplicationImpersonation вручную. Подробности см. ниже в разделе «Примечание».



ВНИМАНИЕ! Учетной записи сканирования нужно назначить роль **ApplicationImpersonation**, чтобы модуль сканирования сканировал почтовые ящики пользователей, находящиеся в базах данных почтовых ящиков Exchange. На сервере Exchange Server 2010 или более новой версии настоятельно рекомендуется настроить политику регулирования для учетной записи сканирования, чтобы предотвратить слишком большое количество запросов на выполнение операций от решения ESET Mail Security. В противном случае сервер Exchange Server станет причиной того, что время ожидания некоторых запросов операций будет истекать.

ПРИМЕЧАНИЕ. Если нужно назначить роль ApplicationImpersonation учетной записи пользователя вручную, вы можете использовать следующие команды (замените при этом `ESET-user` именем учетной записи, которая есть в вашей системе):

Exchange Server 2007

```
Get-ClientAccessServer | Add-AdPermission -User ESET-user -ExtendedRights ms-Exch-EPI-Impersonation

Get-MailboxDatabase | Add-AdPermission -User ESET-user -ExtendedRights ms-Exch-EPI-May-Impersonate
```

Exchange Server 2010

```
New-ManagementRoleAssignment -Name:ESET-ApplicationImpersonation -Role:ApplicationImpersonation
-User:ESET-user
```

На применение может уйти несколько секунд.

```
New-ThrottlingPolicy -Name ESET-ThrottlingPolicy -EWSFindCountLimit $null -EWSFastSearchTimeoutInSeco

Set-ThrottlingPolicyAssociation -Identity user-ESET -ThrottlingPolicy ESET-ThrottlingPolicy
```

Exchange Server 2013

```
New-ManagementRoleAssignment -Name:ESET-ApplicationImpersonation -Role:ApplicationImpersonation
-User:ESET-user
```

На применение может уйти несколько секунд.

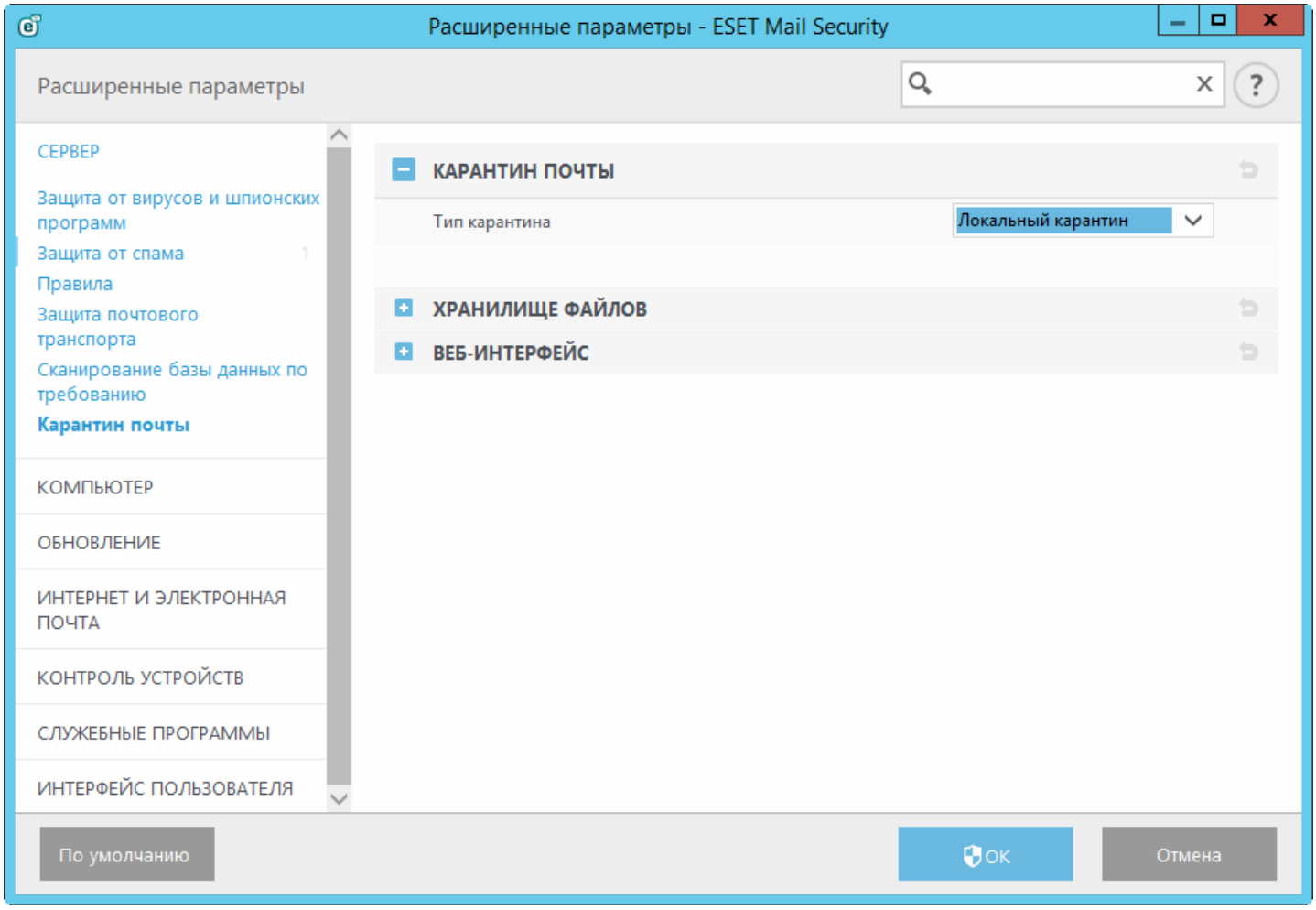
```
New-ThrottlingPolicy -Name ESET-ThrottlingPolicy -EWSMaxConcurrency Unlimited -EwsCutoffBalance Unlim

Set-ThrottlingPolicyAssociation -Identity ESET-user -ThrottlingPolicy ESET-ThrottlingPolicy
```

5.1.9 Карантин почты

Средство управления карантином почты позволяет работать со всеми тремя типами карантина:

- локальный карантин,
- почтовый ящик карантина,
- карантин MS Exchange.



Сведения о карантине почты доступны в средстве управления карантином почты (сведения о всех типах карантина). Кроме того, сведения о локальном карантине доступны в веб-интерфейсе карантина почты.

5.1.9.1 Локальный карантин

Функция локального карантина хранит в локальной файловой системе сообщения, перемещенные на карантин, и базу данных SQLite в качестве индекса. Из соображений безопасности хранящиеся сообщения, перемещенные на карантин, и файл базы данных шифруются. Эти файлы находятся в папке `C:\ProgramData\ESET\ESET Mail Security\MailQuarantine` (в Windows Server 2008 и 2012) или `C:\Documents and Settings\All Users\Application Data\ESET\ESET Mail Security\MailQuarantine` (в Windows Server 2003).

ПРИМЕЧАНИЕ. Если нужно хранить помещенные в карантин файлы не на диске, заданном по умолчанию (`C:`), а на другом диске, нужно изменить путь в поле **Папка данных**, указав во время установки решения ESET Mail Security нужный вам путь.

Функции локального карантина:

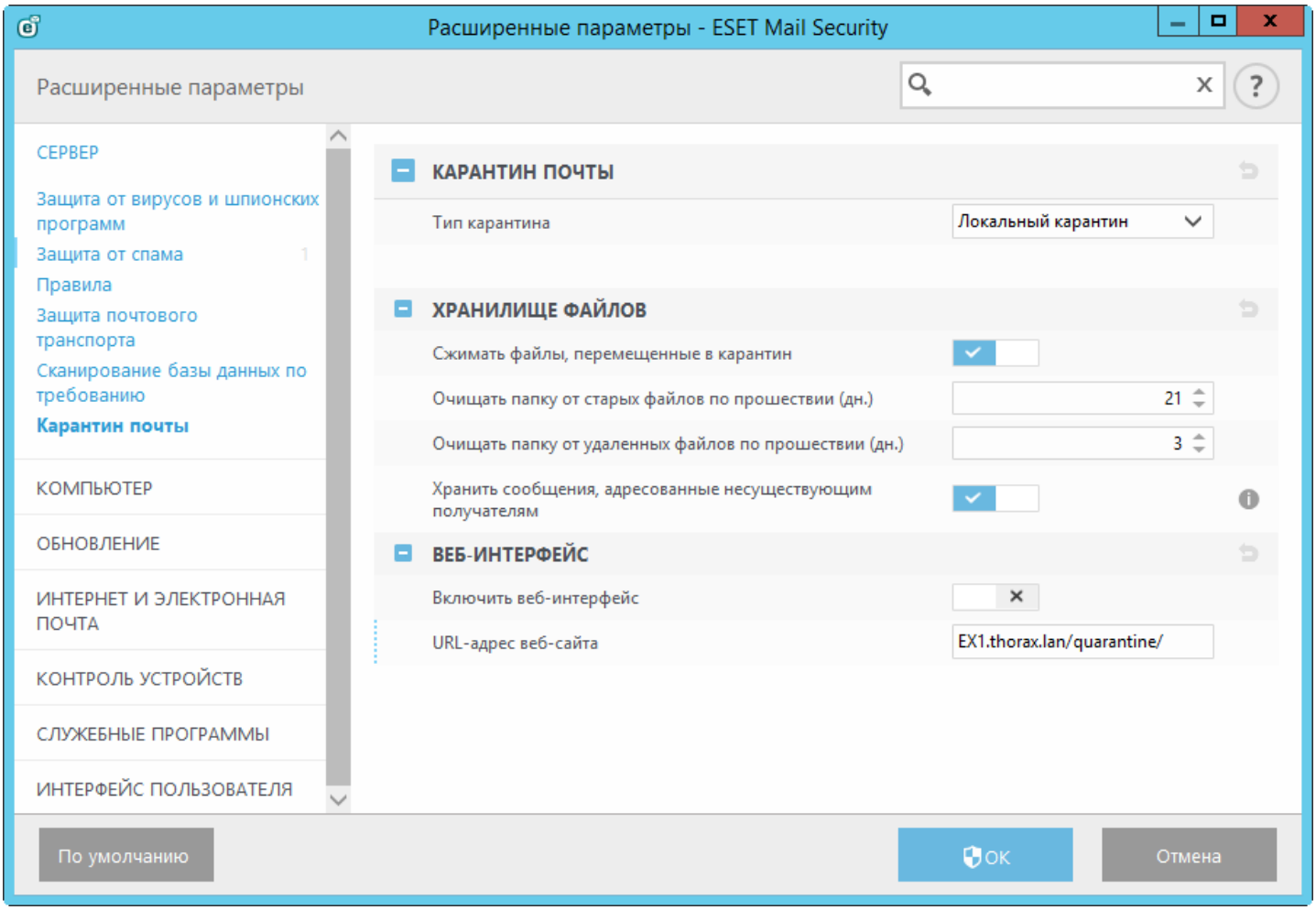
- Нежелательные и помещенные в карантин сообщения будут храниться в локальной файловой системе, то есть их не будет в базе данных почтовых ящиков Exchange.
- Шифрование и сжатие хранящихся на карантине (на локальном диске) сообщений электронной почты.
- Веб-интерфейс карантина почты как альтернатива средству управления карантином почты.
- Отчеты о карантине можно отправлять на указанный адрес электронной почты с помощью запланированной задачи.
- Перемещенные на карантин файлы, удаленные из окна карантина (по умолчанию по прошествии 21 дня), продолжают храниться в файловой системе (до автоматического удаления через указанное количество дней).
- Автоматическое удаление старых файлов электронной почты (по умолчанию по прошествии 3 дней). Дополнительные сведения см. в разделе Параметры хранилища файлов.
- Вы можете восстановить удаленные из карантина файлы электронной почты с помощью eShell (если они еще не удалены из системы).

ПРИМЕЧАНИЕ. Недостаток использования локального карантина заключается в том, что если запустить несколько серверов ESET Mail Security, назначив им роль транспортного сервера-концентратора, нужно будет управлять локальным карантином каждого сервера по отдельности. Чем больше серверов, тем больше случаев карантина, которыми нужно управлять.

Вы можете проверить хранящиеся на карантине сообщения, а затем **удалить** или **освободить** их. Отображать перемещенные на локальный карантин сообщения и управлять ими вы можете с помощью средства управления карантином почты (в основном графическом интерфейсе пользователя) или веб-интерфейса карантина почты.

5.1.9.1.1 Хранилище файлов

В этом разделе интерфейса можно изменить параметры хранилища файлов, используемого для локального карантина.



Сжимать файлы, перемещенные в карантин: если сжать перемещенные в карантин файлы, они занимают

меньше места. Если, тем не менее, вы не хотите их сжимать, то, чтобы отключить сжатие, щелкните переключатель.

Очищать папку от старых файлов по прошествии (дн.): когда срок хранения сообщений достигает указанного количества дней, они удаляются из окна карантина. При этом эти файлы не удаляются с диска в течение того количества дней, которое указано для параметра **Очищать папку от удаленных файлов по прошествии (дн.)**. Так как файлы не удаляются из файловой системы, их можно восстановить с помощью eShell.

Очищать папку от удаленных файлов по прошествии (дн.): файлы удаляются с диска по прошествии указанного количества дней, и после этого их можно восстановить только с помощью решения резервного копирования файловой системы.

Хранить сообщения, адресованные несуществующим получателям: обычно злоумышленники указывают получателей в домене наугад, пытаясь при этом указать тех, кто действительно существует. Сообщения, адресованные пользователям, которых нет в Active Directory, по умолчанию хранятся в папке локального карантина. При этом вы можете отключить этот параметр. В таком случае сообщения, адресованные несуществующим получателям, будут удаляться и папка локального карантина не будет переполнена подобными нежелательными письмами. Кроме того, вы сэкономите место на диске.

5.1.9.1.2 Веб-интерфейс

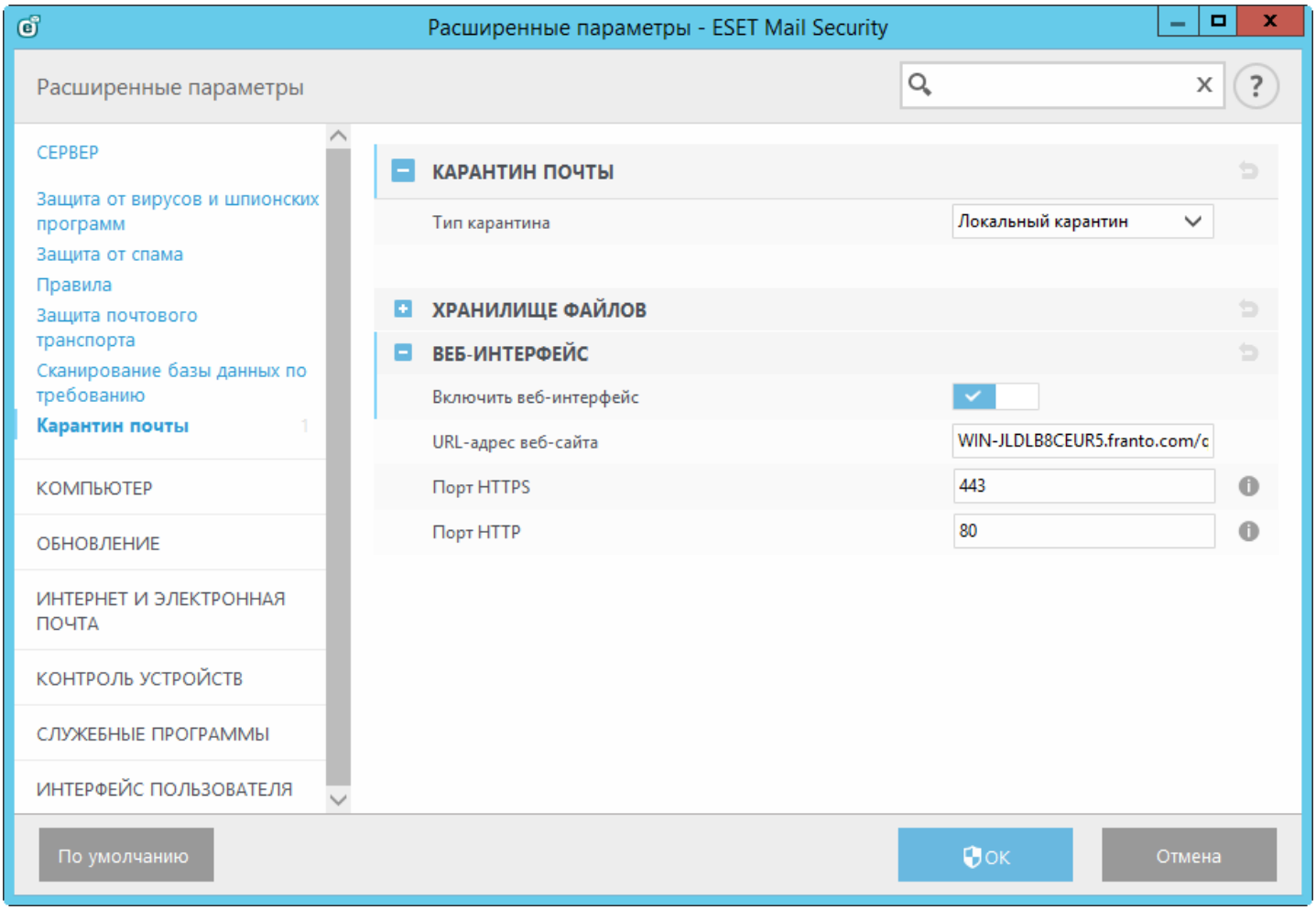
Веб-интерфейс карантина почты — это альтернатива средству управления карантином почты, доступная только для локального карантина.

ПРИМЕЧАНИЕ.: Веб-интерфейс карантина почты недоступен на сервере, который выполняет роль пограничного транспортного сервера, поскольку служба Active Directory недоступна для аутентификации.

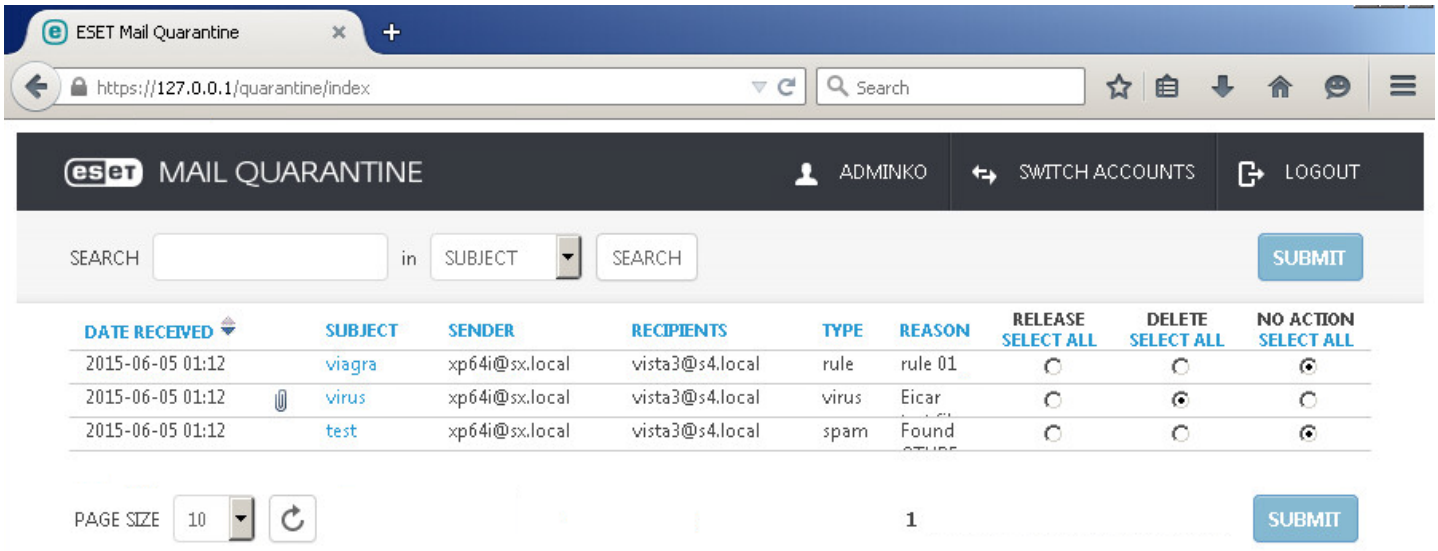
С помощью этого альтернативного средства можно просматривать состояние карантина почты и управлять находящимися в карантине сообщениями электронной почты. Чтобы открыть этот веб-интерфейс, можно перейти по ссылкам, которые находятся в отчетах о карантине, или просто ввести в браузере URL-адрес. Чтобы получить доступ к веб-интерфейсу карантина почты, введите учетные данные домена для проверки подлинности. В Internet Explorer проверка подлинности для пользователя домена выполняется автоматически. При этом сертификат веб-страницы должен быть действителен, в Internet Explorer нужно включить автоматический вход и вам нужно добавить веб-сайт карантина почты в список узлов интрасети.

Вы можете включать и отключать веб-интерфейс с помощью переключателя **Включить веб-интерфейс**.

URL-адрес веб-сайта: это URL-адрес, по которому будет доступен веб-интерфейс карантина почты. По умолчанию это полное доменное имя сервера, к которому добавлено слово `/quarantine` (например, `mailserver.company.com/quarantine`).
HTTPS-порт: номер используемого по умолчанию порта — 443. Если нужно, вы можете изменить номер порта.
HTTP-порт: номер используемого по умолчанию порта — 80. Если нужно, вы можете изменить номер порта.

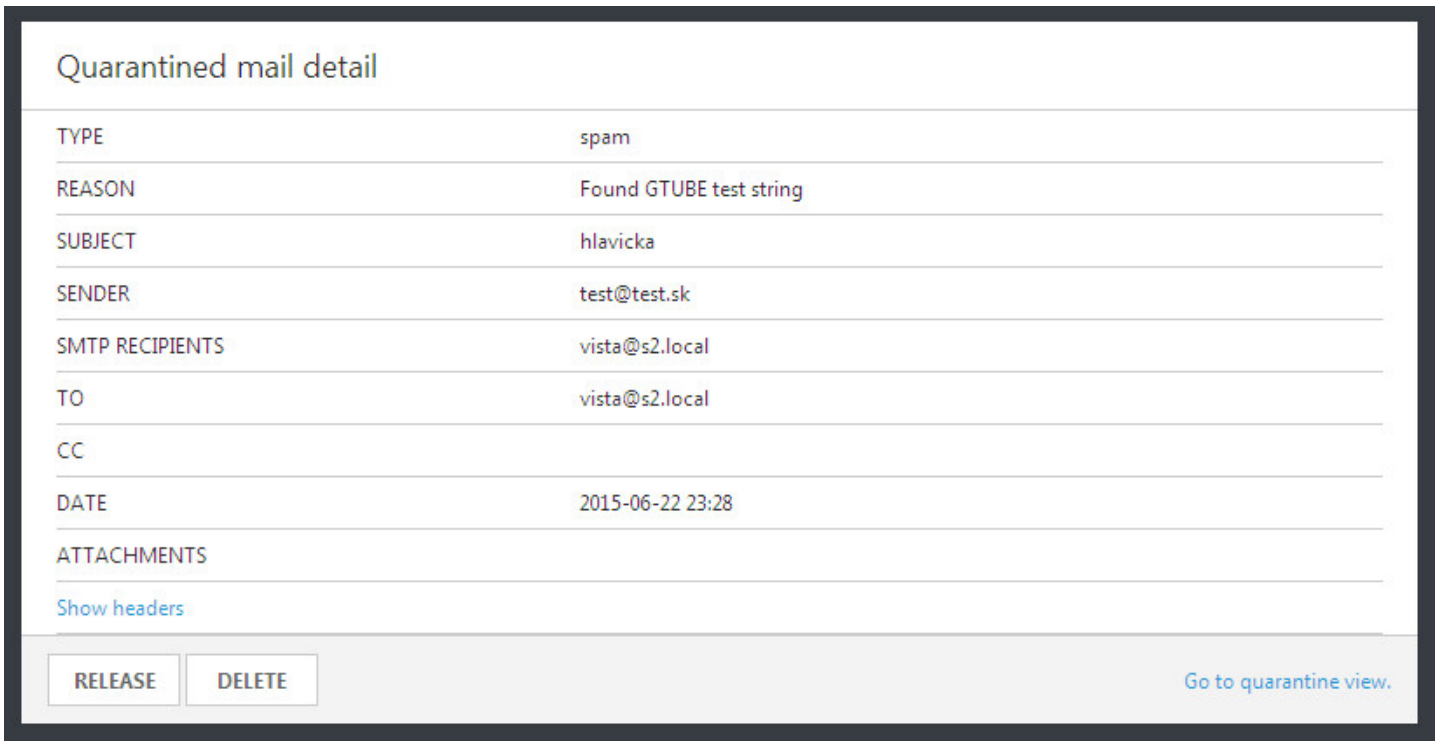


Чтобы получить доступ к веб-интерфейсу карантина почты, откройте веб-браузер и используйте URL-адрес, указанный в разделе **Дополнительные настройки** > **Сервер** > **Карантин почты** > **Веб-интерфейс** > **URL-адрес веб-сайта**.

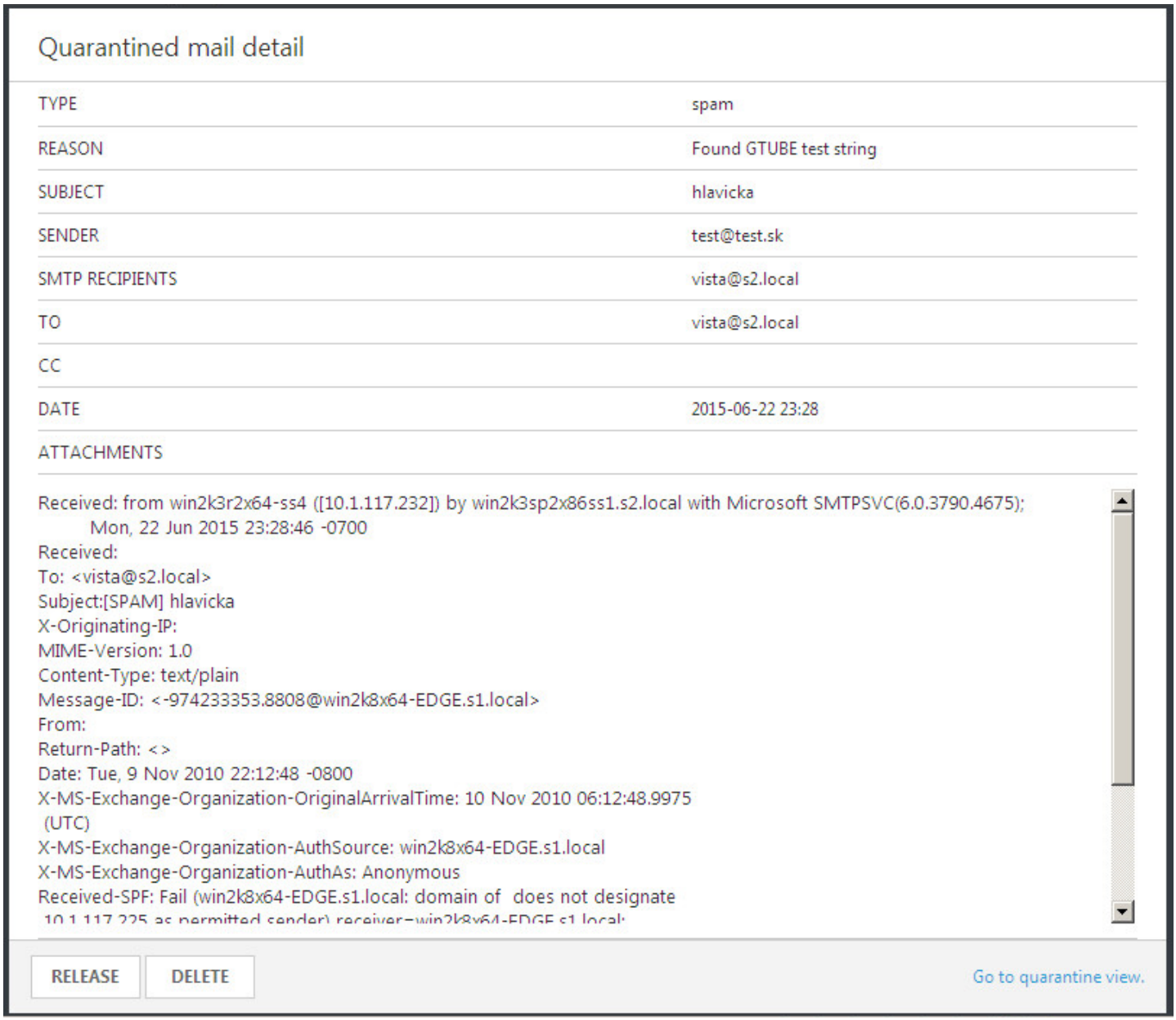


Восстановить: это действие отправляет сообщение электронной почты обратно к отправителю, используя каталог преобразования, и удаляет его из карантина. Нажмите кнопку **Отправить** для подтверждения.
Удалить: это действие удаляет сообщение из карантина. Нажмите кнопку **Отправить** для подтверждения.

Если щелкнуть элемент **Тема**, появляется всплывающее окно со сведениями о перемещенном в карантин сообщении (например, о **типе**, **причине**, **отправителе**, **дате** и **вложении**).



Чтобы отобразился заголовок сообщения, находящегося в карантине, щелкните **Показать заголовки**.



Если по отношению к перемещенному в карантин сообщению электронной почты нужно выполнить действие, выберите команду **Восстановить** или **Удалить**.

ПРИМЕЧАНИЕ. Чтобы полностью выйти из веб-интерфейса карантина почты, закройте браузер. Или же, чтобы вернуться к предыдущему экрану, щелкните **Перейти к представлению карантина**.

ВНИМАНИЕ! Если в браузере не удается получить доступ к веб-интерфейсу карантина почты или если появляется сообщение об ошибке `HTTP Error 403.4 - Forbidden` или похожее на него, проверьте, какой тип карантина выбран, и убедитесь, что это **локальный карантин** и что включен параметр **Включить веб-интерфейс**.

5.1.9.2 Почтовый ящик карантина и карантин MS Exchange

Если вы не хотите использовать локальный карантин, остаются два варианта, **почтовый ящик карантина** и **карантин MS Exchange**. Какой бы вариант вы ни выбрали, вам понадобится создать выделенного пользователя с почтовым ящиком (например, main_quarantine@company.com), в котором будут храниться перемещенные на карантин сообщения. Кроме того, с помощью этого пользователя и почтового ящика средство управления карантином почты будет отображать хранящиеся на карантине сообщения и управлять ими. Сведения об учетной записи этого пользователя нужно указать в разделе Параметры средства управления карантином.

ВНИМАНИЕ! Не рекомендуется использовать учетную запись администратора для почтового ящика карантина.

ПРИМЕЧАНИЕ. **Карантин MS Exchange** недоступен для Microsoft Exchange 2003. Для этого решения доступны только **локальный карантин** и **почтовый ящик карантина**.

- Если выбрать вариант **Карантин MS Exchange**, программа ESET Mail Security будет использовать **систему карантина Microsoft Exchange** (это относится к Microsoft Exchange Server 2007 и более новым версиям). В этом случае внутренний механизм Exchange используется для хранения потенциально зараженных сообщений и спама.

ПРИМЕЧАНИЕ. По умолчанию внутренний карантин не активируется в Exchange. Чтобы активировать его, следует открыть командную консоль Exchange и ввести следующую команду (замените `name@domain.com` на фактический адрес выделенного почтового ящика):

```
Set-ContentFilterConfig -QuarantineMailbox name@domain.com
```

- Выбирая **почтовый ящик карантина**, нужно указать адрес почтового ящика, в котором будут храниться сообщения, помещенные в карантин (например, main_quarantine@company.com).

ПРИМЕЧАНИЕ. Преимущество почтового ящика карантина и карантина MS Exchange по сравнению с локальным карантином заключается в том, что управление элементами карантина почты происходит централизованно, скольким бы серверам ни была назначена роль транспортного сервера-концентратора. В использовании почтового ящика карантина и карантина MS Exchange есть, тем не менее, и один недостаток: нежелательные и помещенные в карантин сообщения хранятся в базах данных почтовых ящиков Exchange, а карантином почты может управлять только администратор.

5.1.9.2.1 Параметры средства управления карантином

Адрес хоста: автоматически отображается, когда в локальной сети присутствует ваш сервер Exchange Server с ролью сервера клиентского доступа. Адрес хоста отображается автоматически и тогда, когда на сервере, на котором установлена программа ESET Mail Security, нет роли сервера клиентского доступа, но ее можно найти в AD. Если имя хоста не отображается, его можно ввести вручную. Автоматическое обнаружение не работает при использовании роли пограничного транспортного сервера.

ПРИМЕЧАНИЕ. IP-адрес не поддерживается. Используйте имя хоста сервера клиентского доступа.

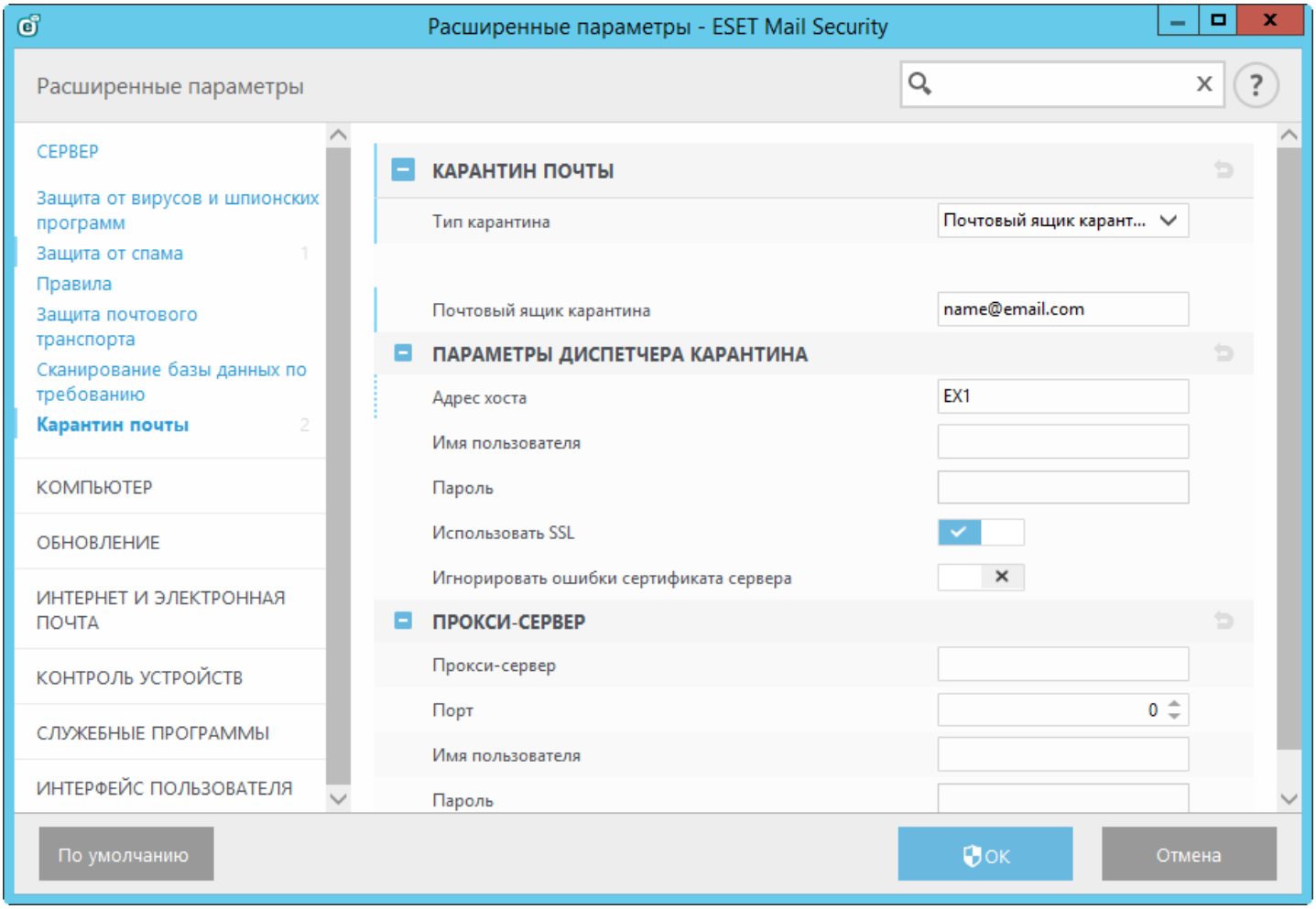
Имя пользователя: выделенная пользовательская учетная запись карантина, созданная для хранения сообщений, перемещенных на карантин (или учетная запись, имеющая доступ к такому почтовому ящику через функцию делегирования доступа). Для роли пограничного транспортного сервера, не являющегося частью домена, необходимо использовать адрес электронной почты целиком (например, main_quarantine@company.com).

Пароль: пароль учетной записи карантина.

Использовать SSL: нужно включить, если в IIS для веб-служб Exchange задано значение **Требовать SSL**. Если протокол SSL включен, сертификат сервера Exchange Server нужно импортировать в систему с ESET Mail Security (если роли Exchange Server активированы на разных серверах). В IIS параметры веб-служб Exchange можно найти в расположении *Sites/Default web site/EWS/SSL Settings*.

ПРИМЕЧАНИЕ. Параметр **Использовать SSL** можно отключать, только если в IIS веб-службы Exchange настроены так, чтобы не требовать SSL.

Игнорировать ошибки сертификата сервера: игнорируются ошибки «самозаверяющий», «неверное имя в сертификате», «неверное использование», «истекший срок действия».



5.1.9.2.2 Прокси-сервер

Если вы используете прокси-сервер в качестве посредника между сервером Exchange Server с ролью сервера клиентского доступа и сервером Exchange Server, на котором установлен продукт ESET Mail Security, укажите параметры этого прокси-сервера. Это нужно потому, что программа ESET Mail Security соединяется с интерфейсом API веб-служб Exchange по протоколу HTTP или HTTPS. В противном случае почтовый ящик карантина и карантин MS Exchange не будут функционировать.

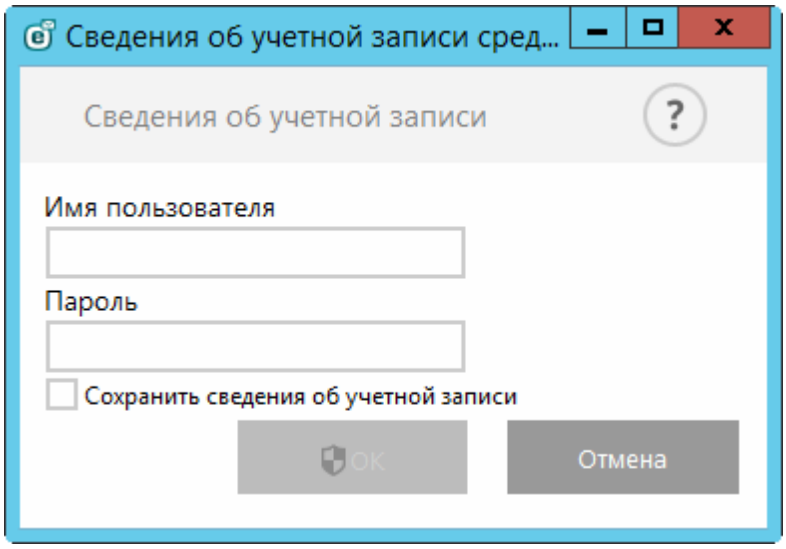
Прокси-сервер: введите IP-адрес или имя используемого вами прокси-сервера.

Порт: укажите номер порта прокси-сервера.

Имя пользователя, Пароль: введите учетные данные, если для вашего прокси-сервера нужна проверка подлинности.

5.1.9.3 Сведения об учетной записи средства управления карантином

Это диалоговое окно отображается, если при настройке учетной записи вы не указали **сведения о средстве управления карантином**. Укажите учетные данные пользователя, у которого есть доступ в **почтовый ящик карантина**, и нажмите кнопку **ОК**. Или же нажмите клавишу F5, чтобы войти в раздел **Дополнительные настройки**, и последовательно выберите **Сервер** > **Карантин почты** > Параметры средства управления карантином. Введите **имя пользователя** и **пароль** для своего почтового ящика карантина.



Чтобы, открывая средство управления карантином, сохранить на будущее параметры учетной записи, выберите **Сохранить сведения об учетной записи**.

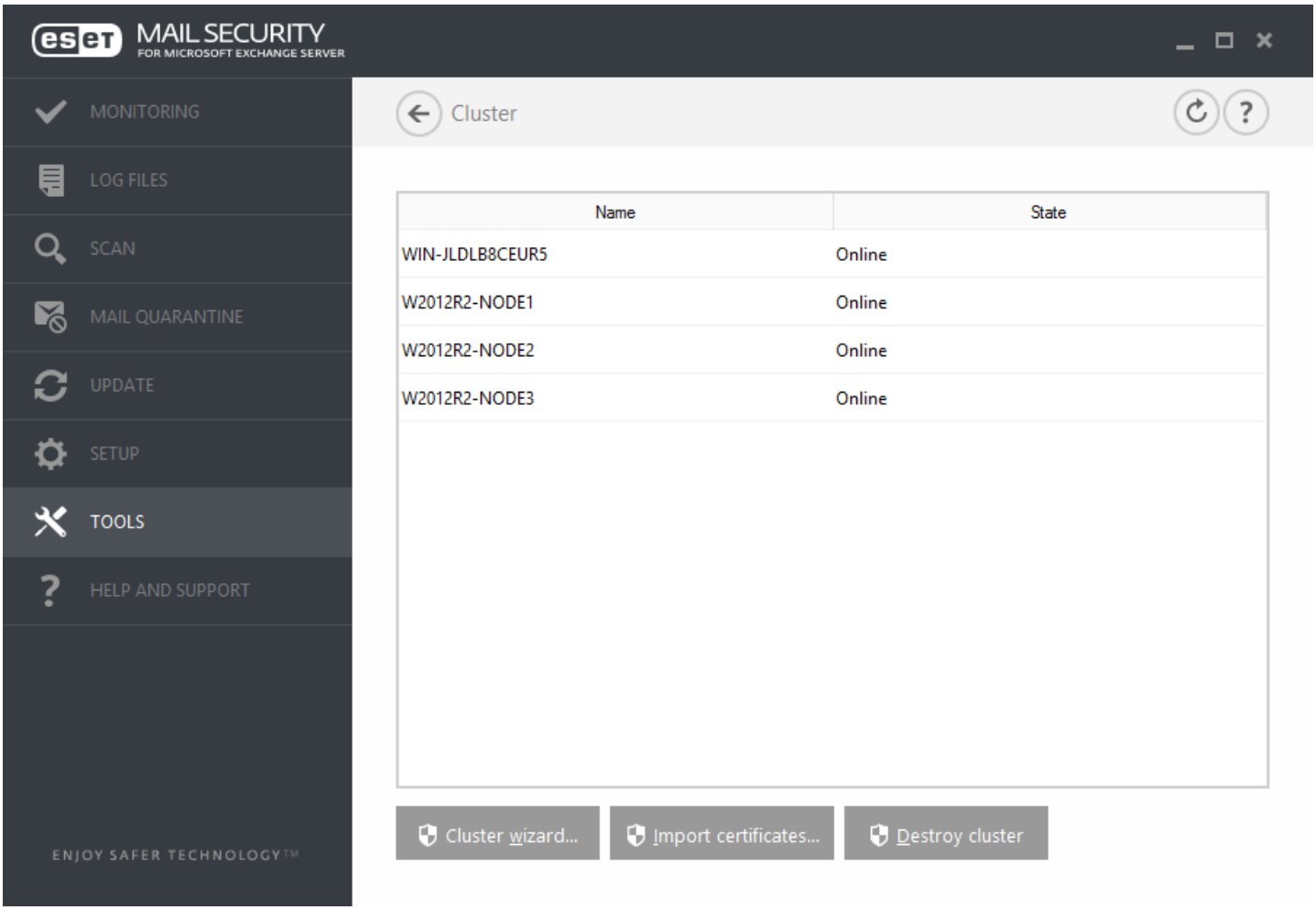
5.1.10 Кластер

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

Эта инфраструктура обеспечивает взаимодействие между серверными продуктами ESET и позволяет им обмениваться такими данными, как конфигурация и оповещения, а также выполнять синхронизацию данных, необходимых для надлежащей 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.

Автоопределение: автоматическое определение узлов, уже входящих в отказоустойчивый кластер Windows или кластер NLB, и добавление их в кластер ESET.
Обзор: узлы можно добавить вручную с помощью ввода имен 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 Mail Security на каждом их них. Это выполняется автоматически в процессе настройки кластера ESET.

Учетные данные, необходимые для удаленной установки программы ESET Mail 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 ESET Mail Security на узлы кластера ESET.

Если необходимо, кластер ESET можно с легкостью демонтировать, выбрав команду **Уничтожение кластера**. 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 Mail 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.

Дополнительную информацию о настройке кластера ESET см. в разделе Рабочий кластер.

5.1.10.1 Мастер кластеров — стр. 1

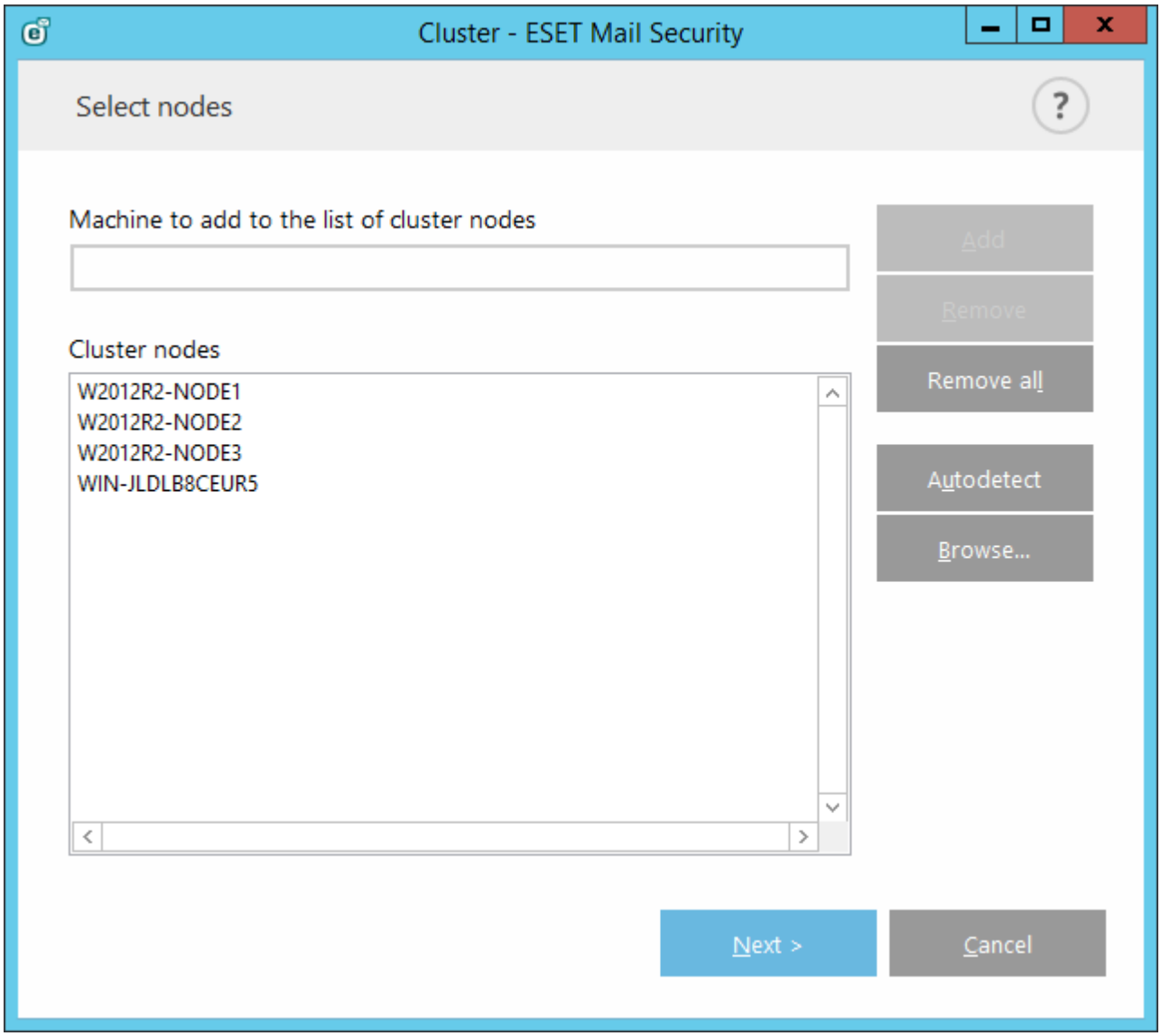
При настройке кластера ESET необходимо начать с добавления узлов. Чтобы добавить узлы, можно использовать функцию **Автоопределение** или команду **Обзор**. Кроме того, в текстовом поле можно ввести имя сервера и нажать кнопку **Добавить**.

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. Если в кластер ESET необходимо добавить только определенные узлы, после создания списка недавно добавленных узлов из него можно удалить ненужные.

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**.

Текущие **узлы кластера**, которые будут добавлены в кластер ESET после нажатия кнопки **Далее**.



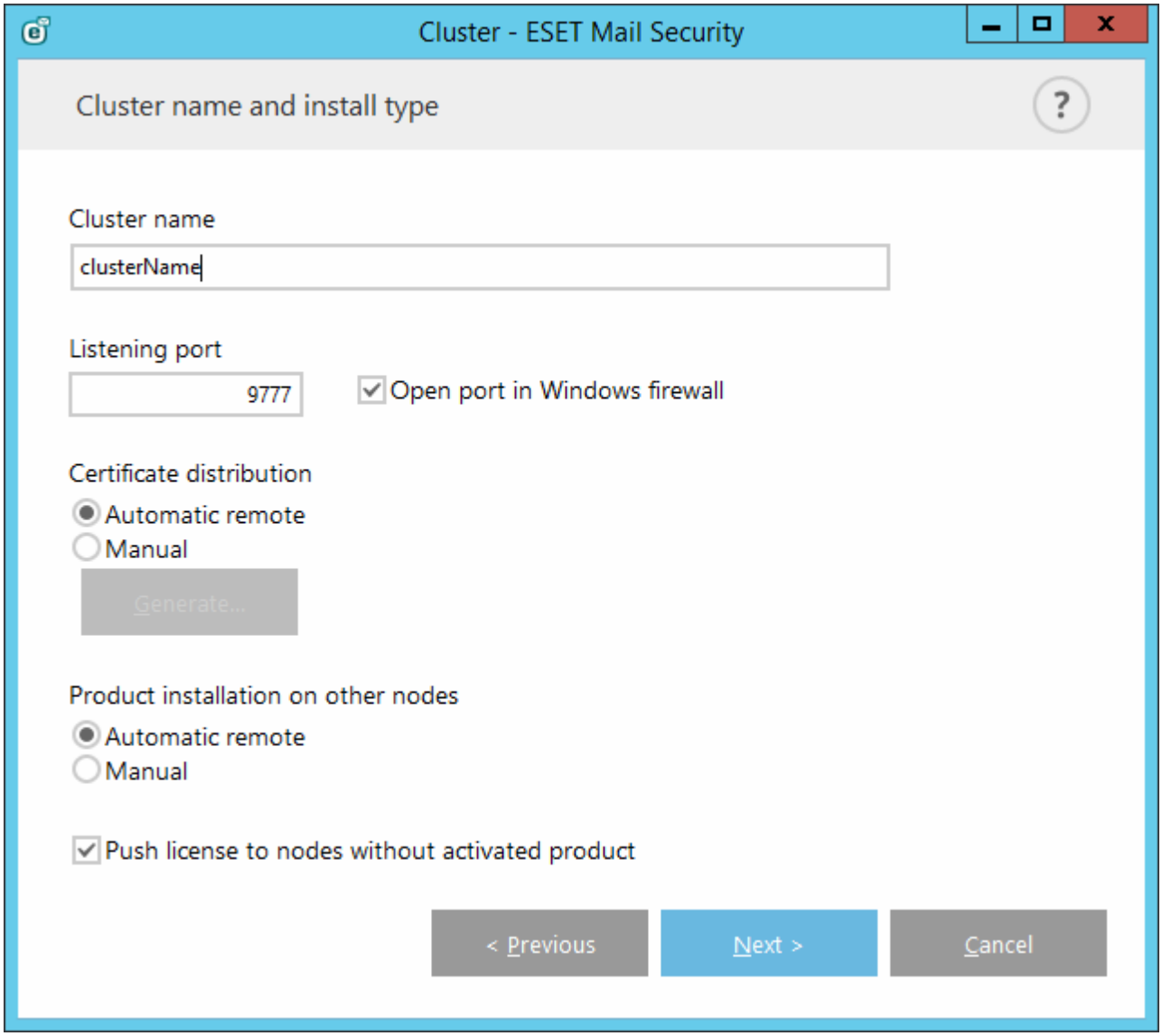
Чтобы изменить **узлы кластера** в списке, выберите узел, который следует удалить, и используйте команду **Удалить**, а чтобы полностью очистить список, выберите команду **Удалить все**.

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.

5.1.10.2 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 файерволе Windows: если установлен этот флажок, в файерволе 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 Mail Security на каждый узел будет выполнена автоматически (если операционная система узла поддерживает архитектуру, которой соответствует продукт).
Вручную: этот параметр дает возможность установить программу ESET Mail Security вручную (например, если на некоторых узлах используется другая архитектура ОС).

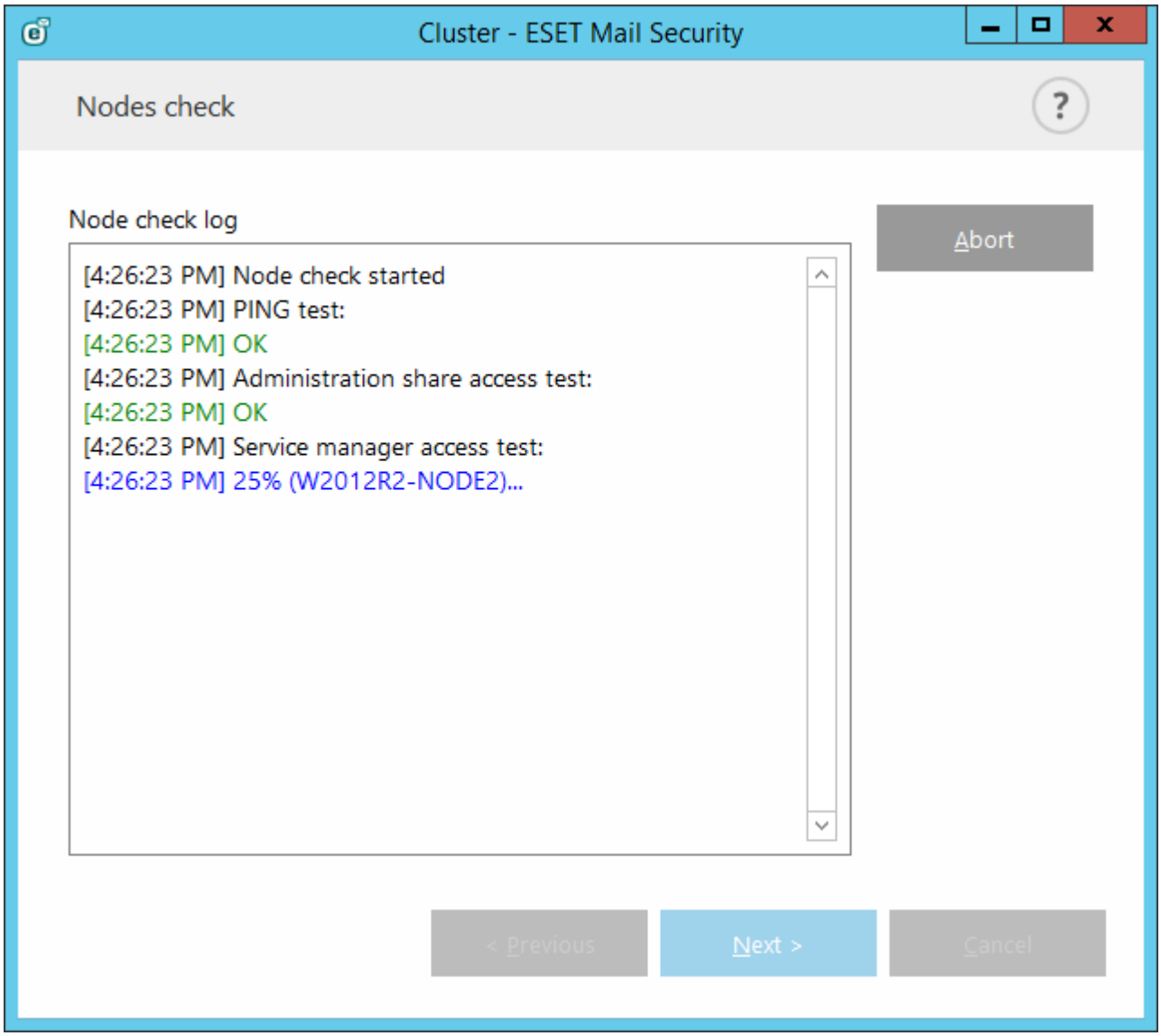
Передать лицензию на узлы без активированного продукта: программа ESET Mail Security активируется при проверке узлов.

ПРИМЕЧАНИЕ. Если необходимо создать кластер ESET с разными архитектурами ОС (32- и 64-разрядная), программу ESET Mail Security следует установить вручную. Этот параметр будет определен на следующих этапах, а данные сведения отобразятся в окне журнала.

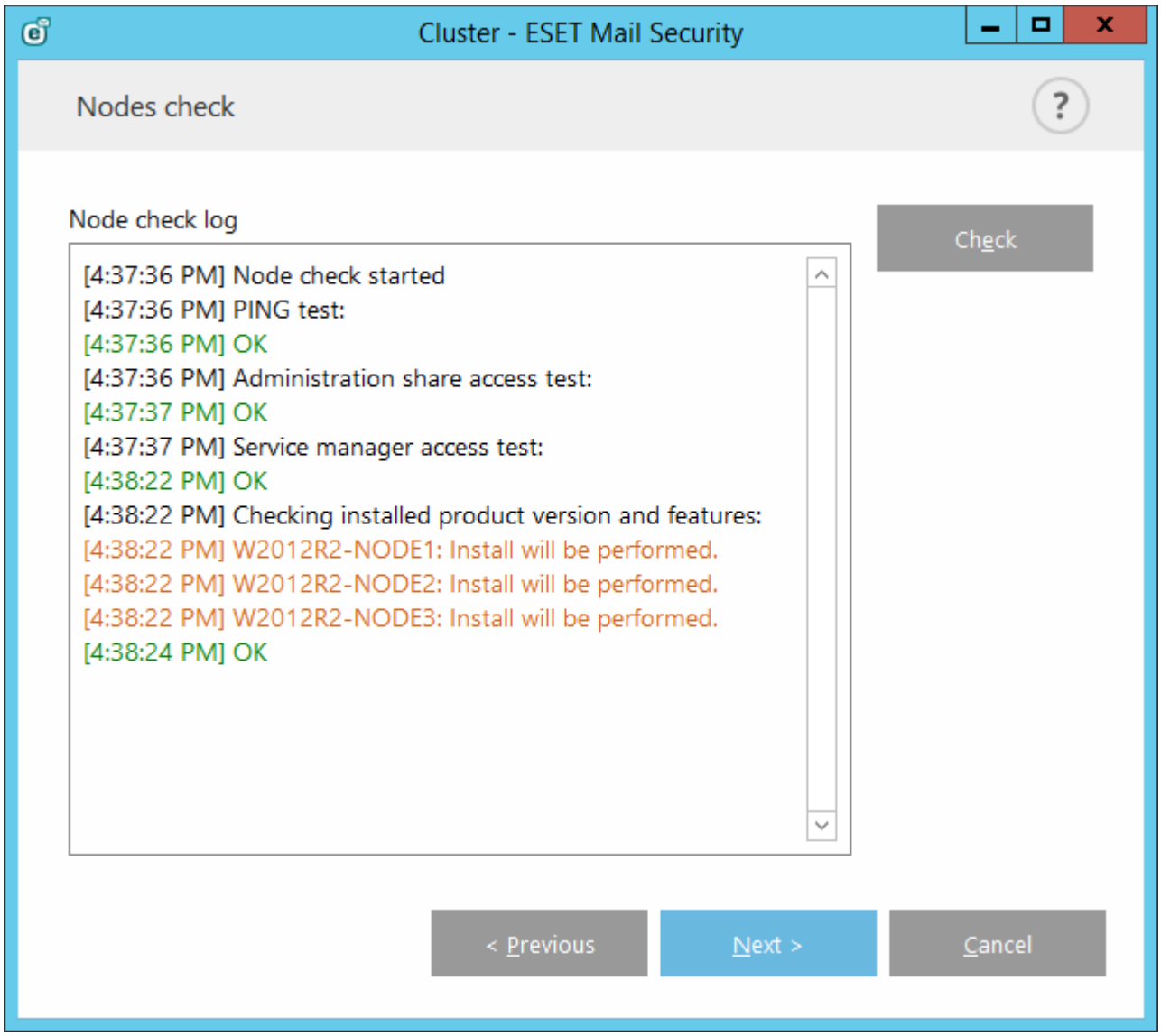
5.1.10.3 Мастер кластеров — стр. 3

После указания деталей установки выполняется проверка узлов. В **журнале проверки узлов** отобразятся сведения о следующих проверках:

- 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;
- проверка правильности установленной версии продукта или отсутствия продукта (только если выбрана автоматическая установка);
- проверка наличия новых сертификатов.

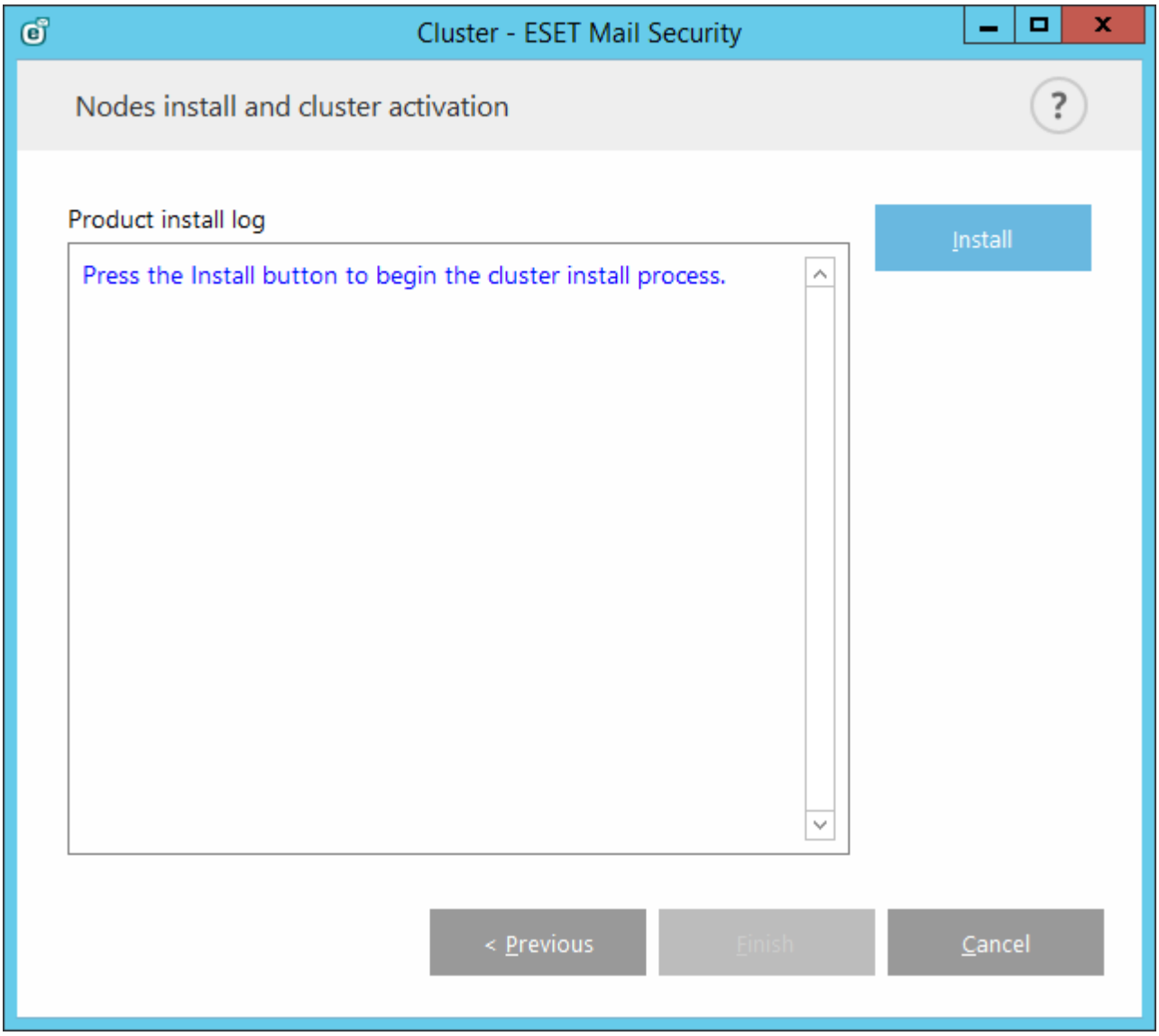


После завершения проверки узлов отобразится следующий отчет.



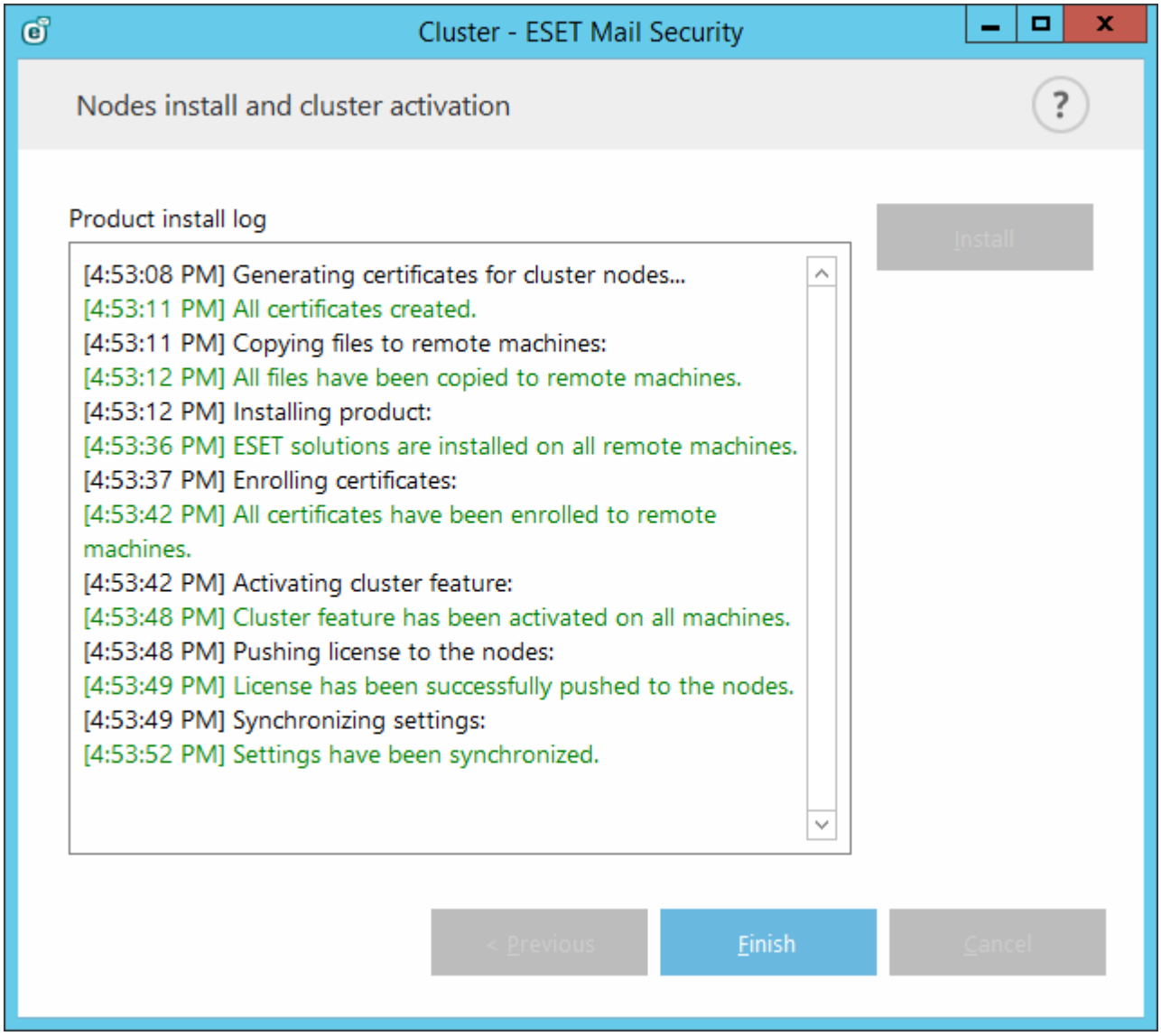
5.1.10.4 Мастер кластеров — стр. 4

Когда продукт на удаленный компьютер нужно установить во время инициализации кластера ESET, пакет установщика проверяет каталог %ProgramData%\ESET\<Produt_name>\Installer на наличие программы установки. Если установочный файл не найден в этом каталоге, отображается запрос на поиск его вручную.

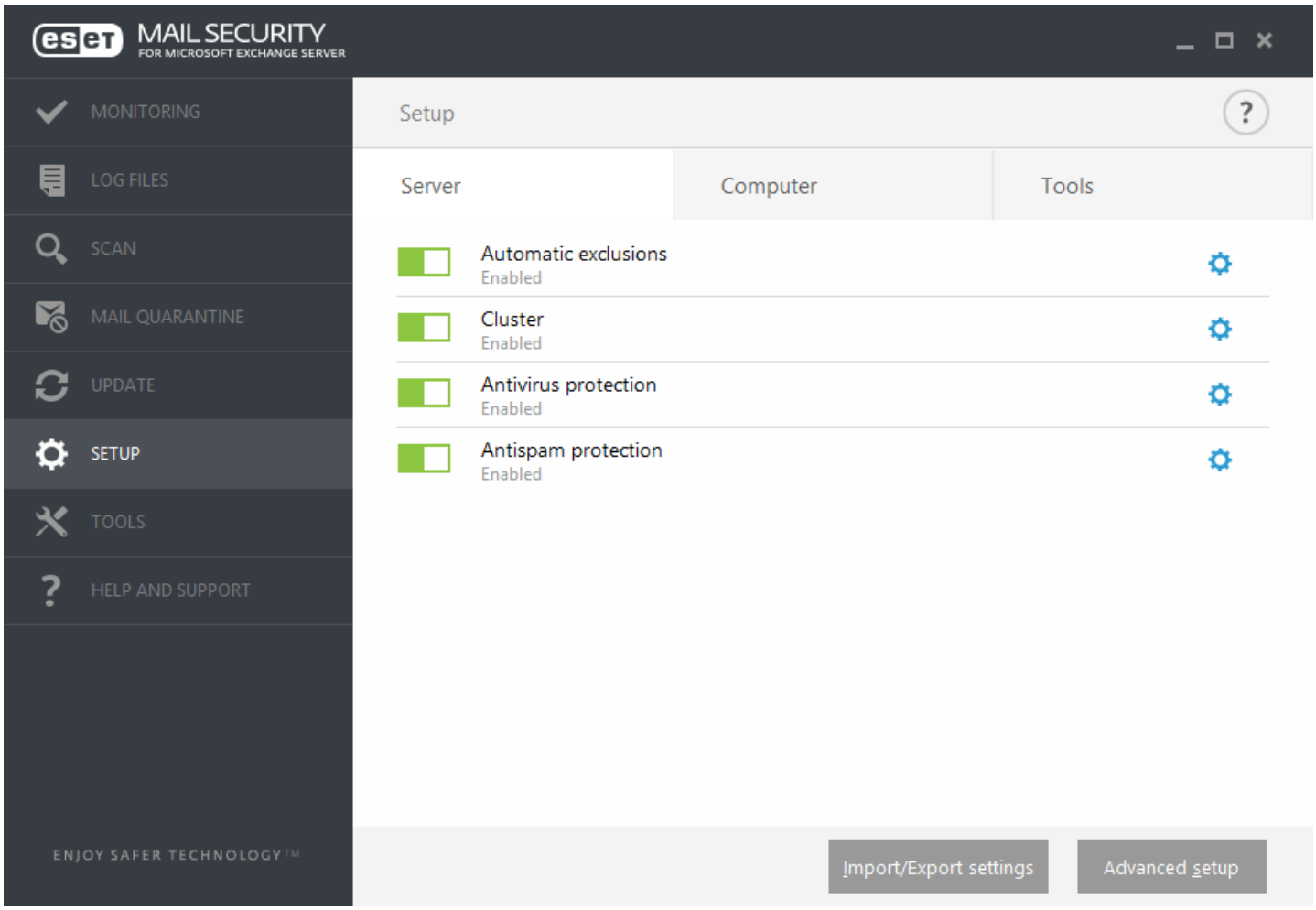


ПРИМЕЧАНИЕ. Если выполняется автоматическая удаленная установка на узел с другой платформой (конфликт между 32- и 64-разрядной платформами), для такого узла будет рекомендована ручная установка.

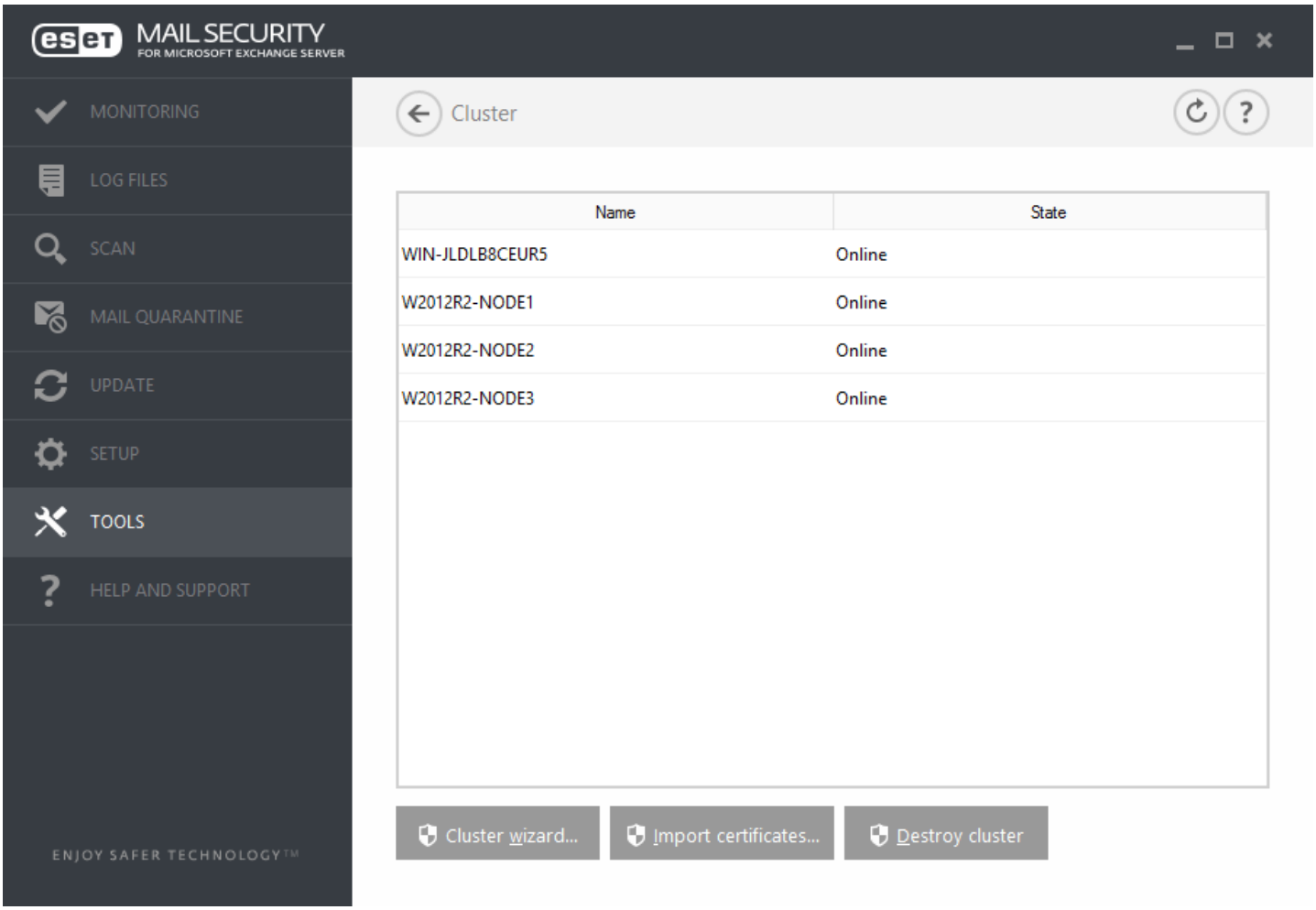
ПРИМЕЧАНИЕ.: Если на некоторых узлах используется старая версия ESET Mail Security, то перед созданием кластера нужно установить на эти компьютеры более новую версию ESET Mail Security. Это может привести к автоматической перезагрузке этих компьютеров. В таком случае отобразится предупреждение.



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



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



Импорт сертификатов

- Перейдите к папке, содержащей сертификаты (создается при использовании мастера кластеров). Выберите файл сертификата и нажмите кнопку **Открыть**.

5.2 Компьютер

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

- Защита файловой системы в режиме реального времени
- Сканирование компьютера по требованию
- Сканирование в состоянии простоя
- Сканирование файлов, исполняемых при запуске системы
- Съемные носители
- Защита документов
- HIPS

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

- Потенциально нежелательные приложения не всегда являются вредоносными, однако могут негативно повлиять на производительность компьютера.
  Дополнительную информацию о приложениях этого типа см. в глоссарии.
- Потенциально опасные приложения — это определение относится к законному коммерческому программному обеспечению, которое может быть использовано для причинения вреда. К потенциально

опасным приложениям относятся средства удаленного доступа, приложения для взлома паролей и клавиатурные шпионы (программы, регистрирующие каждое нажатие пользователем клавиш на клавиатуре). По умолчанию этот параметр отключен.
Дополнительную информацию о приложениях этого типа см. в глоссарии.

- **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 скрываться от операционной системы. Это означает, что их невозможно обнаружить при помощи обычных технологий проверки.

Функция исключения процессов позволяет исключить те или иные 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. Сведения о том, как исключить объект из сканирования, см. в разделе Исключения.

5.2.1 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 программа ESET Mail 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. 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 Mail 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.

5.2.2 Исключения для процессов

Эта функция позволяет исключить процессы приложений 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 Mail 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.

ПРИМЕЧАНИЕ. Исключения для процессов — это исключения только из сканирования на наличие вирусов при доступе. Например, 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.

5.2.3 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, 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 Mail 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.

1. 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** > **Компьютер** > **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.

2. Если деактивировать исключение для приложения или операционной системы, соответствующие критические файлы и папки остаются в списке файлов, исключенных из сканирования (**Дополнительные настройки** > **Компьютер** > **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** > **Компьютер** > **Основное** > **Исключения** > **Изменить**).

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

Автоматические исключения для серверных приложений и операционных систем выбираются на основе рекомендаций Microsoft. Дополнительные сведения см. в следующих статьях базы знаний Майкрософт:

- Рекомендации по проверке корпоративных компьютеров с поддерживаемыми версиями Windows на наличие вирусов
- Рекомендации по устранению неполадок на компьютере с сервером Exchange Server, использующем антивирусные программы
- Поиск вирусов на файловом уровне в Exchange Server 2007
- Антивирусная программа в операционной системе на серверах Exchange

5.2.4 Общий локальный кэш

Общий локальный кэш повышает производительность в виртуализированных средах, устраняя повторное сканирование файлов 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 программа ESET Mail 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).

5.2.5 Быстродействие

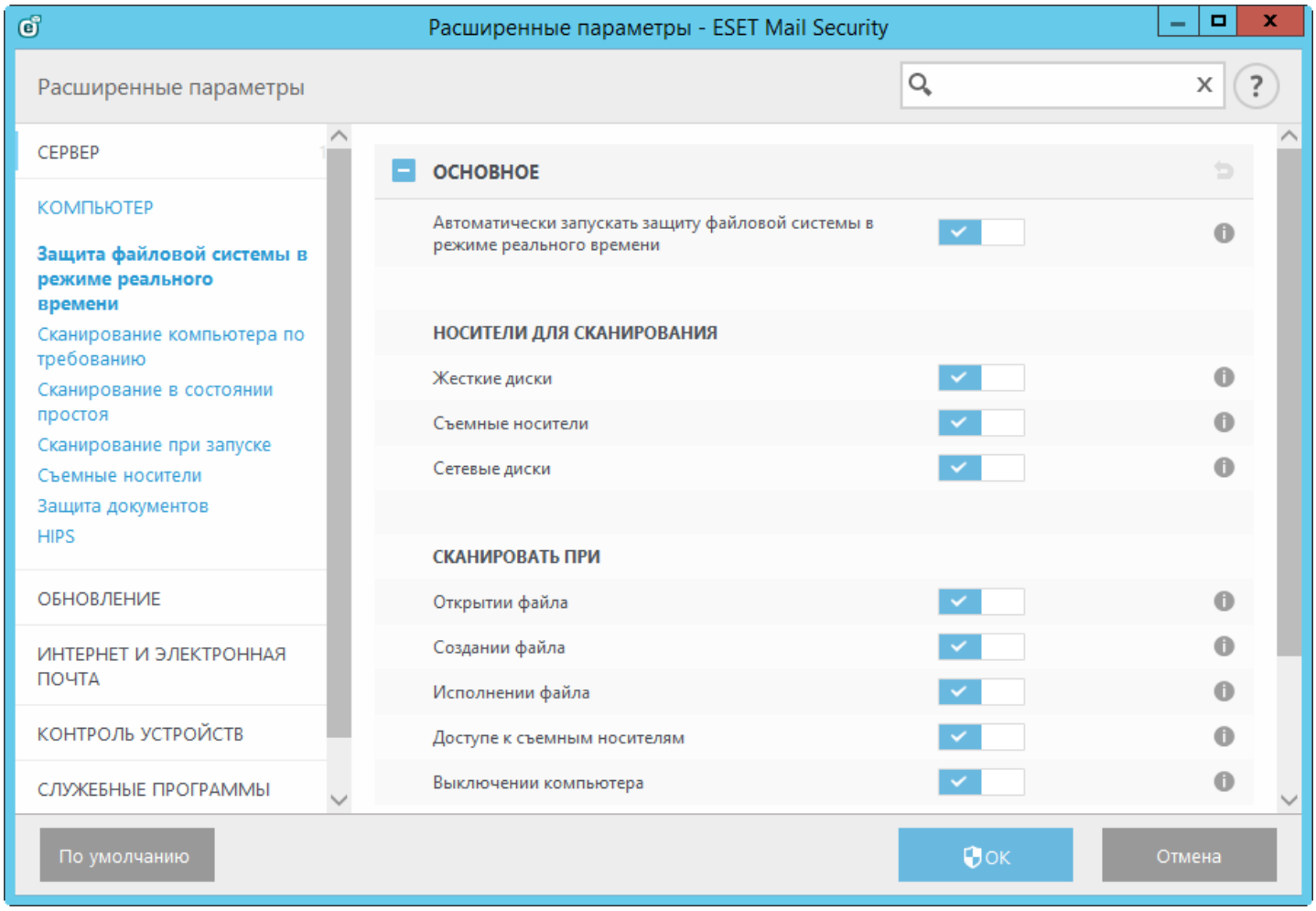
Количество независимых модулей сканирования ThreatSense, одновременно используемых средствами антивирусной и антишпионской защиты.

Если других ограничений нет, рекомендуется увеличить количество модулей сканирования ThreatSense согласно этой формуле: *количество модулей сканирования ThreatSense = (количество физических ЦП x 2) + 1*.

ПРИМЕЧАНИЕ. Диапазон приемлемых значений — это 1–20, поэтому можно использовать максимум 20 модулей сканирования ThreatSense.

5.2.6 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-устройства хранения, Bluetooth-устройства и т. п.
Сетевые диски — сканируются все подключенные сетевые диски.

Рекомендуется оставить параметры по умолчанию, а изменять их только в особых случаях (например, если сканирование определенных носителей приводит к значительному замедлению обмена данными).

- **Сканировать при**

По умолчанию все файлы сканируются при открытии, создании или исполнении. Рекомендуется не изменять настройки по умолчанию, поскольку они обеспечивают максимальную защиту компьютера в режиме реального времени.

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

Защита файловой системы в 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 **Компьютер** > **Защита файловой системы в реальном времени**. Последовательно щелкните элементы **Параметры ThreatSense** > **Другое** и снимите или установите флажок **Включить интеллектуальную оптимизацию**.

5.2.6.1 Исключения

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

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).

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.

Примеры

- 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 известна только первая буква имени (скажем, «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 расширенные параметры** > **Исключить из обнаружения**), либо в разделе **Настройки** > **Карантин**, щелкнув правой кнопкой мыши файл на карантине и выбрав в контекстном меню пункт **Восстановить и исключить из обнаружения**.

Элементы управления

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

5.2.6.1.1 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.

5.2.6.1.2 Формат исключений

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

Примеры

- 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 известна только первая буква имени (скажем, «D»), следует использовать следующий формат: «D????.exe». Вопросительные знаки замещают отсутствующие (неизвестные) символы.

5.2.6.2 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 дополнительных настроек 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.

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

Параметры ThreatSense хорошо оптимизированы для каждого из модулей, а их изменение значительно влияет на поведение системы. Например, 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 злонамеренной активности программ с помощью специального алгоритма. Главным достоинством этого метода является способность идентифицировать вредоносные программы, сведения о которых отсутствуют в существующей базе данных сигнатур вирусов. Недостатком же является вероятность (очень небольшая) ложных тревог.
- **Расширенный эвристический анализ/распределенные сетевые атаки/интеллектуальные сигнатуры** — метод расширенной эвристики базируется на уникальном эвристическом алгоритме, разработанном компанией ESET, оптимизированном для обнаружения компьютерных червей и троянских программ и написанном на языках программирования высокого уровня. Использование расширенной эвристики значительным образом увеличивает возможности продуктов ESET по обнаружению угроз. С помощью сигнатур осуществляется точное обнаружение и идентификация вирусов. Система автоматического обновления обеспечивает наличие новых сигнатур через несколько часов после обнаружения угрозы. Недостатком же сигнатур является то, что они позволяют обнаруживать только известные вирусы (или их незначительно модифицированные версии).
-

Очистка

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

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

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

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

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

ВНИМАНИЕ! Если сервер 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 (режим **Без очистки**). Какой бы уровень очистки ни был выбран, сканирование 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, вы можете 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, журнал будет содержать сведения также о незараженных файлах из архива.
- **Включить интеллектуальную оптимизацию**: при включенной оптимизации Smart используются оптимальные параметры для обеспечения самого эффективного уровня сканирования с сохранением максимально высокой скорости. Разные модули защиты выполняют интеллектуальное сканирование, применяя отдельные методы для различных типов файлов. Если оптимизация Smart отключена, при сканировании используются только пользовательские настройки ядра ThreatSense каждого модуля.
- **Сохранить отметку о времени последнего доступа**: установите этот флажок, чтобы 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

- **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*.

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.

5.2.6.2.1 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.

Иногда нужно исключить файлы, если сканирование файлов, принадлежащих к определенным типам, препятствует нормальной работе программы, которая использует соответствующие расширения. Например, может быть полезно исключить расширения EDB, EML и TMP при использовании серверов Microsoft Exchange.

С помощью кнопок **Добавить** и **Удалить** можно изменять содержимое списка, разрешая или запрещая сканирование определенных расширений. 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**.

Использовать можно и такие специальные символы, как «*» (звездочка) и «?» (знак вопроса) (вопросительный знак). Символ звездочки обозначает любую последовательность символов, а вопросительный знак — любой отдельный символ.

5.2.6.2.2 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 Live Grid, чтобы уменьшить воздействие на производительность системы.

5.2.6.2.3 Уровни очистки

Защита в реальном времени предусматривает три уровня очистки (для доступа к ним выберите элемент **Параметры ThreatSense** в разделе **Защита файловой системы в реальном времени**, а затем нажмите кнопку **Очистка**).

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

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

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

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

ВНИМАНИЕ! Если сервер 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 (режим **Без очистки**). Какой бы уровень очистки ни был выбран, сканирование выполняется в режиме только для чтения.

5.2.6.2.4 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 Mail Security все параметры оптимизированы для максимальной защиты системы. Чтобы восстановить параметры по умолчанию, щелкните возле каждой вкладки в окне (**Дополнительные настройки** > **Компьютер** > **Защита файловой системы в режиме реального времени**).

5.2.6.2.5 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.

5.2.6.2.6 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 установить этот флажок, перейдите в раздел **Дополнительные настройки** (**F5**) и последовательно выберите элементы **Компьютер** > **Защита файловой системы в реальном времени**> **Обычная**. 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.

5.2.6.2.7 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.

5.2.6.2.8 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.

5.2.6.2.9 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).

Когда передавать: 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 **Во время 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.

5.2.7 Сканирование компьютера по требованию и сканирование Hyper-V

В этом разделе можно выбрать параметры сканирования.

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

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

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.

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

5.2.7.1 Средство запуска выборочного сканирования и сканирования Hyper-V

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

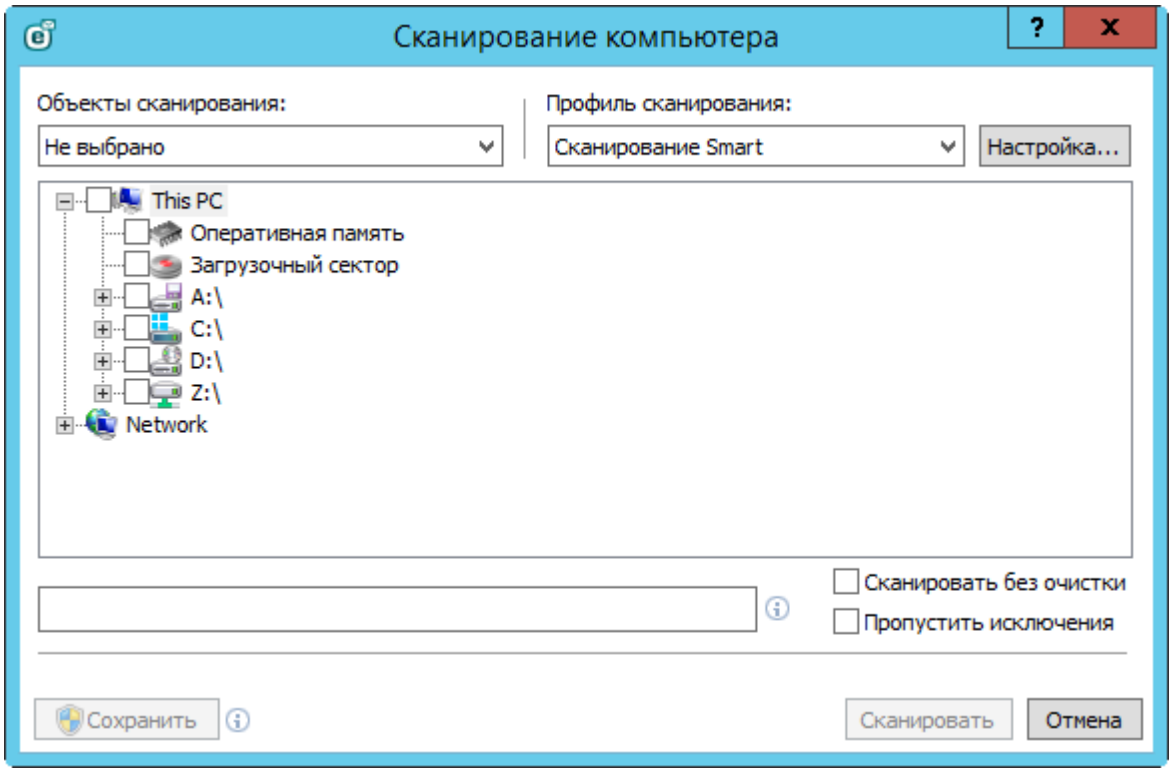
ПРИМЕЧАНИЕ. Этот переключатель объектов сканирования применяется к выборочному сканированию и к сканированию Hyper-V.

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.

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

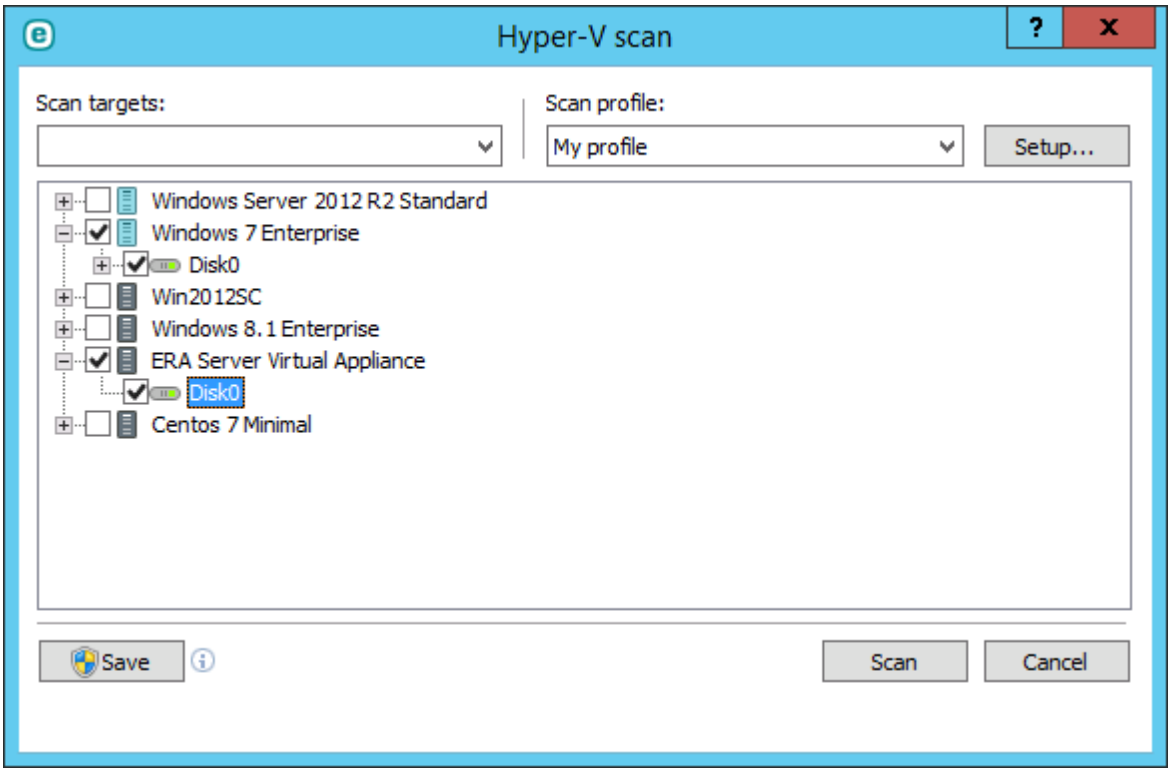
Всплывающее окно **Выборочное сканирование**:



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). Кроме того, 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 **Другое** области интерфейса Настройка параметров модуля ThreatSense.

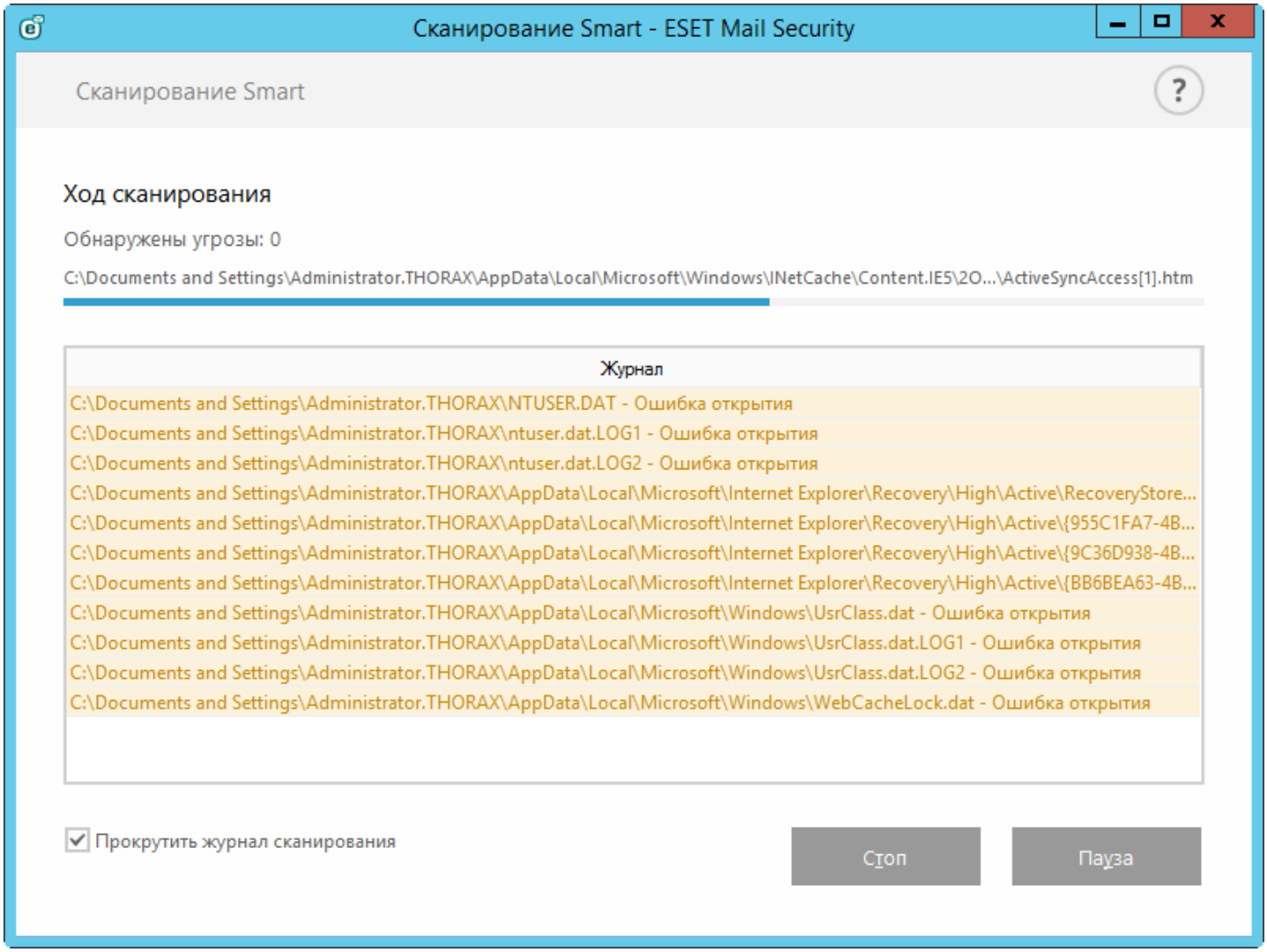
Чтобы сохранить изменения в выборе объектов сканирования, в том числе объектов, выбранных в дереве каталогов, нажмите кнопку **Сохранить**.

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.

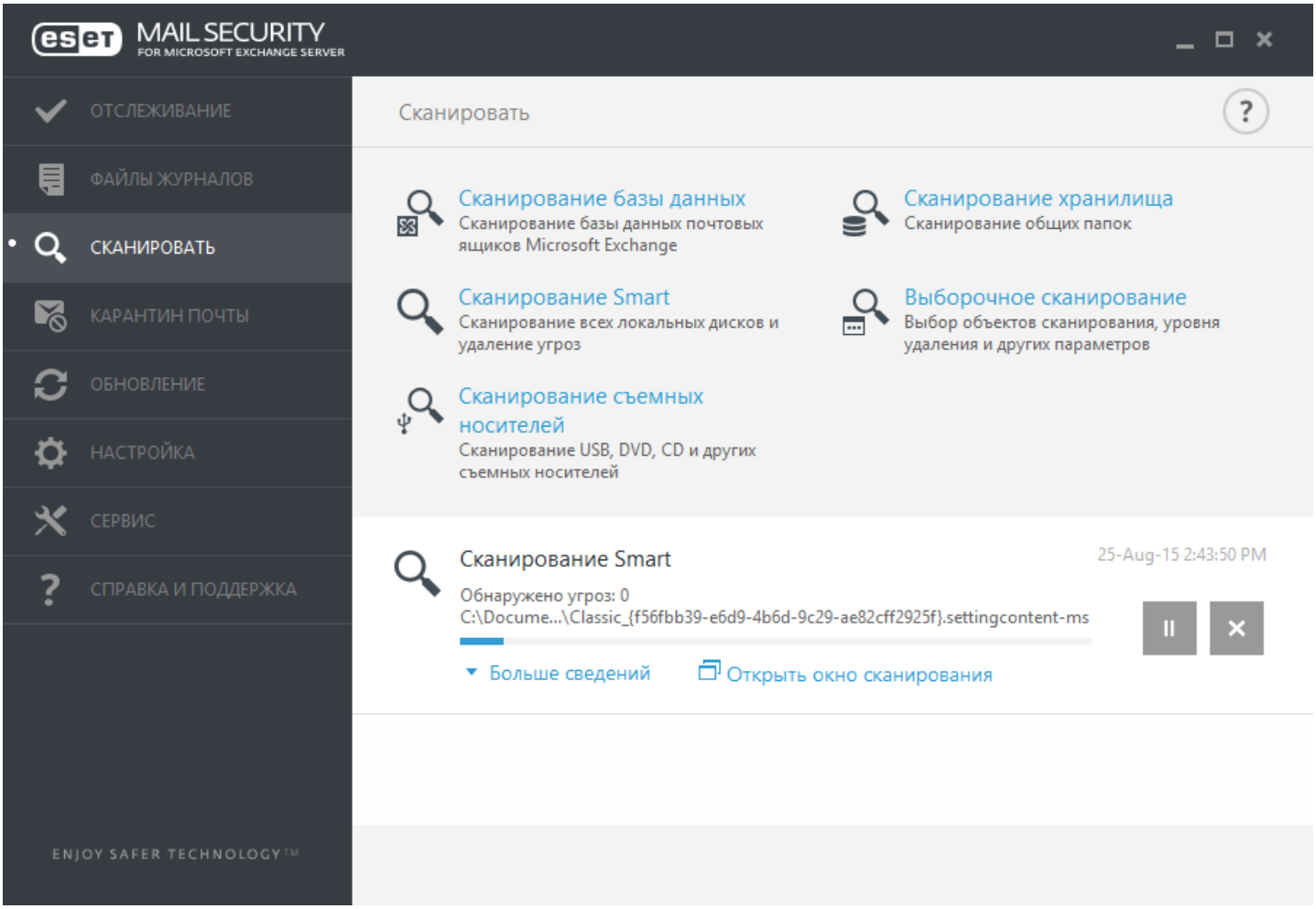
5.2.7.2 Ход сканирования

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 кнопку «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.



5.2.7.3 Диспетчер профилей

Диспетчер профилей используется в двух разделах ESET Mail 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 **Компьютер** > **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. Создавать и использовать собственные пользовательские профили (т. е. профили, отличные от профиля по умолчанию **Мой профиль**) следует только в том случае, если компьютер подключается к серверам обновлений разными способами.

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

5.2.7.4 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.

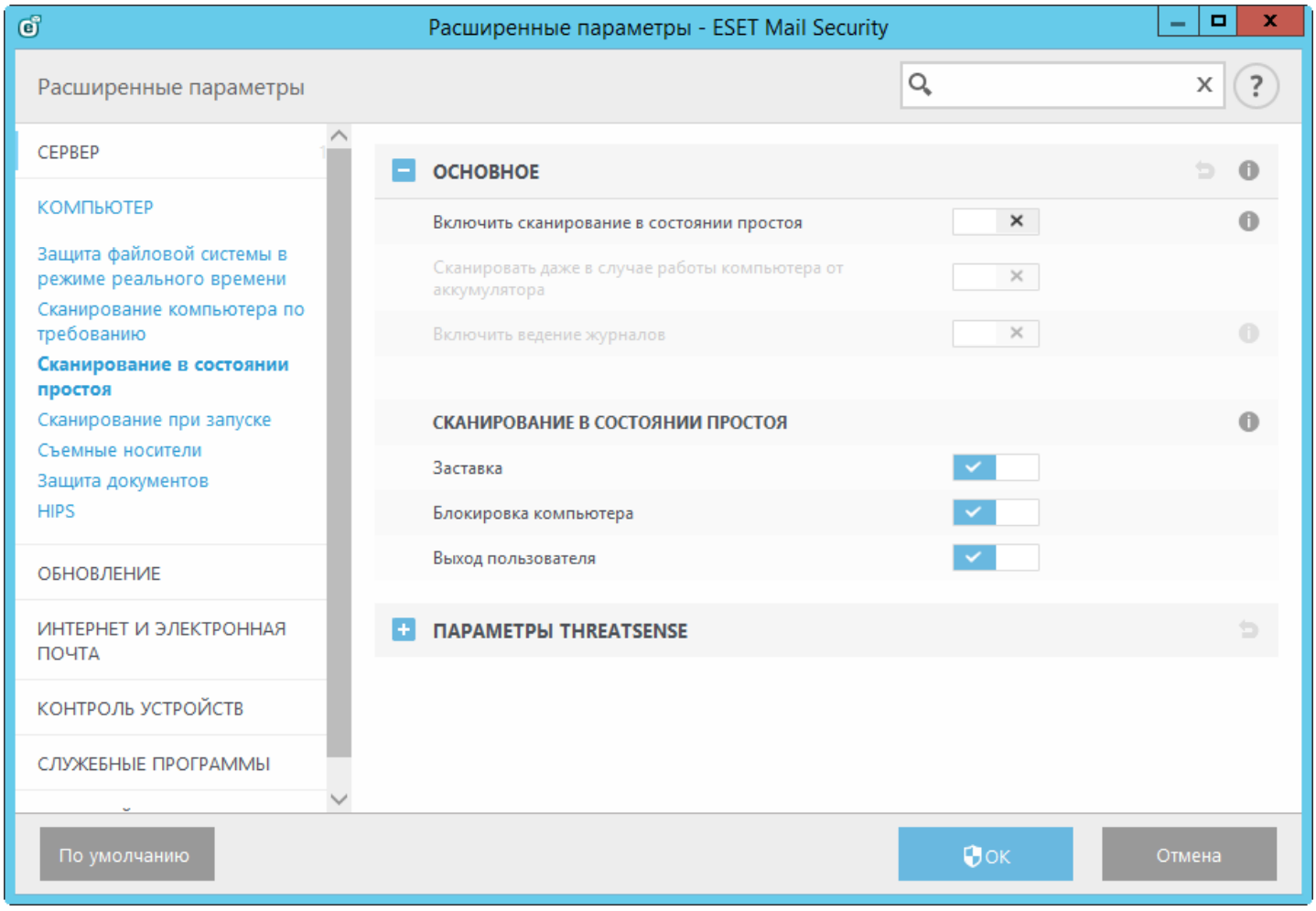
5.2.7.5 Приостановка запланированного процесса сканирования

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

5.2.8 Сканирование в состоянии простоя

Вы можете включить сканирование в состоянии простоя с помощью пункта **Дополнительные настройки** в разделе **Компьютер** > **Сканирование в состоянии простоя** > **Основное**. Чтобы разрешить использование этой функции, установите переключатель возле элемента **Включить сканирование в состоянии простоя** на «Вкл.». 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».



В разделе «Дополнительные настройки» выберите параметр **Включить ведение журналов**, чтобы результаты сканирования компьютера регистрировались в разделе Файлы журналов (в раскрывающемся меню **Журнал** главного окна программы последовательно щелкните элементы **Сервис** > **Файлы журналов** > **Сканирование компьютера**).

Обнаружение в состоянии простоя будет запущено 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).

5.2.9 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.

5.2.9.1 Автоматическая проверка файлов при запуске системы

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

Раскрывающееся меню **Уровень 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)

Также существуют две особые группы **уровней 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.

5.2.10 Съемные носители

Программа ESET Mail 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 будет выполняться при подключении съемного носителя (компакт-диска, DVD-диска, USB-устройства) к компьютеру. Если выбран вариант **Показать параметры сканирования**, на экран будет выведено уведомление, с помощью которого можно выбрать нужное действие.

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

Когда вставляется съемный носитель, отображается 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 программе ESET Mail 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.

5.2.11 Защита документов

Функция защиты документов сканирует документы Microsoft Office перед их открытием, а также проверяет файлы, автоматически загружаемые браузером Internet Explorer, такие как элементы Microsoft ActiveX. Функция защиты документов обеспечивает безопасность в дополнение к функции защиты файловой системы в 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 дополнительных настроек, и щелкните **Компьютер** > **Защита документов** в дереве дополнительных настроек.
- Дополнительные сведения о параметрах защиты документов см. в разделе Параметры Threatsense.

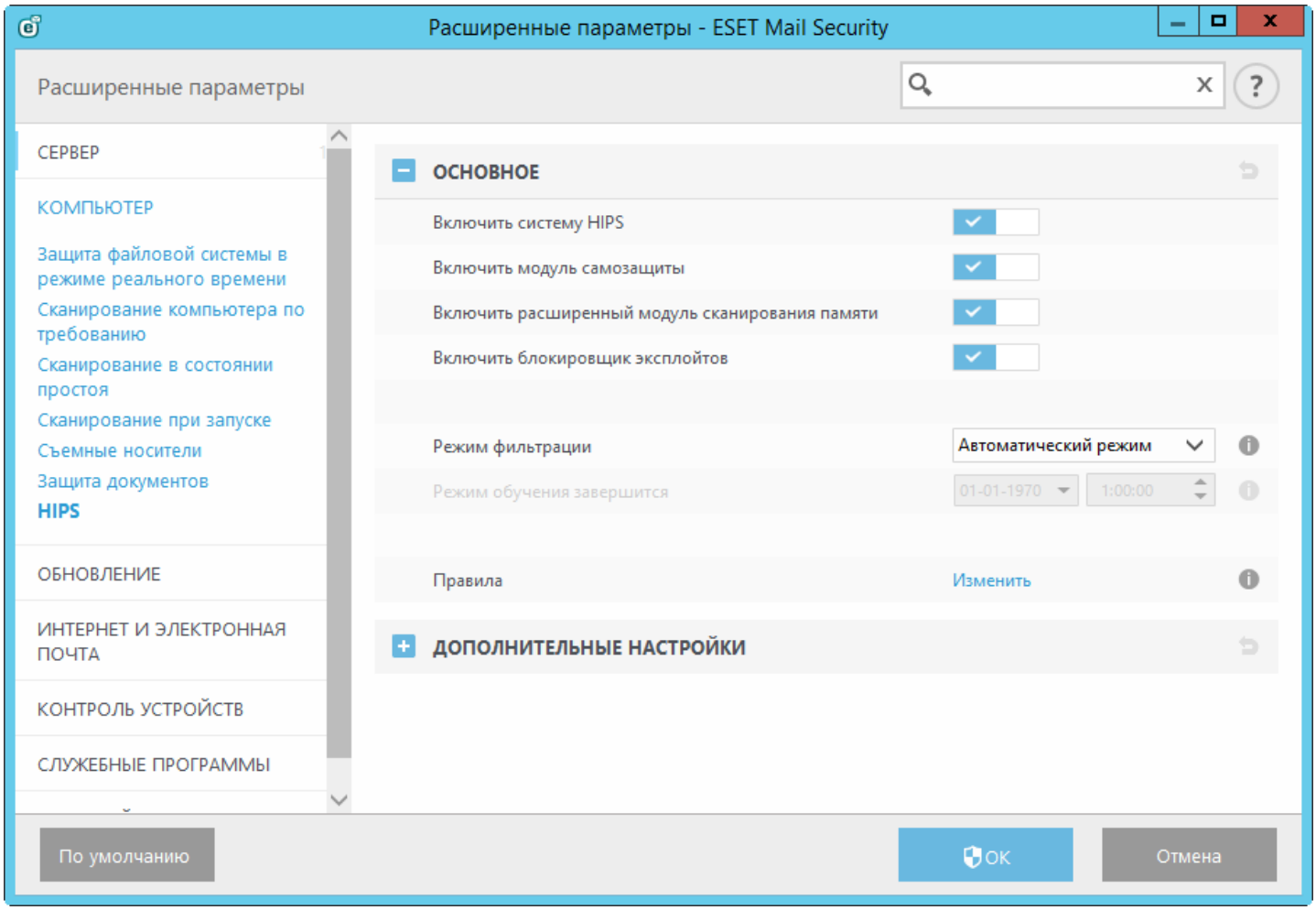
Эта функция активируется приложениями, в которых используется Microsoft Antivirus API (например, Microsoft Office 2000 и более поздние версии или Microsoft Internet Explorer 5.0 и более поздние версии).

5.2.12 HIPS


Изменять параметры системы HIPS должны только опытные пользователи. Неправильная настройка этих параметров может привести к нестабильной работе системы.

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.

Настройки HIPS доступны в разделе **Дополнительные настройки** (F5) > **Компьютер** > **HIPS**. Состояние системы HIPS (включена или отключена) отображается в главном окне ESET Mail Security, в области **Настройки**, в правой части раздела **Компьютер**.



В программе ESET Mail 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. Если в раскрывающемся меню режимов фильтрации HIPS выбран режим обучения, 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. Конкретные параметры можно настроить, щелкнув элемент **Показать параметры**. 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.

5.2.12.1 Правила HIPS

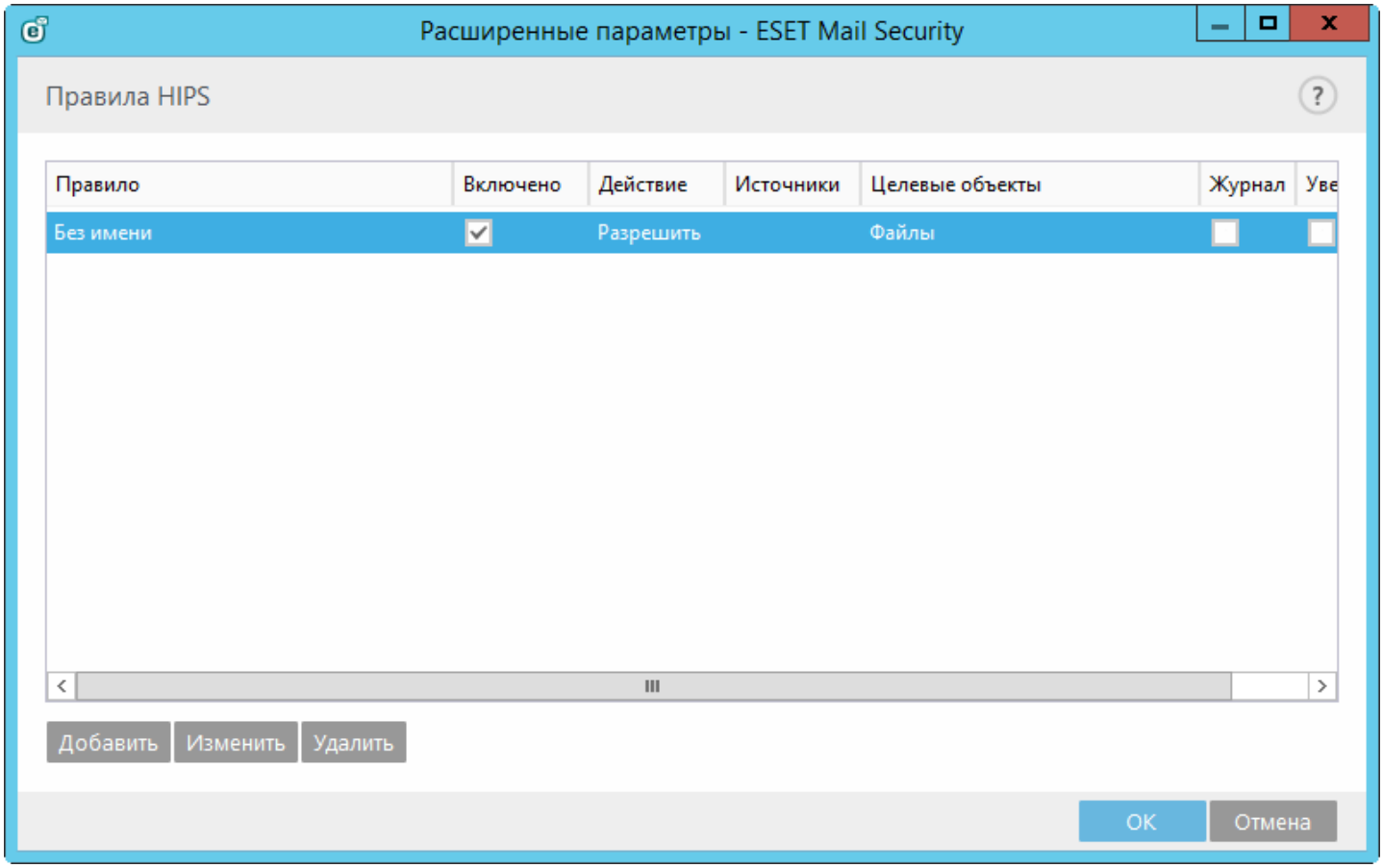
В этом окне отображаются общие сведения об имеющихся правилах HIPS.

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.



5.2.12.1.1 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 пункт «Определенные файлы» в раскрывающемся меню и нажмите кнопку «Добавить», чтобы добавить новые файлы или папки, или выберите пункт «Все файлы», чтобы добавить все приложения.
- **Приложения** — правило будет использоваться только в том случае, если событие вызывается указанными приложениями. Выберите пункт «Определенные приложения» в раскрывающемся меню и нажмите кнопку «Добавить», чтобы добавить новые файлы или папки, или выберите пункт «Все приложения», чтобы добавить все приложения.
- **Записи реестра** — это правило будет использоваться, только если операция относится к данному объекту. Выберите пункт «Определенные записи» в раскрывающемся меню 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 пункт **Определенные файлы** в раскрывающемся меню и нажмите кнопку **Добавить**, чтобы добавить новые файлы или папки, или выберите пункт **Все файлы**, чтобы добавить все приложения.
Приложения — это правило будет использоваться, только если операция относится к данному объекту. Выберите пункт **Определенные приложения** в раскрывающемся меню и нажмите кнопку**Добавить**, чтобы добавить новые файлы или папки, или выберите пункт **Все приложения**, чтобы добавить все приложения.
Записи реестра — это правило будет использоваться, только если операция относится к данному объекту. Выберите пункт **Определенные записи** в раскрывающемся меню и нажмите кнопку**Добавить**, чтобы добавить новые файлы или папки, или выберите пункт **Все записи**, чтобы добавить все приложения.

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 панели «Процессы»).
- **Запустить новое приложение** — запуск новых приложений или процессов.
- **Изменить состояние другого приложения** — исходное приложение пытается осуществить запись в память целевого приложения или выполнить код от его имени. Эта функциональность может быть полезна, 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 (*).

 Если созданное правило будет слишком общим, появится соответствующее предупреждение.

5.2.12.2 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.

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

5.2.12.2.1 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 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.

5.3 Обновление

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

Общие сведения

Текущий профиль обновления отображается в раскрывающемся меню **Выбранный профиль**. Чтобы создать профиль, рядом с элементом **Список профилей** нажмите кнопку **Изменить**, введите **имя профиля** и нажмите кнопку **Добавить**.

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

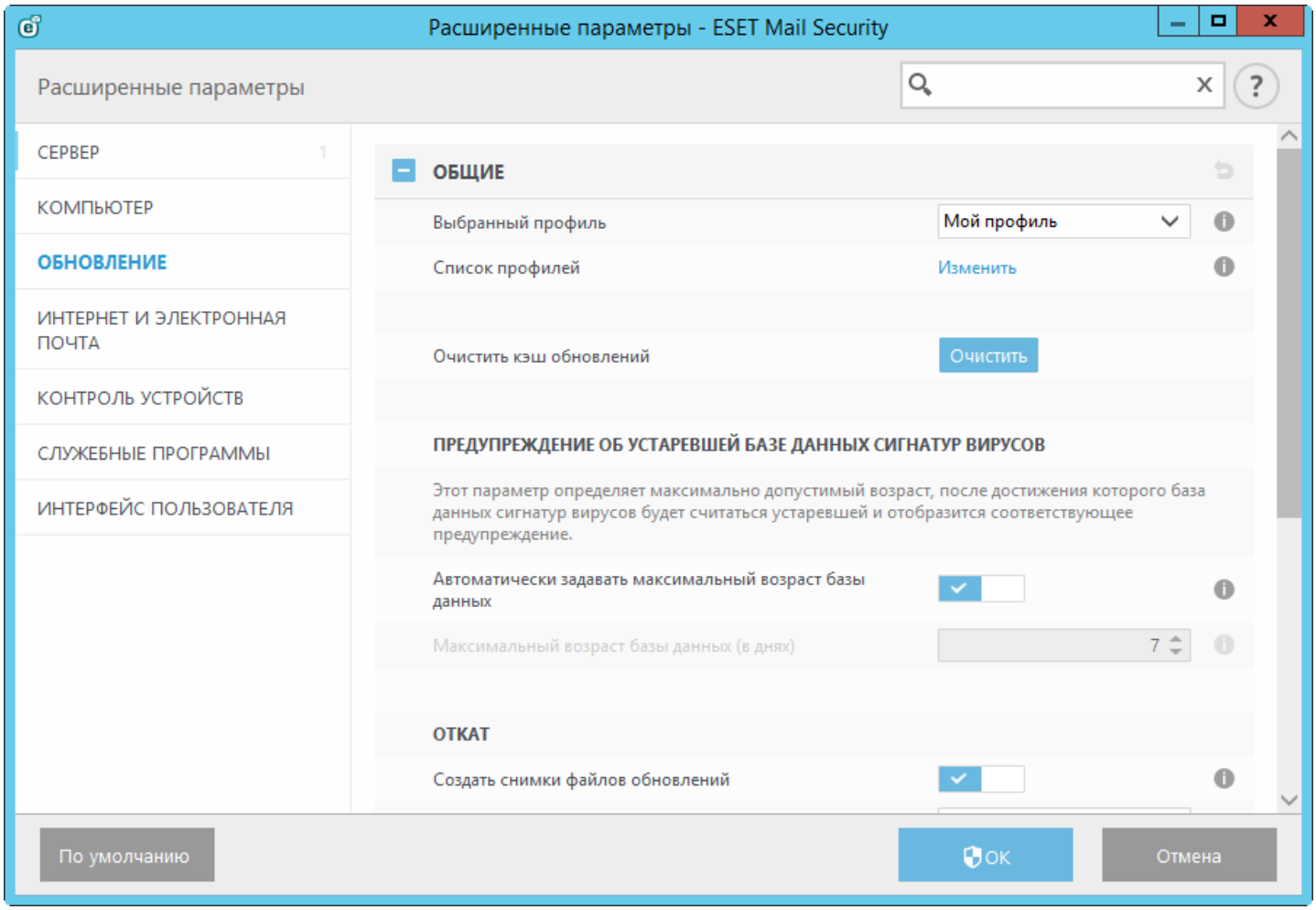
Откат

Если вы подозреваете, что последнее обновление базы данных сигнатур вирусов и/или модулей программы

повреждено или работает нестабильно, вы можете выполнить откат к предыдущей версии и отключить обновления на определенный период времени. Или же можно включить ранее отключенные обновления, если они отложены на неопределенный период времени.

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

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



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

По умолчанию для параметра **Тип обновления**(находится в меню **Обычная**) установлено значение **Регулярное обновление**. Это означает, что файлы обновлений будут автоматически загружаться с сервера ESET, генерируя минимальный трафик.

Основная информация

Отключить уведомления о завершении обновления — 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.

По умолчанию в меню **Сервер обновлений** выбран параметр «Автоматический выбор». Сервер обновлений — это компьютер, на котором хранятся файлы обновлений. При использовании сервера ESET рекомендуется оставить параметры по умолчанию. Если используется пользовательский сервер обновлений и нужно перейти на сервер обновлений по умолчанию, выберите вариант **Автоматически выбор**. Программа ESET Mail Security

автоматически выберет серверы обновлений ESET.

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.

5.3.1 Откат обновления

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

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.

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 Mail Security откройте раздел Обновление.

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

- **Запросить подтверждение перед загрузкой компонентов 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 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.

5.3.3 Прокси-сервер HTTP

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

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

Если выбрать вариант **Использовать глобальные параметры прокси-сервера**, будут использоваться параметры конфигурации прокси-сервера, уже заданные в разделе **Сервис** > **Прокси-сервер** дерева дополнительных настроек.

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

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

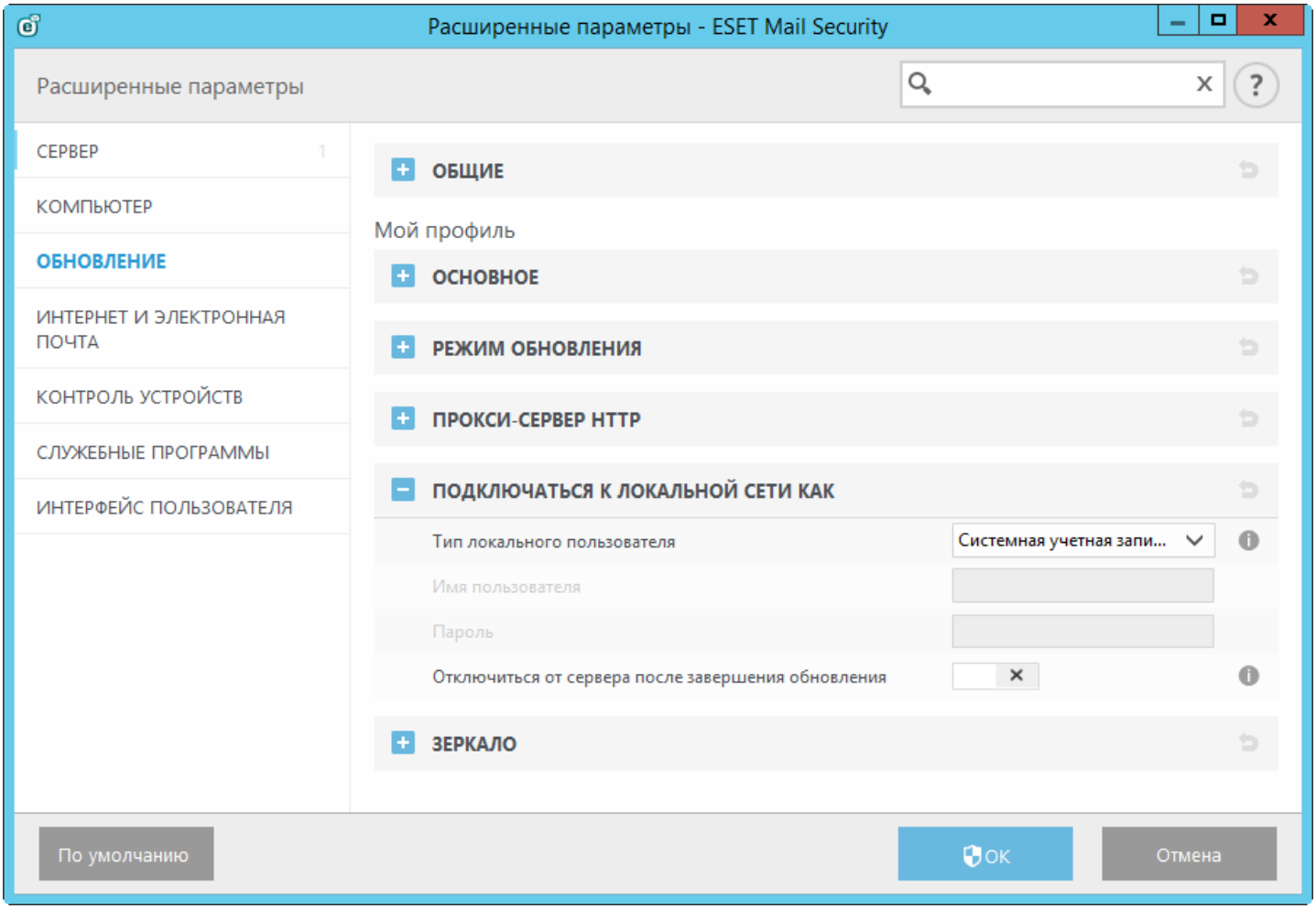
- Для обновления ESET Mail Security должен использоваться прокси-сервер, отличный от указанного в глобальных параметрах (**Сервис** > **Прокси-сервер**). В этом случае нужно указать следующие параметры: адрес **прокси-сервера**, **порт** передачи данных (3128 по умолчанию), а также **имя пользователя** и **пароль** для прокси-сервера (если необходимо).
- Не были заданы общие параметры прокси-сервера, однако программа ESET Mail Security будет подключаться к прокси-серверу для получения обновлений.
- Компьютер подключается к Интернету через прокси-сервер. Параметры берутся из Internet Explorer в процессе установки программы, но 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.

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

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 Mail Security и должны быть заполнены только в том случае, если подключение к Интернету осуществляется через защищенный паролем прокси-сервер.

5.3.4 Подключение к локальной сети

Чтобы выполнить обновление с локального сервера под управлением ОС Windows NT, по умолчанию требуется аутентификация всех сетевых подключений.



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

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

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 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.

ПРЕДУПРЕЖДЕНИЕ. 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

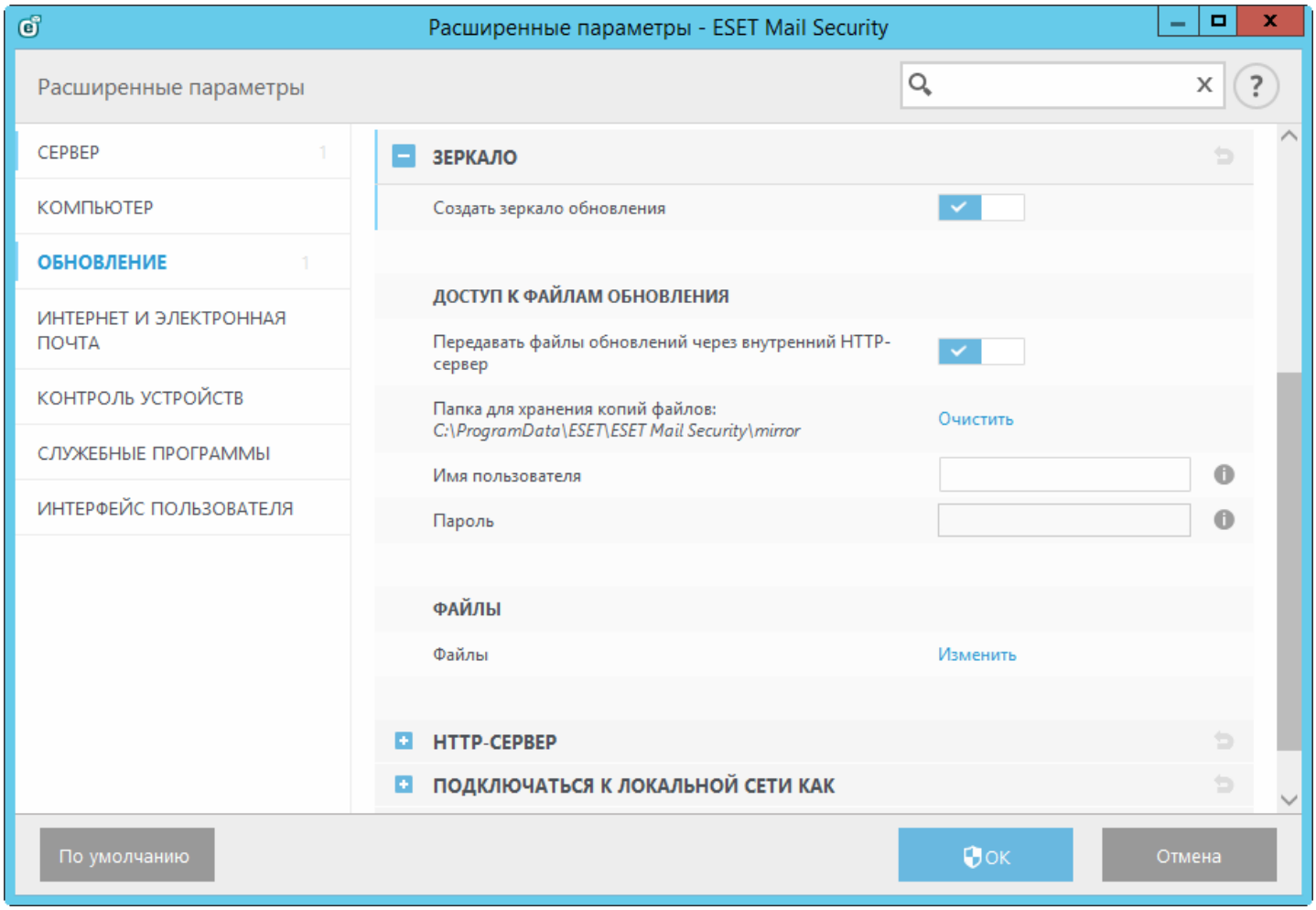
рабочей группы *рабочая_группа\имя*) и пароль. При обновлении по протоколу HTTP с сервера локальной сети аутентификация не требуется.

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

5.3.5 Зеркало

Программа ESET Mail 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.

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



Чтобы создать зеркало на клиентской рабочей станции, установите флажок **Создать зеркало обновления**. После этого станут доступными другие параметры настройки зеркала, такие как способ доступа к файлам обновлений и путь к файлам зеркала.

Доступ к файлам обновления

Передавать файлы обновлений через внутренний HTTP-сервер — если этот параметр активирован, файлы обновлений будут доступны 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, предназначенная для хранения файлов обновлений для зеркала, указывается в разделе **Папка для хранения копий файлов**. Чтобы найти нужную папку на локальном компьютере или в общей сетевой папке, нажмите элемент **Папка**. 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**. Чтобы использовать кодировку base64 и упрощенную аутентификацию по имени пользователя и паролю, выберите вариант **Обычная**. 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.

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

Подключение к локальной сети

Тип локального пользователя — варианты **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.

5.3.5.1 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** > **Обновление** > **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**.

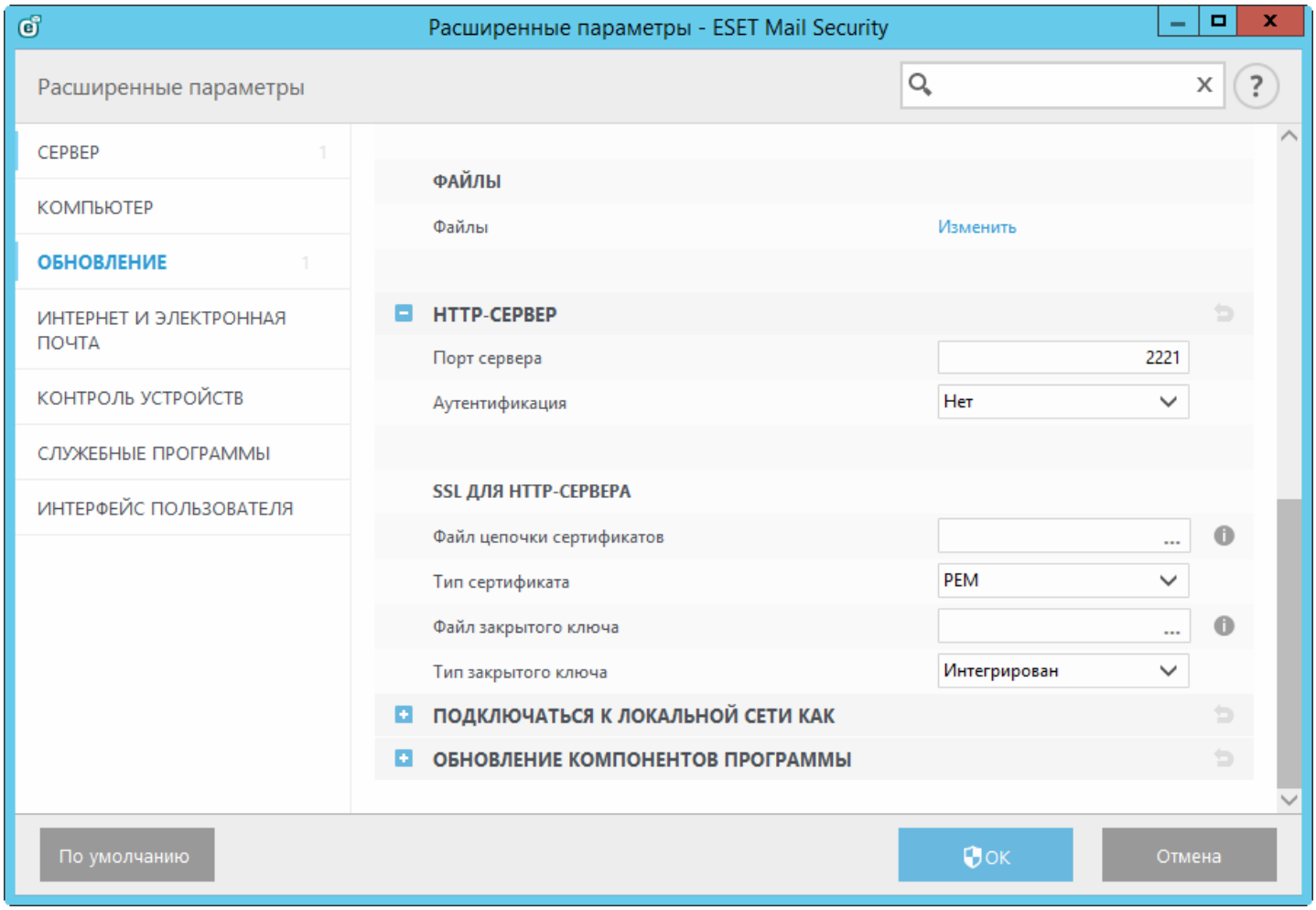
- Чтобы использовать кодировку base64 и упрощенную аутентификацию по имени пользователя и паролю, выберите вариант **Обычная**.
- Вариант **NTLM** обеспечивает шифрование с использованием безопасного способа шифрования. Для аутентификации используется учетная запись пользователя, созданная на рабочей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

ПРЕДУПРЕЖДЕНИЕ. Если планируется организовать доступ к файлам обновлений с помощью HTTP-сервера, папка зеркала должна находиться на том же компьютере, что и экземпляр ESET Mail 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. Если сделано несколько неудачных попыток обновить базу данных сигнатур вирусов с зеркала, в главном меню на панели обновления появится ошибка **Неверные имя пользователя и (или) пароль**. Рекомендуем перейти в меню **Дополнительные настройки** > **Обновление** > **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.

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

Доступ к зеркалу через общие системные папки

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

Далее на вкладке **Дополнительные настройки** > **Обновление** > **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 Mail Security раздел **Дополнительные настройки** (F5) и последовательно щелкните элементы **Обновление** > **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. В программе ESET Mail Security последовательно щелкните элементы **Дополнительные настройки** > **Обновление** > **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-пути. 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.

5.3.5.2 Файлы с зеркала

Список доступных и локализованных файлов компонентов программы.

5.3.5.3 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 Mail 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.
- **Программа ESET Mail Security запрашивает имя пользователя и пароль**: вероятная причина заключается в том, что в разделе обновлений введены неверные данные аутентификации (имя пользователя и пароль). 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 участники» означает то, что папка доступна всем пользователям домена, а не то, что предоставляется доступ без авторизации. В результате, если папка доступна всем участникам, все же необходимо указать доменное имя пользователя и пароль в настройках обновления.
- **Ошибка при подключении ESET Mail Security к серверу зеркала**: подключение к порту, указанному для доступа к HTTP-версии зеркала, блокируется.

5.3.6 Создание задач обновления

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

Обновления также можно выполнять как запланированную задачу. Для конфигурирования запланированной задачи перейдите в раздел **Сервис** > **Планировщик**. По умолчанию в ESET Mail Security активированы указанные ниже задачи.

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

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

5.4 Интернет и электронная почта

В разделе **Интернет и электронная почта** можно настроить защиту почтового клиента, обеспечить защиту обмена данными через Интернет, воспользовавшись защитой доступа в Интернет, и контролировать интернет-протоколы, настроивфильтрацию протоколов. Эти функции имеют принципиально важно значение для защиты компьютера при обмене данными через Интернет.

Функция **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, которая обеспечивается модулем 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 и Windows Server 2008 R2 установка компонента **Интернет и электронная почта** отключена по умолчанию. Если нужно установить этот компонент, выберите тип установки **Выборочная**. Если решение <%PN%> уже установлено, вы можете запустить средство установки еще раз, чтобы изменить уже установленный продукт, добавив к нему компонент Интернет и электронная почта.

5.4.1 Фильтрация протоколов

Фильтрация протоколов

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

«Включить фильтрацию содержимого, передаваемого по протоколам приложений» — может использоваться для отключения фильтрации протоколов. Многие компоненты ESET Mail 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 удаленные адреса из фильтрации протоколов. Полезно, если фильтрация протоколов вызывает проблемы совместимости.

«Исключенные IP-адреса» — позволяет исключить указанные приложения из фильтрации протоколов. Полезно, если фильтрация протоколов вызывает проблемы совместимости.

«Веб-клиенты и почтовые клиенты» — используется только в операционных системах Windows и позволяет выбирать приложения, трафик которых будет проходить фильтрацию протоколов вне зависимости от используемого порта.

«Записывать данные, которые нужны службе поддержки ESET для диагностики проблем с фильтрацией протоколов» —позволяет использовать расширенное ведение журнала, в который вносятся данные диагностики. Используйте только по запросу службы поддержки ESET.

5.4.1.1 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. Рекомендуется использовать эту возможность только для тех приложений, которые работают некорректно, если их соединения проверяются.

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

Изменить: изменение выбранных в списке записей.

Удалить — удаление выделенных записей из списка.

5.4.1.2 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. Этот параметр рекомендуется использовать только для заслуживающих доверия адресов.

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

Изменить — изменение выбранных в списке записей.

Удалить — удаление выделенных записей из списка.

5.4.1.3 Клиенты Интернета и электронной почты

ПРИМЕЧАНИЕ. Начиная с ОС Windows Vista с пакетом обновления 1 и Windows Server 2008, для проверки сетевых соединений используется новая архитектура платформы фильтрации Windows (WFP). Так как технология платформы фильтрации Windows использует особые методы отслеживания, раздел **Веб-клиенты и почтовые клиенты** недоступен.

В условиях перенасыщенности Интернета вредоносными программами безопасное посещение веб-страниц является важным аспектом защиты компьютера. Уязвимости веб-браузеров и мошеннические ссылки позволяют вредоносным программам незаметно проникать в систему. Именно поэтому в программном обеспечении ESET Mail 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.

5.4.2 SSL/TLS

Программа ESET Mail 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. Этот режим позволяет создавать список сертификатов SSL/TLS, которые будут исключены из сканирования.

Блокировать шифрованные подключения, использующие устаревший протокол SSL версии 2 — соединения, использующие более раннюю версию протокола SSL, будут автоматически блокироваться.

Корневой сертификат

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**.

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

5.4.2.1 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 Mail Security настроен на выдачу запросов в таких случаях (по умолчанию запросы отображаются для непроверенных сертификатов, а для недействительных — нет), то 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 Mail 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**.

5.4.2.2 Список известных сертификатов

Список известных сертификатов позволяет настроить поведение ESET Mail Security в отношении конкретных сертификатов SSL, а также настроить запоминание действий пользователя в интерактивном режиме фильтрации протокола SSL. Список можно просмотреть и отредактировать, последовательно выбрав элементы **Дополнительные настройки** (F5) > **Интернет и электронная почта** > **Проверка протокола SSL** > **Список известных сертификатов**.

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

Столбцы

- **Имя** — имя сертификата.
- **Издатель сертификата** — имя создателя сертификата.
- **Субъект сертификата** — это поле указывает на субъект, которому принадлежит открытый ключ, содержащийся в поле открытого ключа субъекта.
- **Доступ** — чтобы разрешить или заблокировать соединение, защищенное сертификатом любого уровня надежности, выберите **Разрешить** или **Заблокировать** в качестве значения параметра **Действие доступа**. Чтобы разрешать доверенные сертификаты и предлагать варианты действий для ненадежных, выберите значение **Автоматически**. Чтобы всегда запрашивать действия пользователя, выберите вариант **Запрашивать**.
- **Сканировать** — чтобы сканировать или игнорировать соединение, защищенное сертификатом, выберите значение **Сканировать** или **Пропустить** для параметра **«Действие сканирования»**. Чтобы сканировать в автоматическом режиме и запрашивать действия в интерактивном, выберите элемент **Автоматически**. Чтобы всегда запрашивать действия пользователя, выберите элемент **Запрашивать**.

Элементы управления

- **Изменить** — выберите сертификат, который нужно настроить, и нажмите кнопку **Изменить**.
- **Удалить** — выберите сертификат, который нужно удалить, и нажмите кнопку **Удалить**.
- **ОК/Отмена** — нажмите кнопку **ОК** для сохранения изменений или **Отмена** для их отмены.

5.4.3 Защита почтового клиента

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

Интеграция с почтовым клиентом

В настоящий момент поддерживаются следующие почтовые клиенты: Microsoft Outlook, Outlook Express, почта Windows и почта Windows Live. Защита электронной почты реализована в этих программах в виде подключаемого модуля. Главное преимущество подключаемого модуля заключается в том, что он не зависит от используемого протокола. При получении почтовым клиентом зашифрованного сообщения оно расшифровывается и передается модулю сканирования. Полный список поддерживаемых почтовых клиентов и их версий см. в статье базы знаний ESET.

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

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

Сканируемая электронная почта

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).

5.4.3.1 Протоколы электронной почты

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

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

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

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

5.4.3.2 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 программа ESET Mail Security позволяет контролировать все соединения почтового клиента (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.

5.4.3.3 Панель инструментов MS Outlook

Защита Microsoft Outlook работает в виде подключаемого модуля. После установки ESET Mail Security панель инструментов, содержащая приведенные ниже функции защиты от вирусов, добавляется в Microsoft Outlook.

ESET Mail Security — если щелкнуть этот значок, откроется главное окно ESET Mail 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.

5.4.3.4 Панель инструментов Outlook Express и Почты Windows

Защита для Outlook Express и почты Windows функционирует в качестве подключаемого модуля. После установки ESET Mail Security панель инструментов, содержащая приведенные ниже функции защиты от вирусов, добавляется в Outlook Express или почту Windows.

ESET Mail Security — если щелкнуть этот значок, откроется главное окно ESET Mail 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 — 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.

5.4.3.5 Окно подтверждения

Это уведомление нужно, чтобы пользователь подтвердил, что выбранное действие действительно нужно выполнить. Благодаря этому можно избежать возможных ошибок.

Кроме того, в окне также есть возможность отключить подтверждения.

5.4.3.6 Повторное сканирование сообщения

Панель инструментов ESET Mail Security, интегрированная в почтовые клиенты, дает пользователю возможность указать ряд параметров для проверки сообщений 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.

Флажок **Повторно сканировать уже сканированные сообщения** дает возможность сканировать уже просканированные сообщения еще раз.

5.4.4 Защита доступа в Интернет

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

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

Настоятельно рекомендуется не отключать защиту доступа в Интернет. Чтобы получить доступ к этой функции, в главном окне программы ESET Mail Security выберите **Настройка** > **Компьютер** > **Защита доступа в Интернет**.

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

- **Основная**: позволяет полностью включать и отключать защиту доступа в Интернет. Если защита отключена, перечисленные ниже параметры станут неактивными.
- **Веб-протоколы** — дает возможность настроить отслеживание в стандартных протоколах, которые используются в большинстве веб-браузеров.
- **Управление URL-адресами** — здесь можно задать HTTP-адреса, которые следует блокировать, разрешать или исключать из проверки.
- **Настройка параметров модуля ThreatSense** — расширенная настройка модуля сканирования. Дает возможность настраивать определенные параметры, например тип сканируемых объектов (сообщения электронной почты, архивы и т. д.), методы обнаружения для защиты доступа в Интернет и т. д.

Веб-протоколы

По умолчанию программа ESET Mail Security настроена на отслеживание протокола HTTP, используемого большинством интернет-браузеров.

В Windows Vista и более поздних версиях, HTTP-трафик отслеживается для всех портов и приложений. В Windows XP/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.

Программа ESET Mail Security поддерживает также проверку протокола HTTPS. В этом типе соединения для передачи информации между сервером и клиентом используется зашифрованный канал. Программа ESET Mail 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. Для включения сканирования зашифрованных соединений перейдите к элементу Проверка протокола SSL в разделе «Дополнительные настройки», выберите элементы **Интернет и электронная почта** > **Проверка протокола SSL**, а затем щелкните элемент **Включить фильтрацию протокола SSL**.

5.4.4.1 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 Mail Security выберите **Настройка** > **Компьютер** > **Защита доступа в Интернет**.

5.4.4.2 Управление URL-адресами

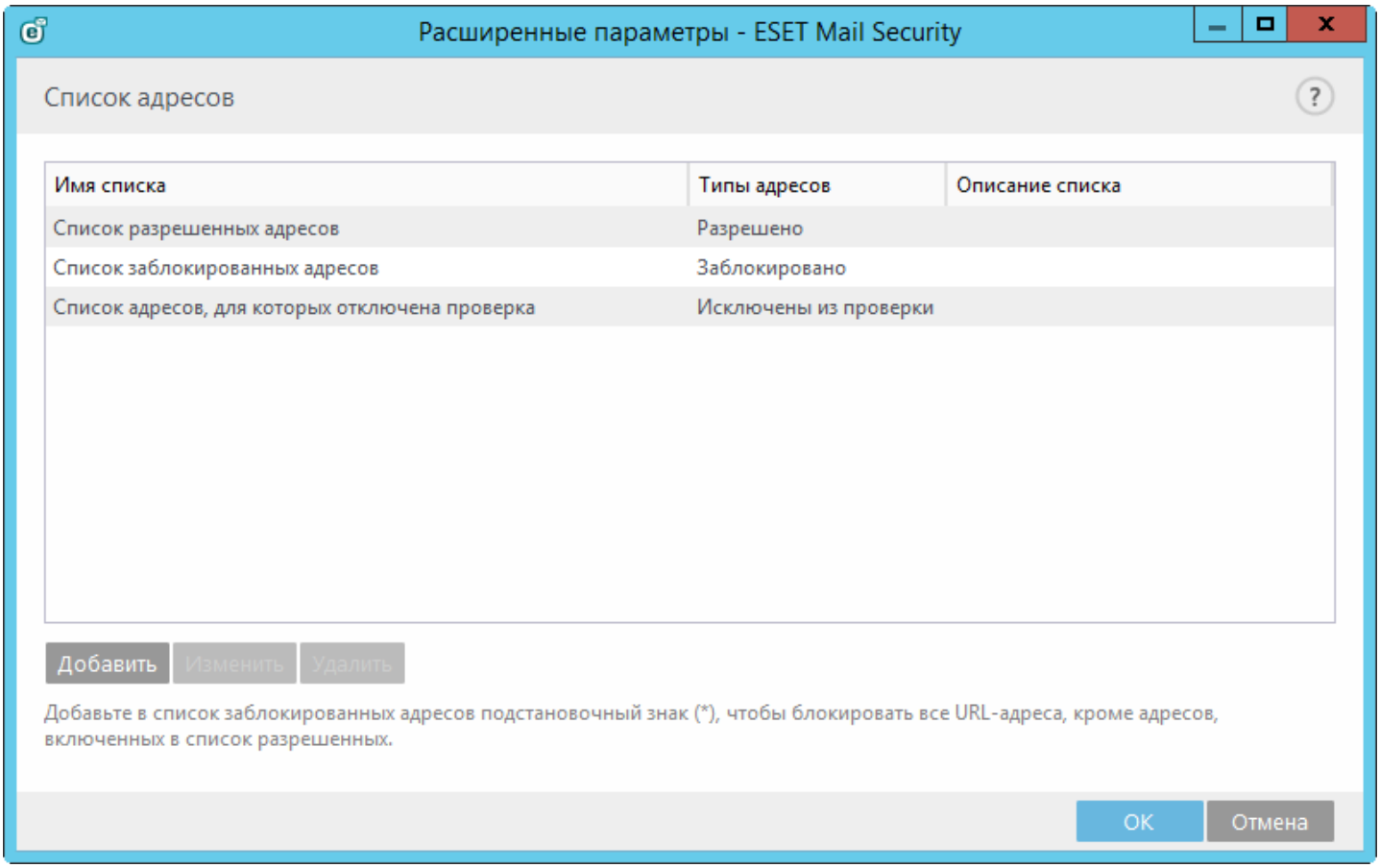
В разделе управления URL-адресами можно задавать HTTP-адреса, которые будут блокироваться, разрешаться или исключаться из проверки.

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.

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

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.

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



Добавить — создание нового списка, дополняющего уже имеющиеся. Это может быть полезно в случае, если вы хотите логически разделить разные группы адресов. Например, один список заблокированных адресов может содержать адреса, полученные из внешнего публичного «черного» списка, а второй — адреса, добавленные вами. Таким образом внешний список можно будет легко обновить, не внося изменений в ваш личный список.
Изменить — редактирование существующих списков. Используйте этот пункт для добавления или удаления адресов из списков.
Удалить — удаление существующих списков. Только для списков, созданных посредством добавления. Удаление списков по умолчанию невозможно.

5.4.4.2.1 Создание списка

В этом разделе можно указать списки URL-адресов и масок, которые будут блокироваться, разрешаться или исключаться из проверки.

При создании списка можно настроить следующие параметры.

Тип списка адресов. Доступны три типа списков:

- **Список адресов, для которых отключена проверка**. Для всех добавленных в этот список адресов не будет выполняться проверка на наличие вредоносного кода.
- **Список заблокированных адресов**. Пользователь не сможет получить доступ к адресам из этого списка. (только если используется протокол HTTP). Другие протоколы блокироваться не будут.
- **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.

Имя списка. Здесь указывается название списка. При изменении одного из трех предварительно заданных списков это поле будет неактивно.

Описание списка. Здесь указывается краткое описание списка (необязательно). При изменении одного из трех предварительно заданных списков поле будет неактивно.

Чтобы активировать его, рядом со списком щелкните элемент **Список активен**. Чтобы получать уведомления о том, что при оценке HTTP-сайта использовался определенный список, установите флажок **Уведомлять о применении**. Например, когда доступ к веб-сайту блокируется или разрешается по причине его присутствия в списке заблокированных или разрешенных адресов, на рабочем столе отображается соответствующее уведомление, в котором указывается имя списка, где фигурирует этот веб-сайт.

Добавить. Добавление нового URL-адреса в список (несколько адресов следует указывать через запятую).

Изменить. Изменение существующего адреса в списке. Удалять можно только те адреса, которые были добавлены посредством команды «Добавить».

Удалить. Удаление существующего адреса в списке. Удалять можно только те адреса, которые были добавлены посредством команды «Добавить».

Импорт. Импорт файла с URL-адресами (в качестве разделителя следует использовать разрыв строки, например в текстовом файле с кодировкой UTF-8).

5.4.4.2.2 HTTP-адреса

В этом разделе можно указать списки HTTP-адресов, которые будут блокироваться, разрешаться или исключаться из проверки.

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.

Чтобы создать новый список, нажмите кнопку **Добавить**. Для удаления выделенных списков нажмите кнопку **Удалить**.

5.4.5 Защита от фишинга

Кроме того, <%PN%> обеспечивает защиту от фишинга. Защита от фишинга является частью модуля «Интернет и электронная почта». Если вы установили <%PN%>, выбрав тип **Полная** установка, модуль «Интернет и электронная почта» по умолчанию устанавливается со включенной функцией защиты от фишинга. При этом это не относится к системам под управлением Microsoft Windows Server 2008.

ПРИМЕЧАНИЕ. Компонент «Интернет и электронная почта» не устанавливается в рамках **полной установки** <%PN%> в ОС Windows Server 2008 и Windows Server 2008 R2. Если потребуется, вы можете добавить в установленный продукт компонент Интернет и электронная почта, чтобы можно было использовать защиту от фишинга.

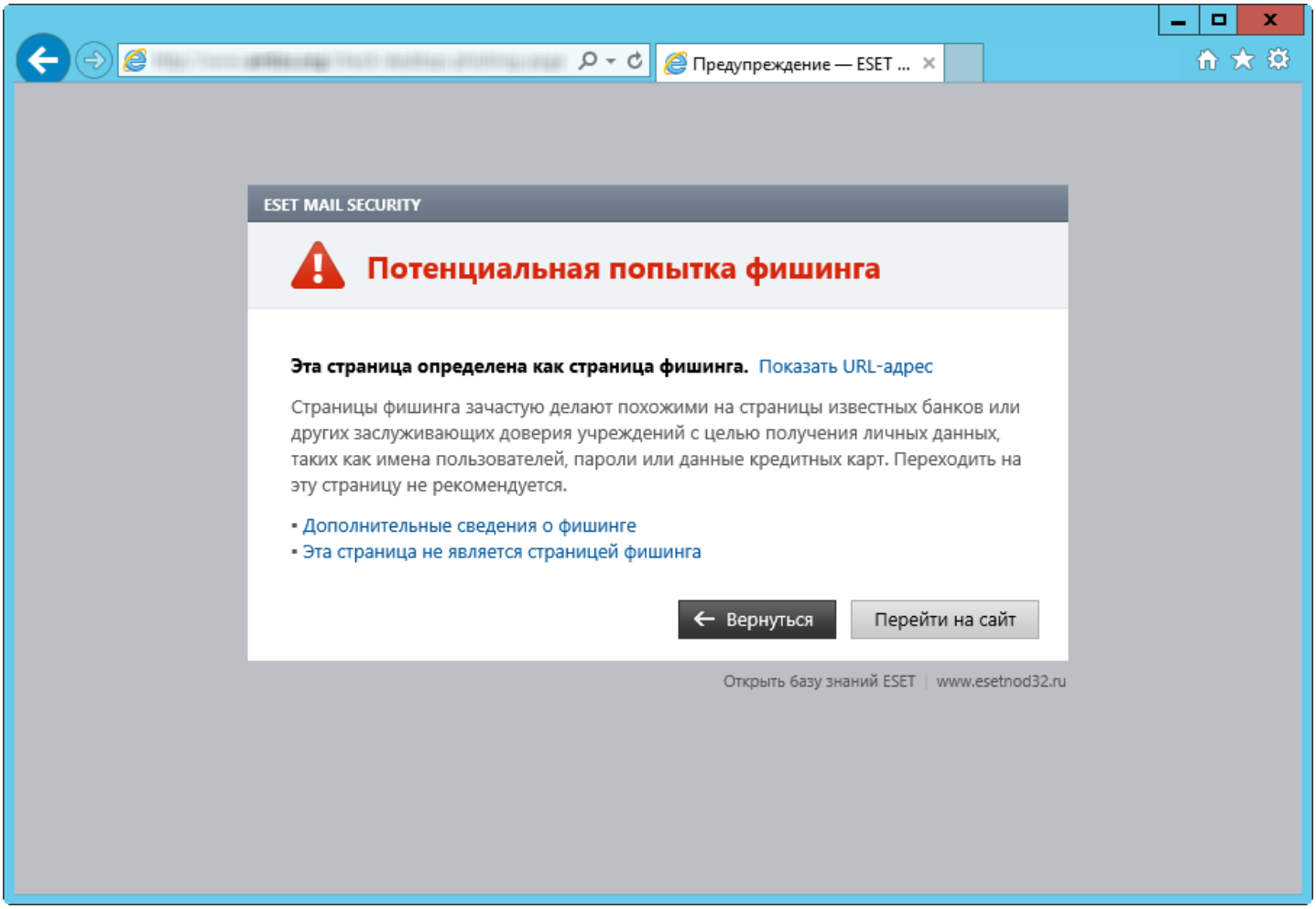
Термин «фишинг» обозначает преступную деятельность, в рамках которой используется социальная инженерия (манипулирование пользователями, направленное на получение конфиденциальной информации). Фишинг часто используется для получения доступа к конфиденциальным сведениям, таким как номера банковских счетов,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

Настоятельно рекомендуется включить защиту от фишинга в программе ESET Mail 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 Mail 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.).

5.5 Контроль устройств

Программа ESET Mail Security обеспечивает автоматическое управление устройствами (компакт- и DVD-дисками, USB-устройствами и т. п.). Данный модуль позволяет сканировать, блокировать и изменять расширенные фильтры и разрешения, а также указывать, может ли пользователь получать доступ к конкретному устройству и работать с ним. Это может быть удобно, если администратор компьютера хочет предотвратить использование устройств с нежелательным содержимым.

Поддерживаемые внешние устройства:

- дисковый накопитель (жесткий диск, съемный USB-диск);
- компакт- 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.

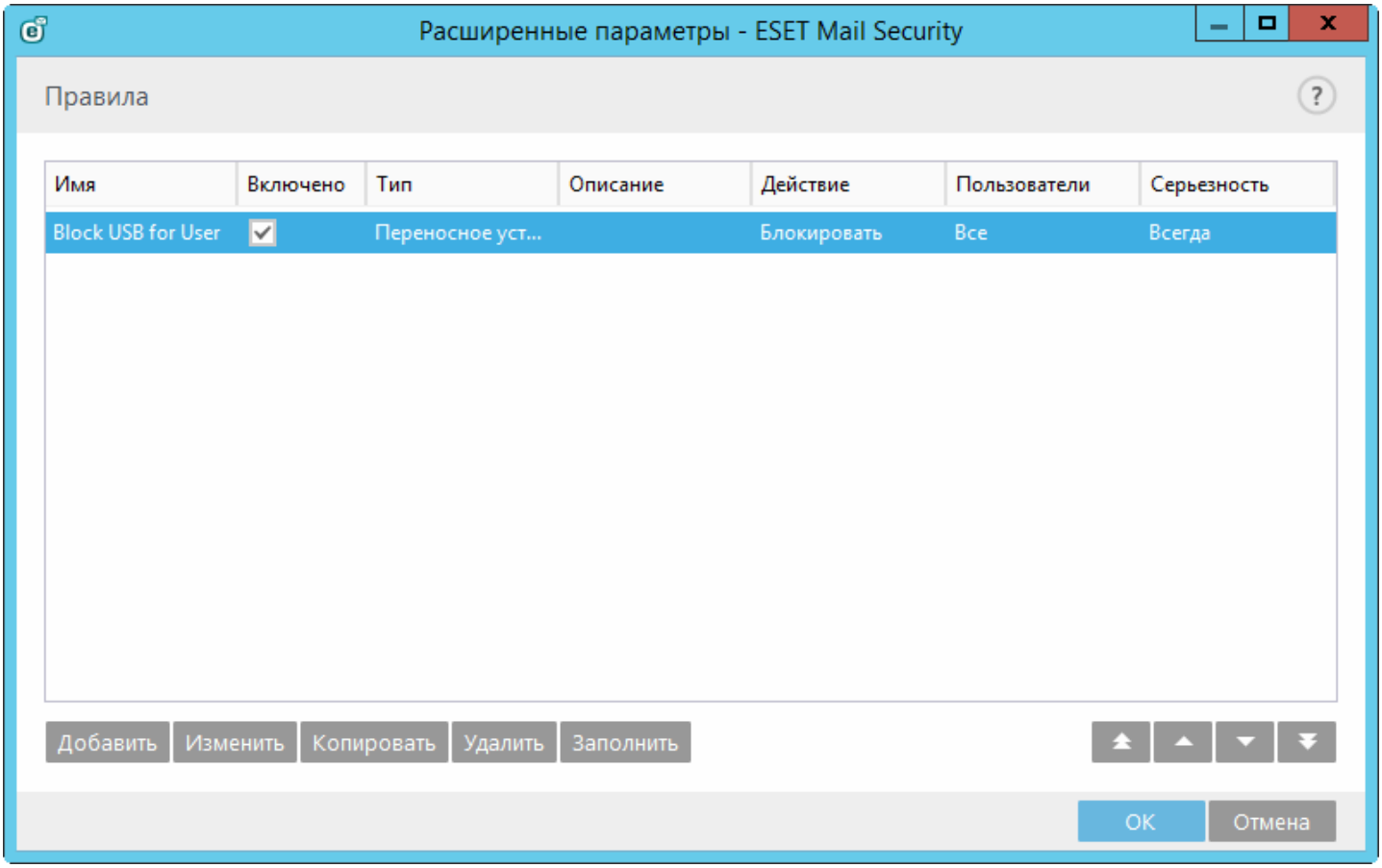
Параметры контроля устройств можно изменить в разделе **Дополнительные настройки** (F5) > **Контроль устройств**.

Если рядом с параметром **Интеграция с системой** поставить переключатель, в программе ESET Mail Security будет включена функция контроля устройств. Чтобы это изменение вступило в силу, необходимо перезапустить компьютер. После того как функция контроля устройств будет включена, кнопка **Редактор правил** станет активной и вы сможете открывать окно Редактор правил.

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

5.5.1 Правила 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. В списке правил для каждого правила отображается описание, включающее название и тип внешнего устройства, действие, выполняемое после его подключения к компьютеру, а также серьезность для журнала.

Для управления правилом используйте кнопки **Добавить** или **Изменить**. Чтобы удалить выбранное правило, нажмите кнопку **Удалить**. Чтобы отключить это правило, снимите флажок **Включено** рядом с ним. Это может быть полезно, если вы не хотите полностью удалять правило и собираетесь воспользоваться им позднее.

Копировать — с помощью этой команды создается правило на основе параметров выбранного правила.

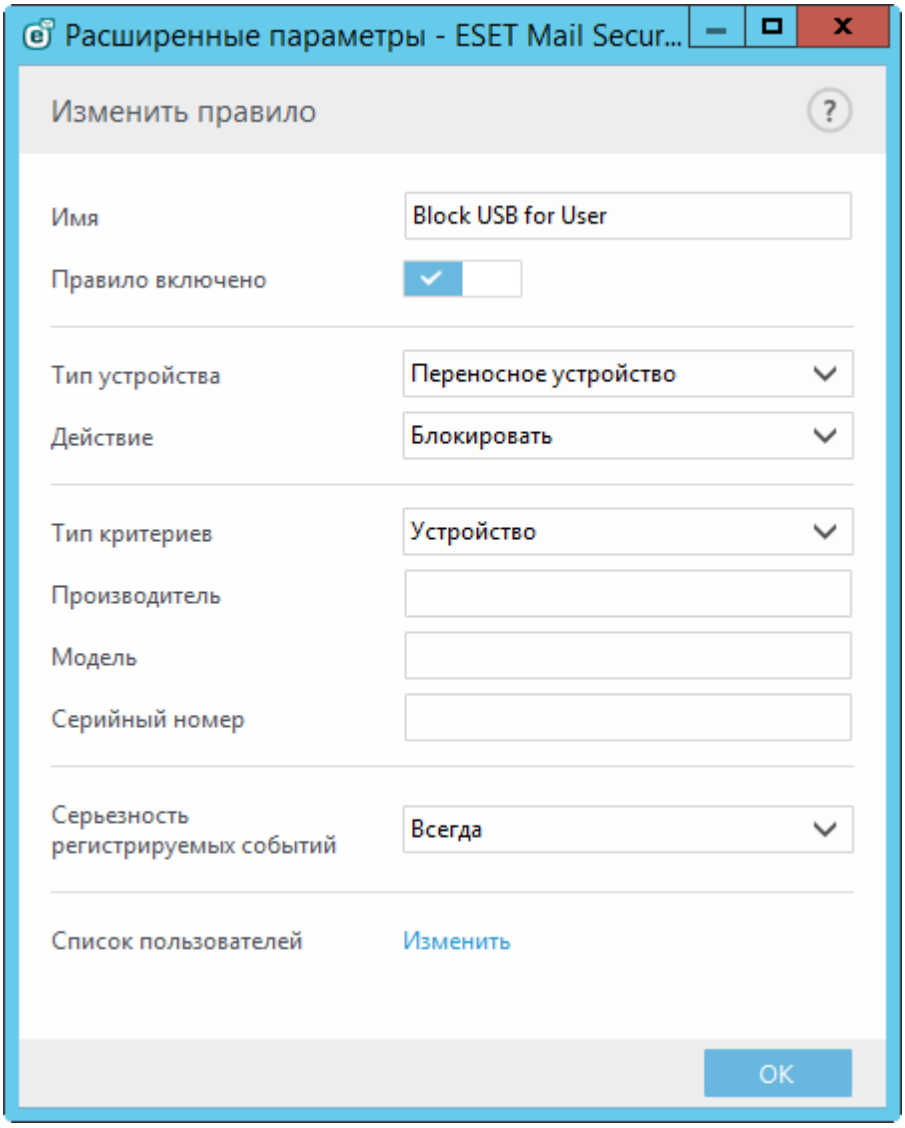
Чтобы автоматически заполнить параметры для съемных носителей, подключенных к компьютеру, щелкните элемент **Заполнить**.

Правила приведены в порядке приоритета: имеющие более высокий приоритет располагаются в начале списка. Чтобы выделить несколько правил и применить к ним необходимые действия, например удалить или переместить к началу либо концу списка, воспользуйтесь элементами **В начало/вверх/вниз/в конец** (стрелки).

Записи журналов можно просмотреть в главном окне программы ESET Mail Security в разделе **Сервис** > Файлы журналов.

5.5.2 Добавление правил контроля устройств

Правило контроля устройств определяет действие, выполняемое при подключении к компьютеру устройств, которые соответствуют заданным критериям.



Чтобы упростить идентификацию правила, введите его описание в поле **Имя**. Чтобы включить или отключить это правило, щелкните переключатель рядом с элементом **Правило включено**. Это может быть полезно, если полностью удалять правило не нужно.

Тип устройства

В раскрывающемся меню выберите тип внешнего устройства (дисковый накопитель, портативное устройство, Bluetooth, FireWire и т. д.). 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 (*, ?).

Совет. 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).

5.5.3 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).

5.5.4 Группы устройств

 Устройство, подключенное к компьютеру, может представлять угрозу безопасности.

Окно групп устройств разделено на две части. В правой части окна отображается список устройств, входящих в выбранную группу, а в левой части — список созданных групп. Выберите группу, содержащую устройства, которые нужно отобразить на правой панели.

Открыв окно групп устройств и выбрав группу, вы можете добавлять устройства в список или удалять их из него. Добавлять устройства в группу также можно посредством импорта данных об устройствах из файла. Или же можно нажать кнопку **Заполнить**. В этом случае все устройства, подключенные к компьютеру, отобразятся в окне **Обнаруженные устройства**. Выберите устройства из этого списка и нажмите кнопку **ОК**, чтобы добавить их в группу.

Элементы управления

Добавить — позволяет добавить устройство в существующую группу или добавить группу (для этого нужно указать ее имя) (по выбору можно указать такие сведения, как имя производителя, модель и серийный номер), в зависимости от того, в какой части окна нажата эта кнопка.

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 — импортирует список устройств из файла.

С помощью кнопки **Заполнить** можно ознакомиться со следующей информацией о подключенных на данный момент устройствах: тип устройства, производитель, модель и серийный номер (если есть).

Завершив настройки, нажмите кнопку **ОК**. Чтобы закрыть окно **Группы устройств** без сохранения изменений, нажмите кнопку **Отмена**.

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

Обратите внимание, что полный список действий (прав) 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.

5.6 Сервис

Ниже приведены дополнительные параметры для всех служебных программ, доступных на вкладке **Сервис** в главном окне программы ESET Mail Security.

5.6.1 ESET Live Grid

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

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

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

По умолчанию программа ESET Mail 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 Live Grid использует «белый» и «черный» списки, которые хранятся в облаке. Для доступа к настройкам ESET Live Grid нажмите клавишу F5, чтобы открыть окно дополнительных настроек, а затем последовательно откройте элементы **Сервис** > **ESET Live Grid**.

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

Отправить анонимную статистическую информацию — с помощью этого параметра можно разрешить продукту ESET собирать информацию о недавно обнаруженных угрозах: название угрозы, дата и время обнаружения, способ обнаружения, связанные метаданные, версия и конфигурация продукта (включая информацию о системе).

Отправить файлы — компании ESET на анализ отправляются подозрительные файлы, похожие на угрозы, и файлы 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 Live Grid использовалась ранее, но была отключена, могут существовать пакеты данных,

предназначенные для отправки. Эти пакеты будут отправлены в ESET даже после выключения системы. После отправки всей текущей информации новые пакеты создаваться не будут.

5.6.1.1 Фильтр исключений

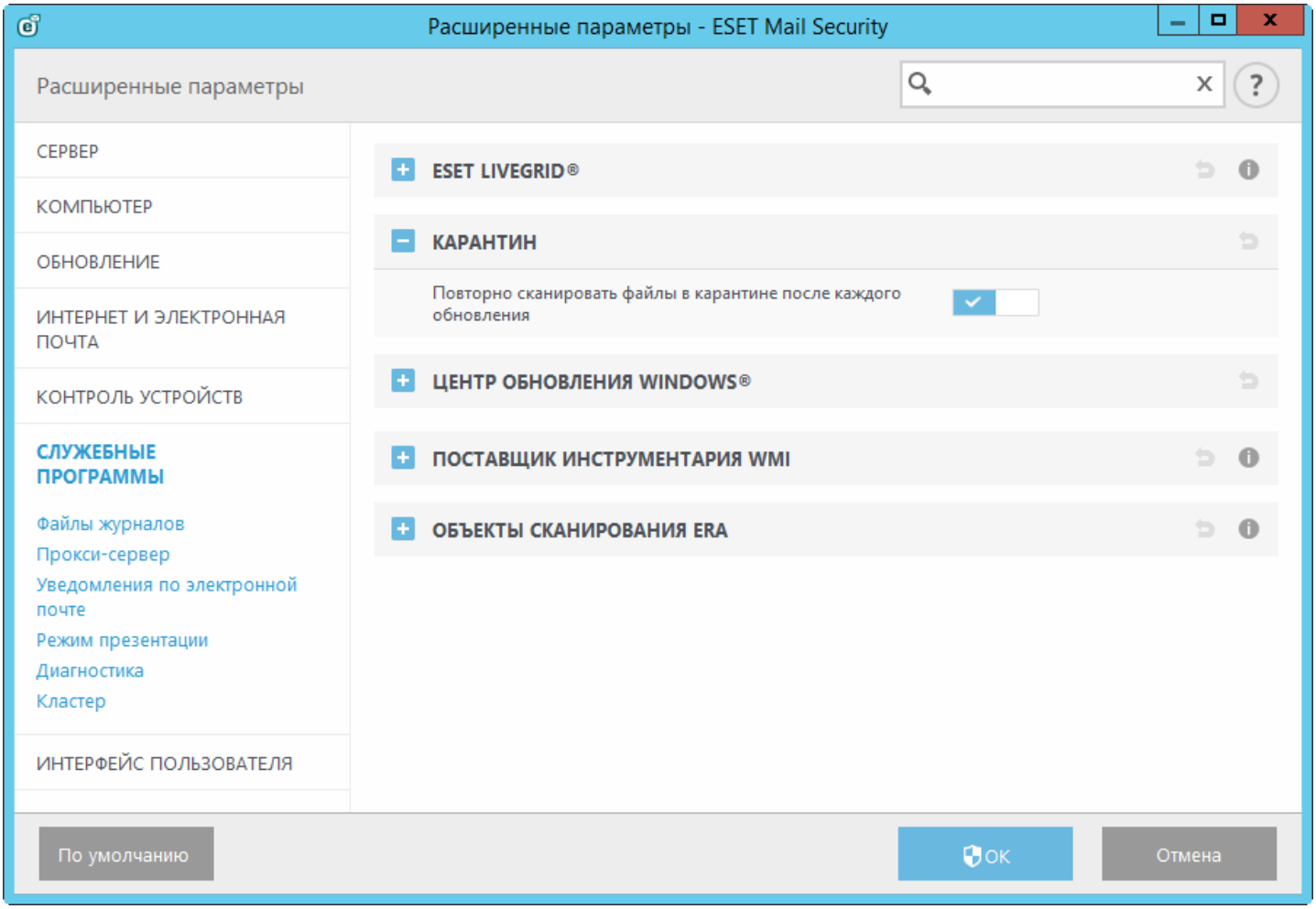
С помощью параметра **Изменить** рядом с элементом «Исключения» в ESET Live Grid можно настроить способ отправки сведений об угрозах в антивирусную лабораторию ESET для анализа.

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.

5.6.2 Карантин

Зараженные и подозрительные файлы хранятся в папке карантина в неопасном виде. По умолчанию, чтобы избежать заражения, модуль защиты в режиме реального времени помещает на карантин все вновь созданные подозрительные файлы.

Повторно сканировать файлы в папке карантина после обновлений: все объекты, помещенные на карантин, сканируются после каждого обновления базы данных сигнатур вирусов. Это особенно полезно, если файл помещен в карантин из-за ложного срабатывания функции обнаружения. Если включить эту функцию, файлы некоторых типов будут автоматически восстанавливаться в исходных папках.



5.6.3 Центр обновления Windows

Обновления Windows содержат важные исправления потенциально опасных уязвимостей и повышают общий уровень безопасности компьютера. По этой причине обновления Windows следует устанавливать сразу после их появления. Программа ESET Mail 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.

5.6.4 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.

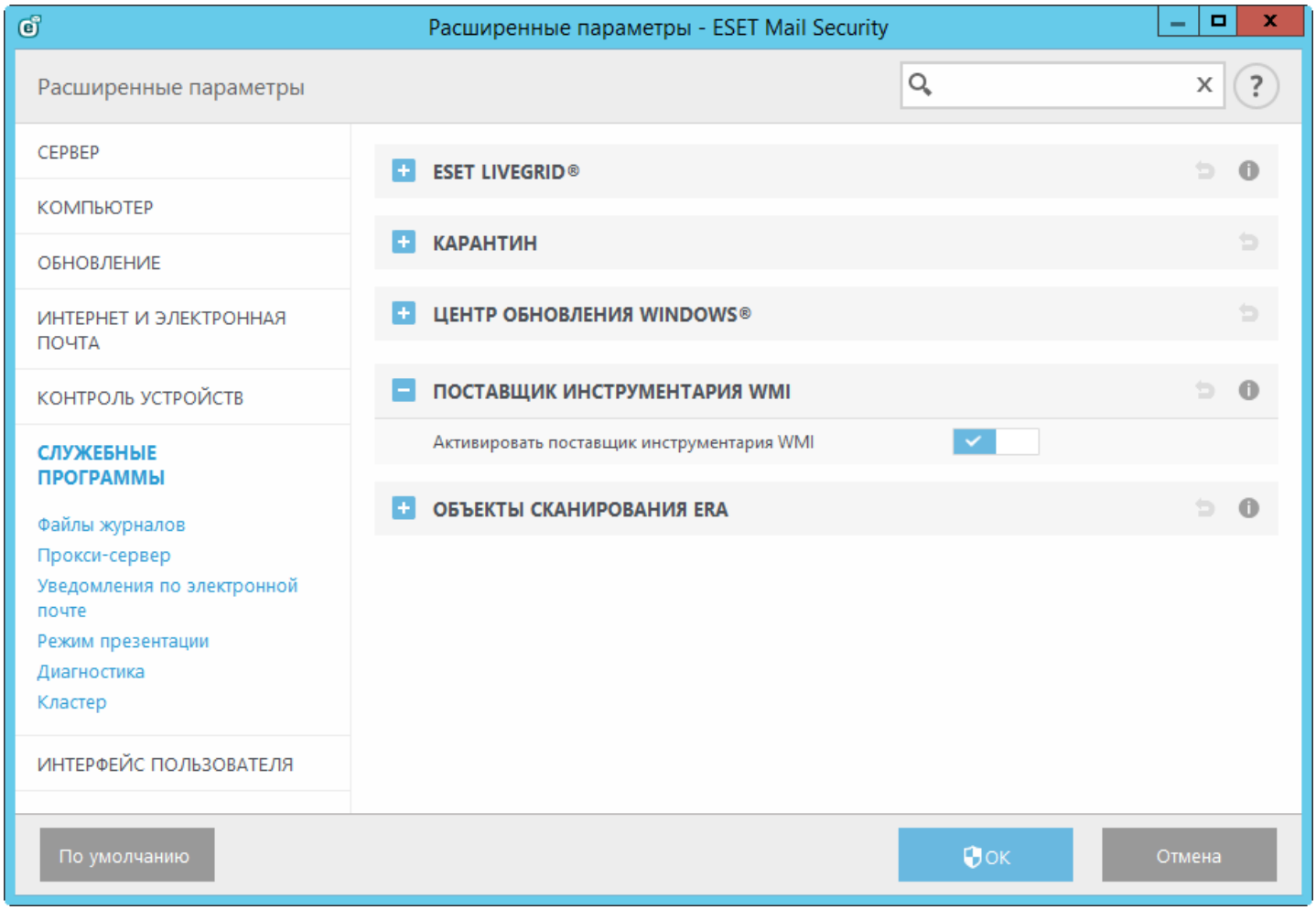
Дополнительные сведения об инструментарии WMI см. в статье по адресу http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642(v=vs.85).aspx

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.



5.6.4.1 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_GreylistLog
- ESET_SpamLog

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 «essbe».
- **Name** — название продукта, например ESET Security.
- **Edition** — выпуск продукта, например Microsoft SharePoint Server.
- **Version** — версия продукта, например 4.5.15013.0.
- **VirusDBVersion** — версия базы данных вирусов, например 7868 (20130107).
- **VirusDBLastUpdate** — отметка о времени последнего обновления вирусной базы данных. В строке содержится отметка о времени в формате даты и времени WMI, например 20130118115511.000000+060.
- **LicenseExpiration** — время окончания срока действия лицензии. В строке содержится отметка о времени в формате даты и времени WMI, например 20130118115511.000000+060.
- **KernelRunning** — логическое значение, например «Истина», указывающее на то, запущена ли на компьютере служба eKrn.
- **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 Mail Security.
- **SERVER_EMAIL_AV** — защита от вирусов сообщений электронной почты в защищенном серверном продукте, например сообщений в MS Exchange или IBM Lotus Domino.
- **SERVER_EMAIL_AS** — защита от спама сообщений электронной почты в защищенном серверном продукте, например сообщений в MS Exchange или IBM Lotus 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 примерно так: 20130118115511.000000+060.
- ResetTime — отметка о времени последнего сброса счетчика статистики. В формате даты и времени WMI эта отметка выглядит примерно 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 компьютеров 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_EventLog 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.

ESET_SpamLog

Класс ESET_EventLog имеет несколько экземпляров, каждый из которых представляет запись из журнала «Журнал спама». 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.
- **Sender** — отправитель сообщений электронной почты.
- **Recipients** — получатели сообщений электронной почты.
- **Subject** — тема сообщения.
- **Received** — время получения.
- **Score** — оценка нежелательности в процентах в диапазоне 0–100.
- **Reason** — причина, по которой сообщение электронной почты помечено как спам.
- **Action** — выполненное действие.
- **DiagInfo** — дополнительные диагностические сведения.

5.6.4.2 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
```

5.6.5 Объекты сканирования ERA

Благодаря этому компоненту ESET Remote Administrator использует надлежащие объекты сканирования базы данных по требованию при выполнении клиентской задачи **Сканирование сервера** на сервере, на котором установлена программа ESET Mail Security.

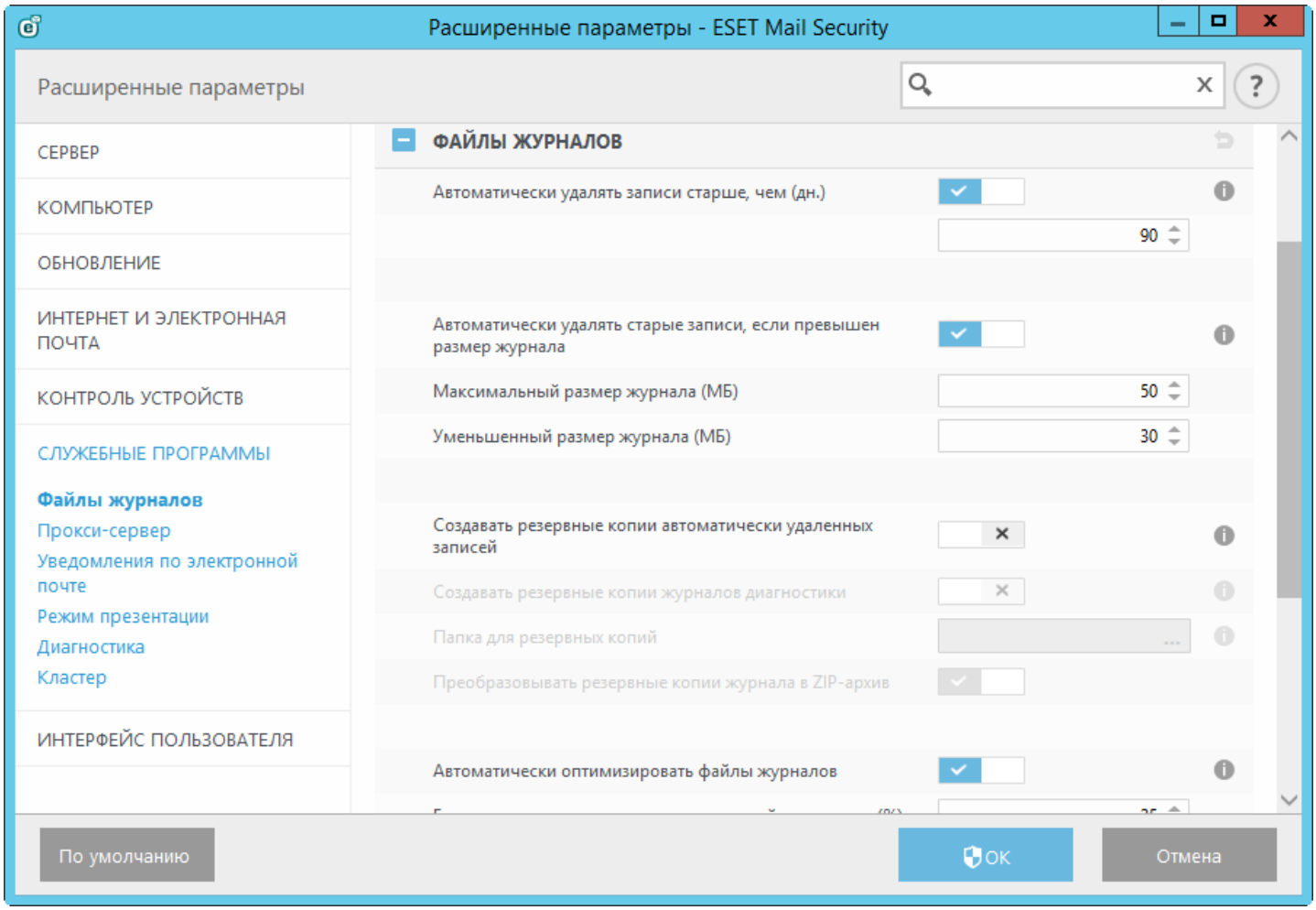
При включении функции **Создание списка объектов** ESET Mail Security создает список доступных объектов сканирования базы данных. Этот список создается время от времени в зависимости от **интервала обновления**, заданного в минутах. Перед запуском клиентской задачи **Сканирование сервера** ERA создает список и дает пользователю возможность выбрать объекты для сканирования базы данных по требованию на заданном сервере.

5.6.6 Файлы журналов

Если потребуется, можно использовать переключатель для включения или отключения **ведения журнала диагностики** кластера. По умолчанию он включен. Это означает, что ведение журнала кластера будет выполняться в рамках ведения общего журнала диагностики. Чтобы запустить фактическое ведение журнала, необходимо включить ведение журнала общей диагностики на уровне продукта, последовательно щелкнув «Главное меню» > «Настройка» > Сервис. После включения ведение журнала диагностики обеспечит также сбор подробных журналов в кластере ESET.

Раздел **Файлы журналов** позволяет изменять конфигурацию ведения журналов программы ESET Mail Security.

Можно определить способ управления журналами. Программа автоматически удаляет старые файлы журналов, чтобы сэкономить дисковое пространство.



5.6.6.1 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.

5.6.6.2 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.

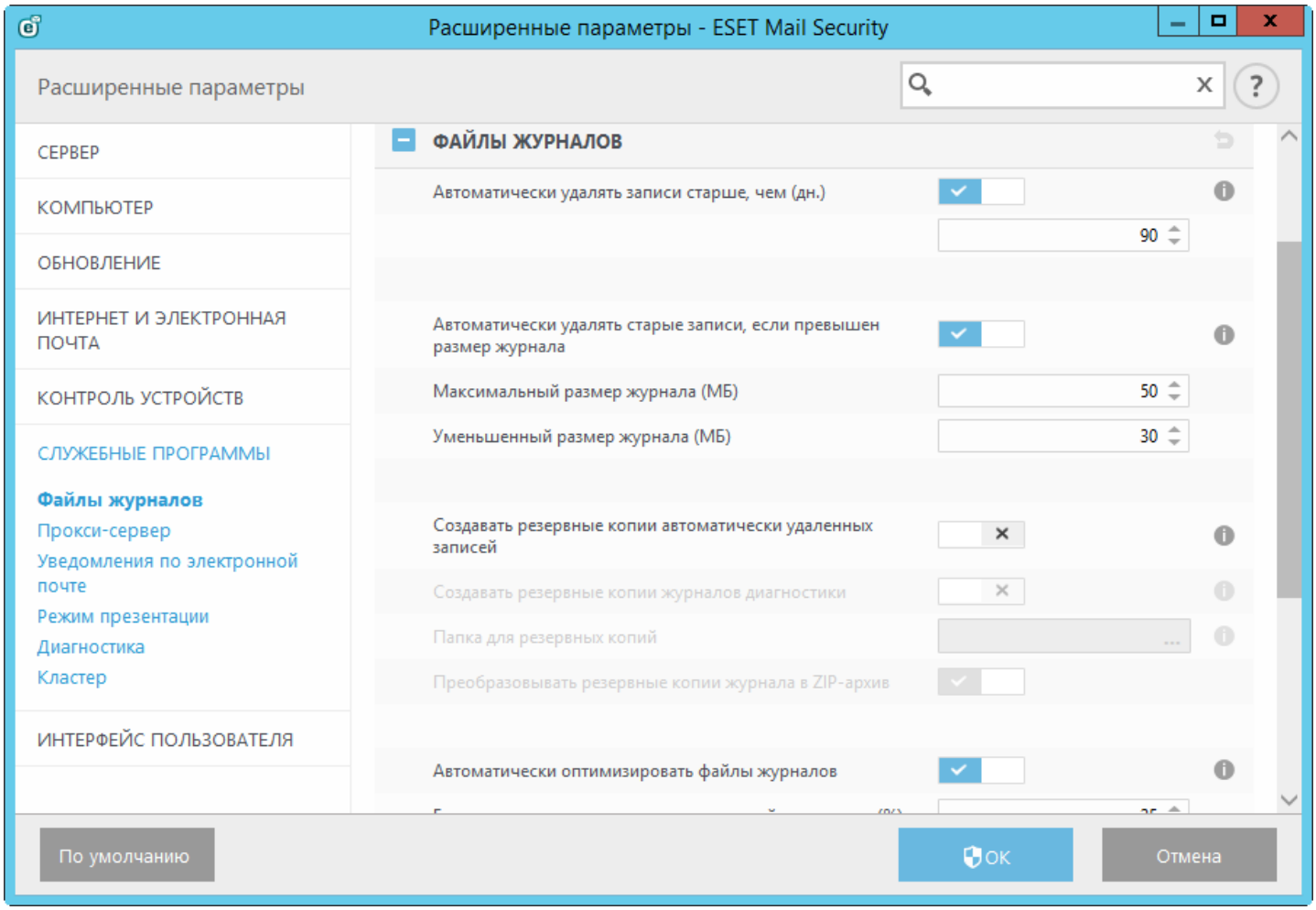
После конфигурирования параметров поиска нажмите кнопку **Найти**, чтобы начать поиск. Поиск прекращается, когда находится первая соответствующая его критериям запись. Чтобы отобразились дополнительные записи, нажмите кнопку **Найти** еще раз. Поиск в файлах журналов ведется сверху вниз, начиная с текущего положения (выделенной записи).

5.6.6.3 Обслуживание журнала

Если потребуется, можно использовать переключатель для включения или отключения **ведения журнала диагностики** кластера. По умолчанию он включен. Это означает, что ведение журнала кластера будет выполняться в рамках ведения общего журнала диагностики. Чтобы запустить фактическое ведение журнала, необходимо включить ведение журнала общей диагностики на уровне продукта, последовательно щелкнув «Главное меню» > «Настройка» > Сервис. После включения ведение журнала диагностики обеспечит также сбор подробных журналов в кластере ESET.

Раздел **Файлы журналов** позволяет изменять конфигурацию ведения журналов программы ESET Mail Security.

Можно определить способ управления журналами. Программа автоматически удаляет старые файлы журналов, чтобы сэкономить дисковое пространство.



- **Удалять записи автоматически**: записи журнала, созданные ранее указанного количества дней, автоматически удаляются.
- **Автоматически оптимизировать файлы журналов**: включается автоматическая дефрагментация файлов журналов при превышении указанного значения неиспользуемых данных в процентах.
- **Минимальная степень детализации журнала**: задается степень детализации ведения журнала. Возможны следующие варианты.

- **Диагностические записи**: в журнал вносится информация, необходимая для точной настройки программы, а также все перечисленные выше записи.
- **Информационные записи**: 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 вносятся только сообщения типа «Ошибка при загрузке файла», а также критические ошибки.
- **Критические предупреждения**: в журнал вносятся только критические ошибки (ошибки запуска защиты от вирусов и т. п.).

5.6.7 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 Mail Security настройку прокси-сервера можно выполнить в двух разных разделах дерева расширенных параметров.

Во-первых, параметры прокси-сервера можно конфигурировать в разделе **Дополнительные настройки**, в котором нужно последовательно щелкнуть элементы **Сервис** > **Прокси-сервер**. Настройка прокси-сервера на этом уровне позволяет задать его параметры для программы ESET Mail Security в целом. Они используются всеми модулями программы, которым требуется подключение 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.

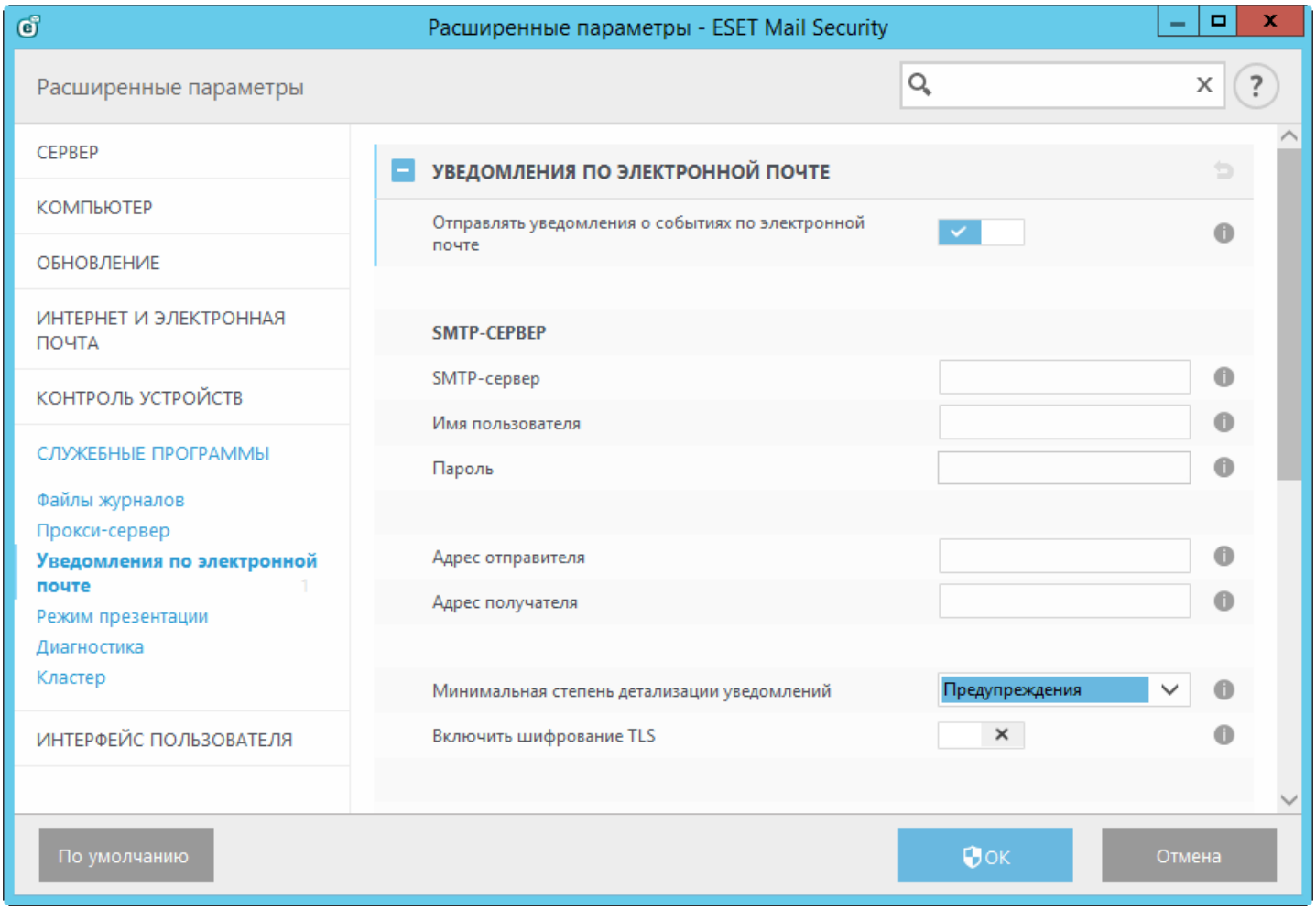
Если для подключения требуется аутентификация на прокси-сервере, включите переключатель **Прокси-сервер требует аутентификации**, а затем укажите **имя пользователя** и **пароль** в соответствующих полях. Нажмите кнопку **Найти**, чтобы автоматически определить параметры прокси-сервера и подставить их.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

ПРИМЕЧАНИЕ. Эта функция не позволяет получить данные аутентификации (имя пользователя и пароль), пользователь должен указать их самостоятельно.

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

5.6.8 Уведомления по электронной почте

Программа ESET Mail Security поддерживает автоматическую отправку сообщений электронной почты при возникновении событий с заданной степенью детализации. Чтобы включить эту функцию, установите флажок **Отправлять уведомления о событиях по электронной почте**.



ПРИМЕЧАНИЕ. Программа ESET Mail 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** — в этом поле указывается адрес отправителя, который будет отображаться в заголовке писем с уведомлением.
- **Адрес получателя** — в этом поле указывается адрес получателя, который будет отображаться в заголовке писем с уведомлением.

- **Минимальная степень детализации уведомлений** — 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).

5.6.8.1 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 событие.
- **%ProgramName%** — программа, создавшая предупреждение.
- **%InfectedObject%** — имя зараженного файла, сообщения и т. п.
- **%VirusName%** — идентифицирующие данные заражения.
- **%ErrorDescription%** — описание события, не имеющего отношения к вирусам.

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

5.6.9 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.

Чтобы включить режим презентации вручную, последовательно выберите элементы **Настройки** > **Компьютер** и затем щелкните переключатель напротив этого режима. В окне **Дополнительные настройки** (F5) выберите элементы **Сервис** > **Режим презентации** и затем щелкните переключатель **Автоматически включать режим презентации при работе приложений в полноэкранном режиме**, чтобы при запуске приложений в полноэкранном режиме продукт ESET Mail Security автоматически переходил в режим презентации. Включая режим презентации, вы подвергаете систему угрозе, поэтому значок состояния защиты на панели задач станет оранжевым, чтобы тем самым предупредить вас. Данное предупреждение 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. Это особенно удобно для включения режима презентации 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.

5.6.10 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 Mail 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.

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*.

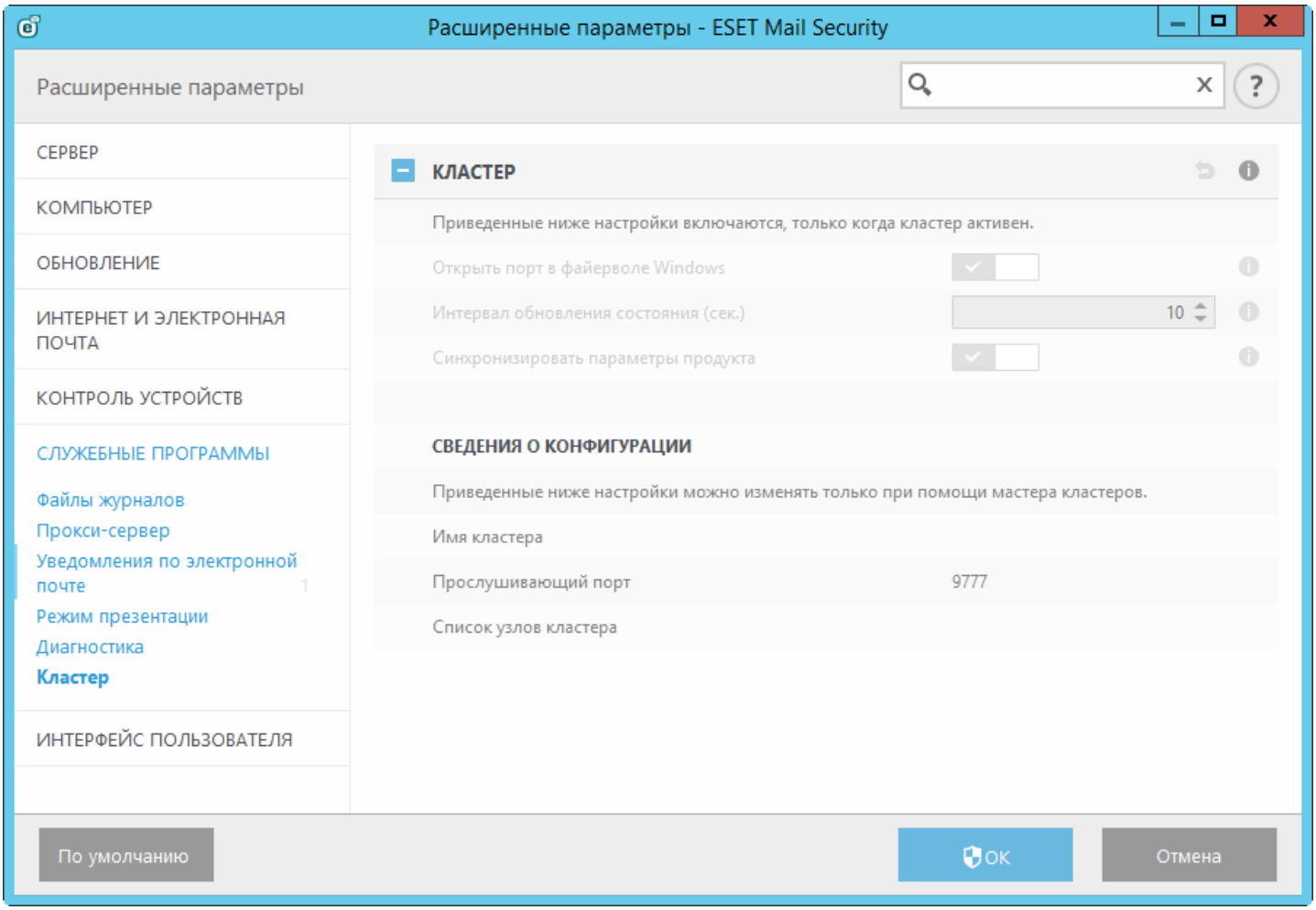
5.6.11 Служба поддержки клиентов

Отправить данные о конфигурации системы — чтобы перед отправкой получать запрос, в раскрывающемся меню выберите элемент **Отправлять всегда** или **Запрашивать подтверждение перед отправкой**.

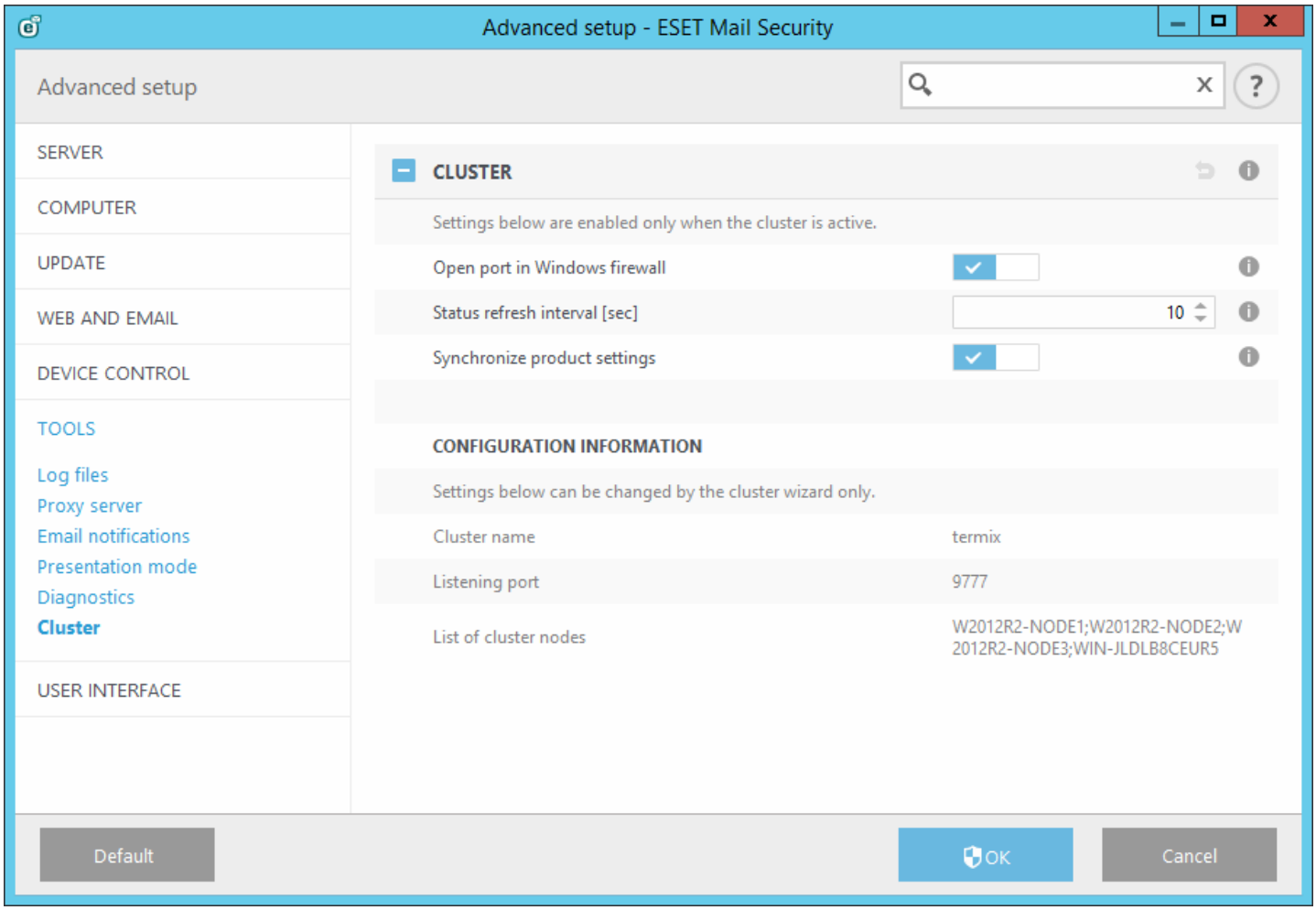
5.6.12 Кластер

Если кластер ESET настроен, параметр **Включить кластер** включается автоматически. Его можно отключить вручную с помощью переключателя в окне дополнительных настроек (это можно сделать, если необходимо изменить конфигурацию, не затрагивая другие узлы в кластере ESET). Данный переключатель только включает или отключает функцию кластера ESET. Чтобы правильно настроить или уничтожить кластер, необходимо использовать мастер кластеров или команду «Уничтожение кластеров» 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.

5.7 Интерфейс пользователя

В разделе **Интерфейс** можно конфигурировать поведение графического интерфейса программы. Здесь можно изменить внешний вид программы и используемые эффекты.

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

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.

Щелчок выделенного объекта правой кнопкой мыши открывает инструмент интеграции в контекстное меню. Этот инструмент позволяет интегрировать элементы управления ESET Mail Security в контекстное меню.

Режим презентации удобен для пользователей, которые хотят работать с приложениями, не отвлекаясь на всплывающие окна, запланированные задачи и любые компоненты, которые могут загружать ресурсы системы.

Элементы интерфейса

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

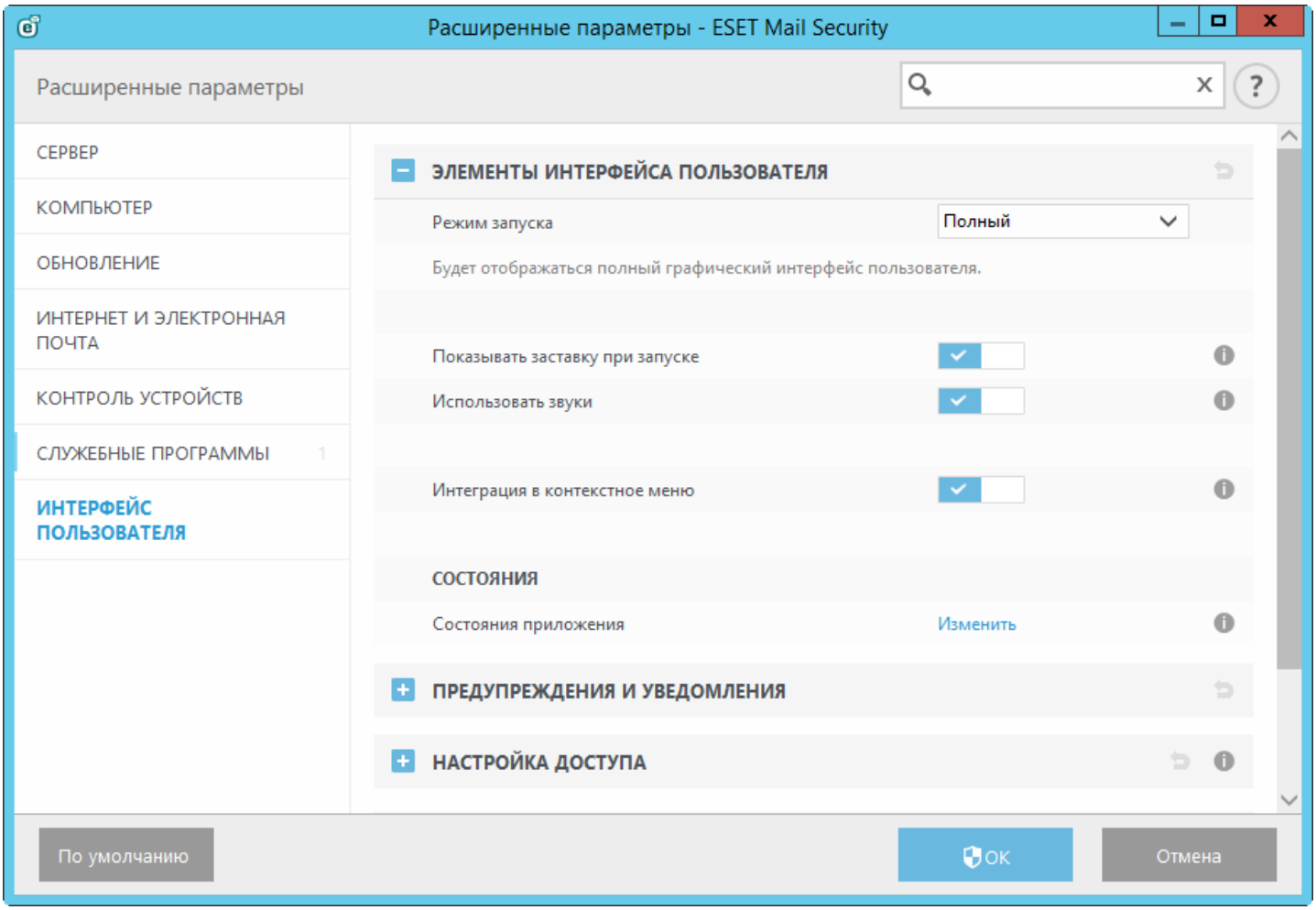
В разделе **Элементы интерфейса пользователя** можно настроить рабочую среду. Если графические элементы снижают производительность компьютера или вызывают другие проблемы, для параметра интерфейса необходимо задать значение **Терминал**. Кроме того, на сервере терминалов рекомендуется отключить графический интерфейс пользователя. Дополнительные сведения о программе ESET Mail Security, установленной на сервере терминалов, см. в разделе Отключение графического интерфейса пользователя на сервере терминалов.

Щелкните раскрывающееся меню **Режим запуска** и выберите один из следующих режимов запуска.
Полный — графический интерфейс будет отображаться полностью.
Терминал — уведомления и предупреждения не отображаются. Графический интерфейс пользователя может быть запущен только администратором.

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

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

Интеграция в контекстное меню — интеграция элементов управления ESET Mail Security в контекстное меню.



Состояния — чтобы управлять состояниями (включать их или выключать), отображаемыми в главном меню на панели Мониторинг, щелкните элемент Изменить. **Состояния приложения** — возможность включения и отключения отображения состояний в главном меню в области **Состояние защиты**.

Информация о лицензии: этот параметр включает информацию о лицензии, сообщения и оповещения.

5.7.1 Предупреждения и уведомления

При помощи раздела **Предупреждения и уведомления** вкладки **Интерфейс** для программы ESET Mail Security можно настроить способ обработки предупреждений об угрозах и системных уведомлений (например, 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).

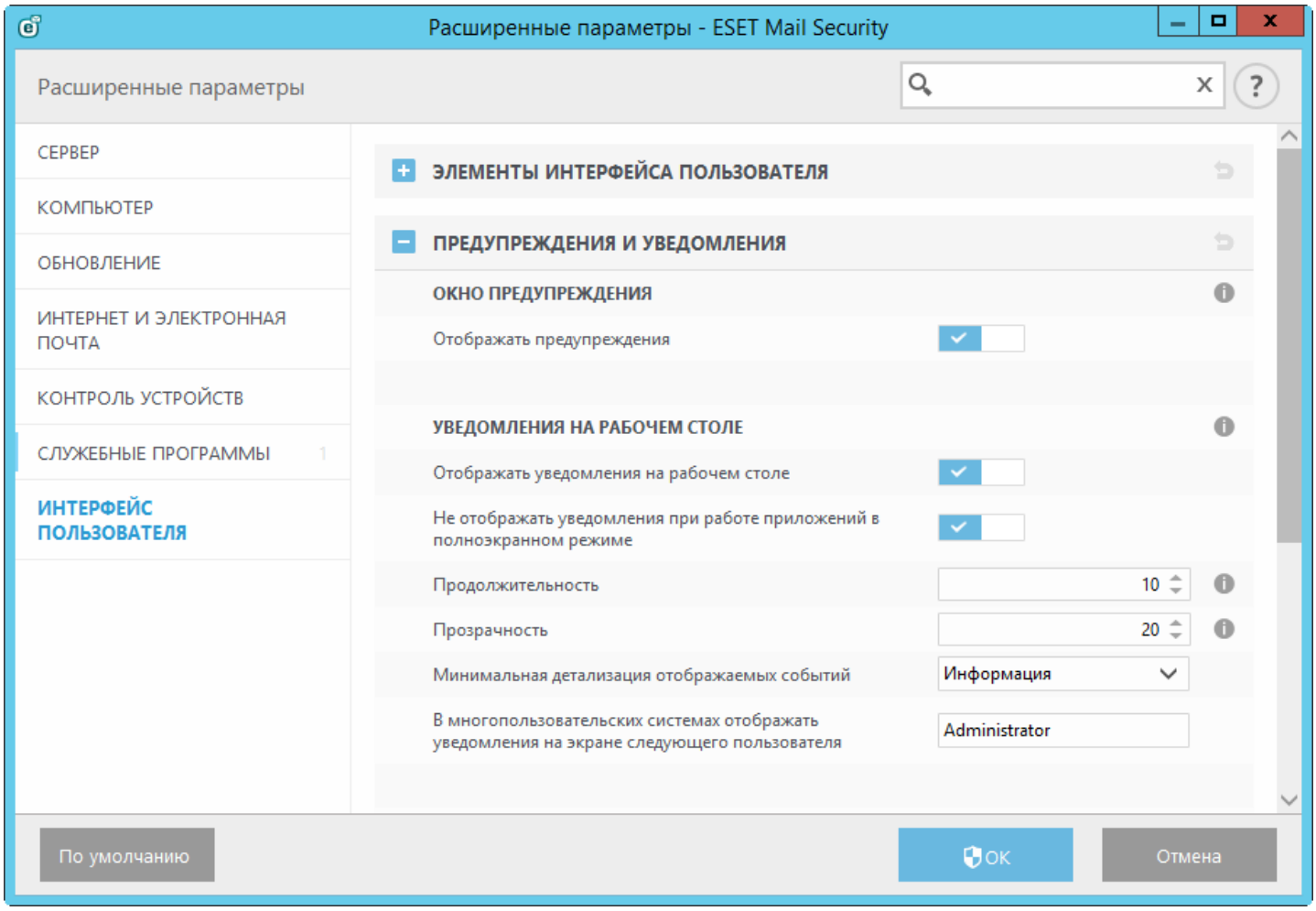
Окна предупреждений

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).

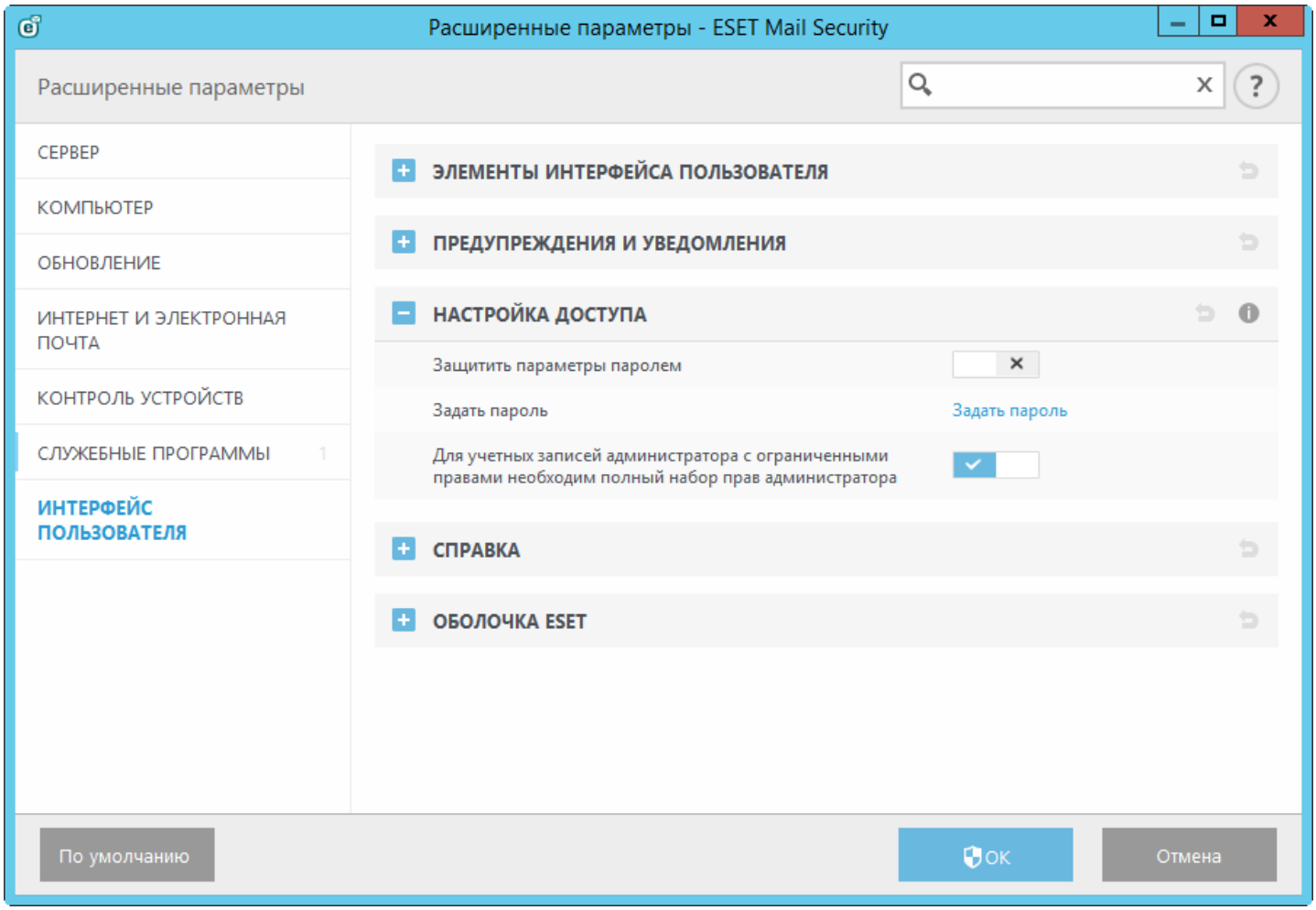
Последний параметр этого раздела позволяет настроить, кто именно должен получать уведомления в многопользовательской среде. В поле **В многопользовательских системах отображать уведомления для пользователя** указывается пользователь, который будет получать системные и прочие уведомления, если одновременно 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.

5.7.2 Настройка доступа

Для обеспечения максимальной безопасности системы важно правильно настроить ESET Mail Security. Неквалифицированное изменение параметров может привести к потере важных данных. Для предотвращения несанкционированного изменения параметры ESET Mail Security можно защитить паролем. Параметры защиты паролем расположены в подменю **Настройка доступа** в разделе **Интерфейс** в дереве «Дополнительные настройки».



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.

5.7.2.1 Пароль

Для предотвращения несанкционированного изменения параметры ESET Mail Security можно защитить паролем.

5.7.2.2 Настройка пароля

Для защиты параметров установки ESET Mail 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 **ОК**. Этот пароль будет необходим для внесения в будущем любых изменений в ESET Mail Security.

5.7.3 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.

5.7.4 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. 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.

5.7.5 Отключение графического интерфейса пользователя на сервере терминалов

В этой главе описывается процесс отключения графического интерфейса пользователя программы ESET Mail Security при выполнении на сервере терминалов Windows для сеансов работы пользователя.

Обычно графический интерфейс пользователя ESET Mail 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 Mail Security на сервер Citrix, рекомендуется использовать параметры, описанные в нашей статье базы знаний.

5.7.6 Отключенные сообщения и состояния

Подтверждения — показывает список подтверждений, отображение которых можно включить или выключить.

Отключенные состояния приложений — возможность включения и отключения отображения состояний в главном меню в области **Состояние защиты**.

5.7.6.1 Подтверждения

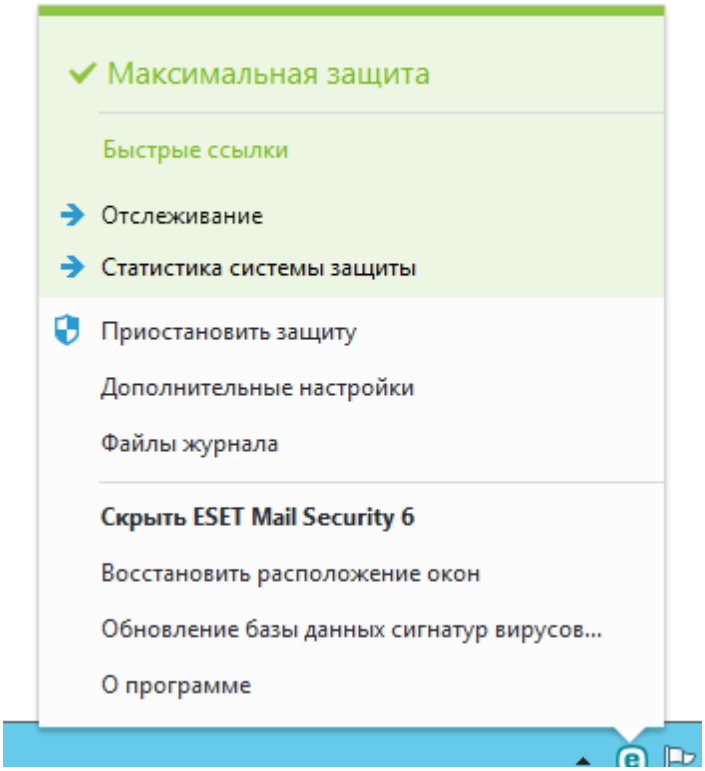
В этом диалоговом окне отображаются подтверждения, выводимые программой ESET Mail Security перед выполнением какого-либо действия. Установите или снимите флажок рядом с каждым типом подтверждения, чтобы включить или отключить подтверждения этого типа.

5.7.6.2 Отключенные состояния приложений

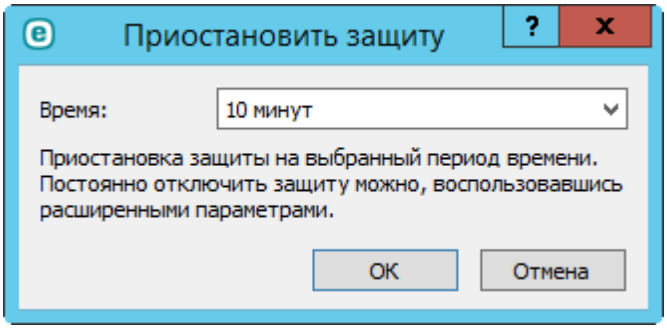
В этом диалоговом окне можно выбрать, какие состояния приложений нужно отображать, а какие — нет. Например, временное отключение защиты от вирусов и шпионских программ или включение режима презентации. Кроме того, состояние приложения будет отображаться, если продукт не активирован или срок действия лицензии истек.

5.7.7 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 к дереву **Дополнительные настройки**. Перейти к дополнительным настройкам можно также с помощью клавиши F5 или через меню **Настройки**.

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

Скрыть ESET Mail Security — эта команда позволяет скрыть окно ESET Mail Security.

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

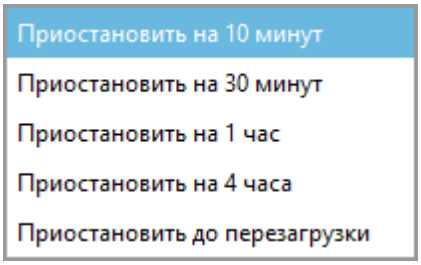
Обновление базы данных сигнатур вирусов — запуск обновления базы данных сигнатур вирусов для поддержания необходимого уровня защиты от вредоносного кода.

О программе — отображение системной информации, сведений об установленной версии ESET Mail Security и модулях программы, а также срока действия лицензии. В нижней части окна представлена информация об

операционной системе и системных ресурсах.

5.7.7.1 Приостановка защиты

Когда пользователь щелкает значок на панели задач, чтобы временно приостановить защиту от вирусов и шпионских программ, отображается диалоговое окно **Временная приостановка защиты**. В этом окне можно приостановить защиту от вредоносного ПО на определенный период времени (чтобы отключить защиту насовсем, откройте область интерфейса «Расширенные параметры»). Будьте осторожны: отключение защиты может сделать систему уязвимой для угроз.

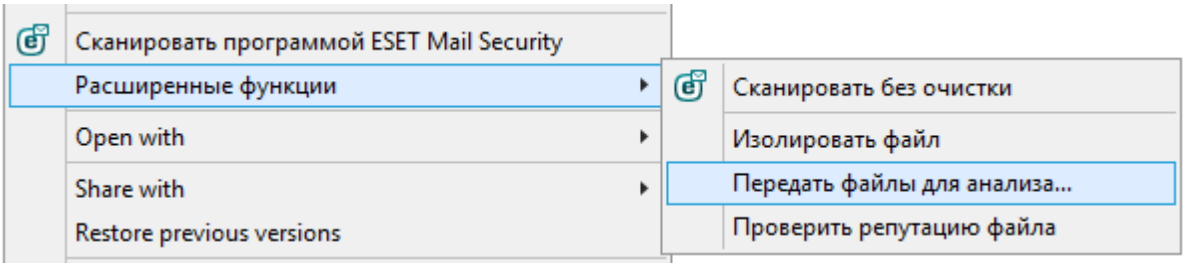


5.7.8 Контекстное меню

Если щелкнуть объект (файл) правой кнопкой мыши, отобразится контекстное меню. В меню указаны все действия, которые можно выполнить с объектом.

В контекстное меню можно интегрировать элементы управления ESET Mail Security. Настройка этой функции выполняется в дереве дополнительных настроек, в разделе **Интерфейс** > **Элементы интерфейса пользователя**.

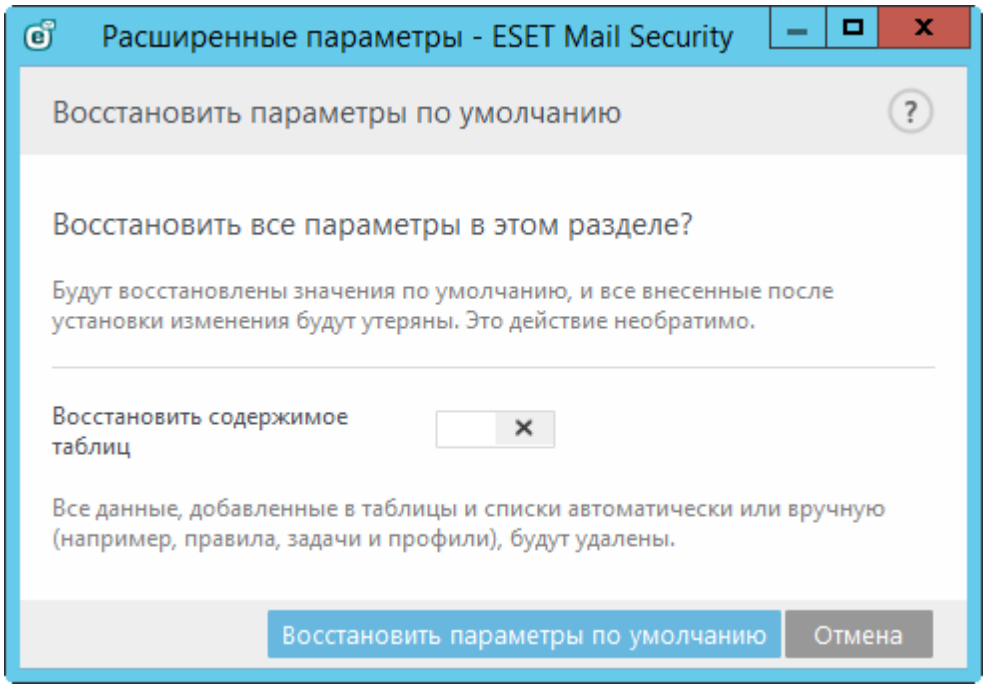
Интеграция в контекстное меню — интеграция элементов управления ESET Mail Security в контекстное меню.



5.8 Восстановление всех параметров в разделе

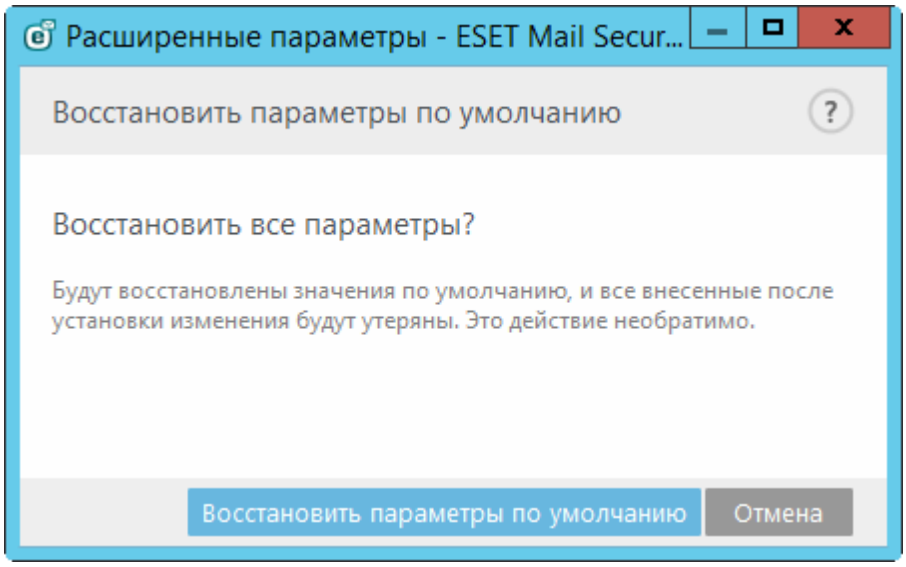
Восстановление параметров модуля по умолчанию, заданных компанией ESET. Следует помнить, что после нажатия кнопки **Восстановить параметры по умолчанию** любые внесенные изменения будут утеряны.

Восстановить содержимое таблиц — при активации этой функции все правила, задачи и профили, добавленные автоматически или вручную, будут удалены.



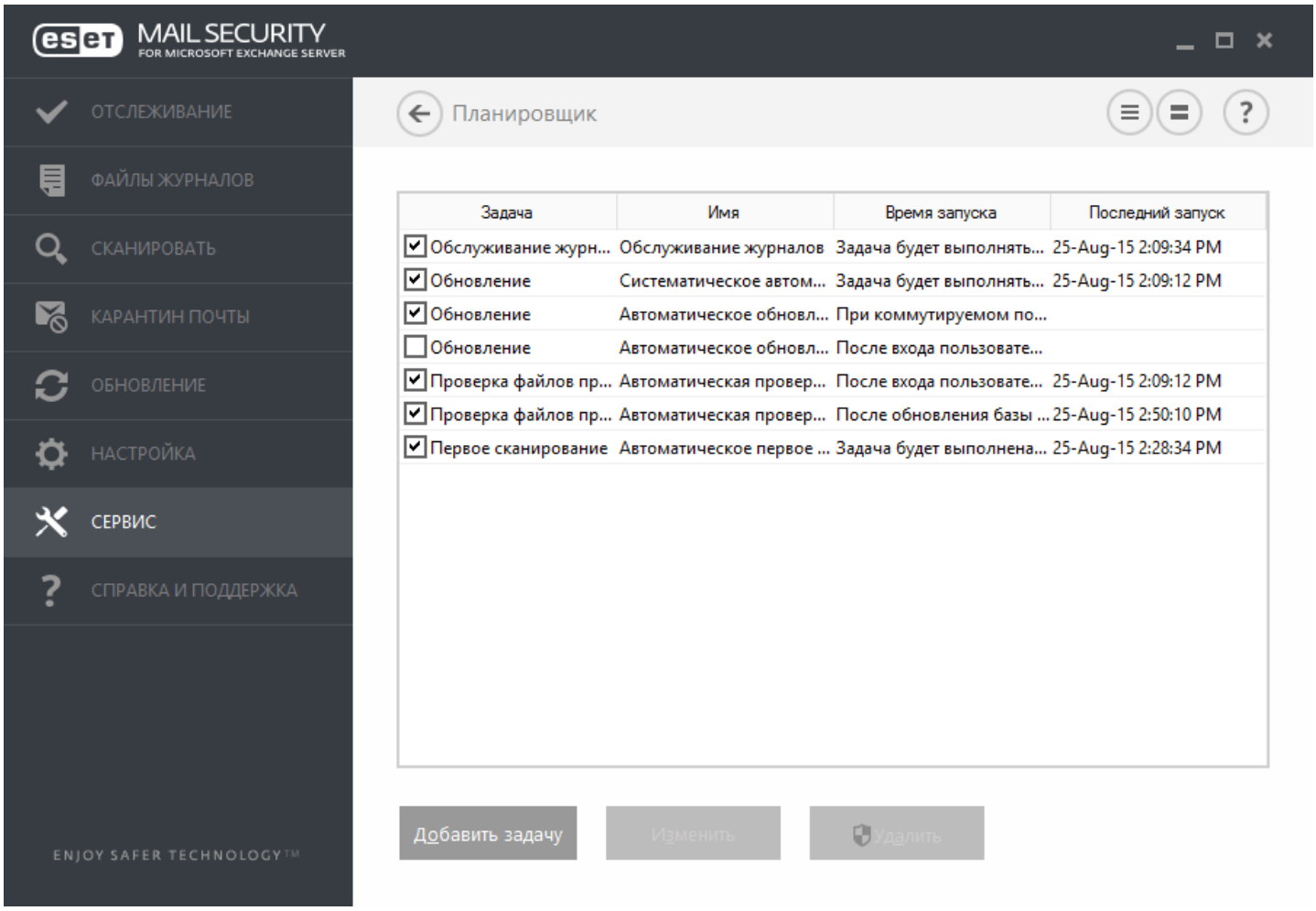
5.9 Восстановление параметров по умолчанию

Все параметры программы для всех модулей будут восстановлены до состояния, в котором они бы были после установки заново.



5.10 Планировщик

Перейти к **планировщику** можно через главное меню ESET Mail Security, воспользовавшись пунктом **Сервис**. В планировщике содержится полный список всех запланированных задач и их свойства, такие как заданные дата, время и используемый профиль сканирования.



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

- **Обслуживание журнала**
- **Регулярное автоматическое обновление**
- **Автоматическое обновление после установки коммутируемого соединения**
- **Автоматическое обновление после входа пользователя в систему**
- **Автоматическая проверка файлов при запуске системы (после входа пользователя в систему)**
- **Автоматическая проверка файлов при запуске (после обновления базы данных сигнатур вирусов)**
- **Автоматическое первое сканирование**

Для изменения параметров существующей запланированной задачи (как существующей по умолчанию, так и пользовательской) щелкните нужную задачу правой кнопкой мыши и выберите в контекстном меню пункт **Изменить...** или выделите задачу, которую необходимо изменить, и нажмите кнопку **Изменить...**.

5.10.1 Сведения о задаче

Введите имя задачи и выберите элемент **Тип задачи**, а затем нажмите кнопку **Далее**.

- **Запуск внешнего приложения**
- **Обслуживание журнала**
- **Проверка файлов, исполняемых при запуске системы**
- **Создать снимок состояния компьютера**
- **Сканирование компьютера по требованию**
- **Первое сканирование**
- **Обновление**
- **Сканирование базы данных**
- **Отправить отчеты о карантине почты**: отправляется отчет о карантине почты (применяется только к локальному карантину) на основании, определенном в запланированной задаче, и на указанный адрес электронной почты. Если используется не локальный карантин почты, отчеты о карантине отправляться не будут.

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

Задача может быть пропущена, если компьютер выключен или работает от аккумулятора. Нажмите кнопку **Далее**, выбрав один из следующих режимов запуска задачи:

- В следующее запланированное время
- как можно скорее;
- незамедлительно, если с момента последнего запуска прошло больше времени, чем указано (в часах).

5.10.2 Время задачи: однократно

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

5.10.3 Время задачи

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

- **Однократно** — задача будет выполнена однократно в установленные дату и время.
- **Многократно** — задача будет выполняться регулярно через указанный промежуток времени (в часах).
- **Ежедневно** — задача будет выполняться раз в сутки в указанное время.
- **Еженедельно** — задача будет выполняться один или несколько раз в неделю в указанные дни и время.
- **При определенных условиях** — задача будет выполнена при возникновении указанного события.

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

5.10.4 Время задачи: ежедневно

Задача будет выполняться один раз в сутки в указанное время.

5.10.5 Время задачи: еженедельно

Задача будет выполняться в выбранный день недели в указанное время.

5.10.6 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.

5.10.7 Сведения о задаче: запуск приложения

На этой вкладке можно запланировать выполнение внешнего приложения.

- **Исполняемый файл**: выберите исполняемый файл в дереве каталогов, щелкните элемент **...** или введите путь вручную.
- **Рабочая папка**: задайте рабочий каталог внешнего приложения. В этом каталоге будут создаваться все временные файлы выбранного **исполняемого файла**.
- **Параметры** — параметры командной строки для приложения (необязательно).

Для применения задачи нажмите кнопку **Готово**.

5.10.8 Сведения о задаче — отправка отчетов о карантине почты

Эта задача помещает в расписание отправку по электронной почте отчета Карантин почты.

- **Адрес отправителя**: с помощью этого параметра можно указать адрес электронной почты, который будет отображен в качестве отправителя отчета о карантине почты.
- **Максимальное число записей в отчете**: вы можете ограничить количество записей, приходящихся на отчет. По умолчанию задано 50 записей.
- **URL-адрес веб-сайта**: этот URL-адрес будет включен в отчет о карантине почты. Получателю достаточно будет щелкнуть его, чтобы получить доступ к веб-интерфейсу карантина почты.
- **Получатели**: этот параметр позволяет выбрать тех, кто будет получать отчеты о карантине почты. Щелкните **Изменить**, чтобы выбрать почтовые ящики определенных получателей. Вы можете выбрать нескольких получателей.

Нажмите кнопку **Готово**, чтобы завершить создание запланированной задачи.

5.10.9 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 этого параметра задача всегда будет повторяться через указанный период времени (в часах).

5.10.10 Информация о задаче планировщика

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

5.10.11 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.

5.10.12 Создание новых задач

Чтобы создать задачу в планировщике, нажмите кнопку **Добавить задачу** или щелкните правой кнопкой мыши и выберите в контекстном меню команду **Добавить**. Запланировать можно пять типов задач.

- **Запуск внешнего приложения** — планирование запуска внешнего приложения.
- **Обслуживание журнала**: в файлах журналов также содержатся остатки удаленных записей. Для эффективной работы эта задача регулярно оптимизирует записи в файлах журналов.
- **Проверка файлов, исполняемых при запуске системы** — проверка файлов, исполнение которых разрешено при запуске системы или входе пользователя в систему.
- **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 программные модули и база данных сигнатур вирусов.

Поскольку **обновление** — одна из самых часто используемых запланированных задач, ниже описано добавление задачи обновления.

Введите имя задачи в поле **Имя задачи**. В раскрывающемся меню **Тип задачи** последовательно выберите элементы **Обновление** и **Далее**.
Активируйте кнопку **Включено** при необходимости активировать задачу (это можно сделать позже, установив или сняв флажок в списке запланированных задач), нажмите кнопку **Далее** и выберите один из режимов времени выполнения:
Однократно, **Многократно**, **Ежедневно**, **Еженедельно** и **При определенных условиях**. В зависимости от указанной частоты запуска будут запрошены различные параметры обновления. Затем укажите, какое действие следует предпринимать, если задача не может быть выполнена в установленное время. Доступны следующие три варианта.

- **В следующее запланированное время**
- **Как можно скорее**
- **Незамедлительно, если с момента последнего запуска прошло больше времени, чем указано** (интервал можно указать с помощью полосы прокрутки «Время с момента последнего запуска»).

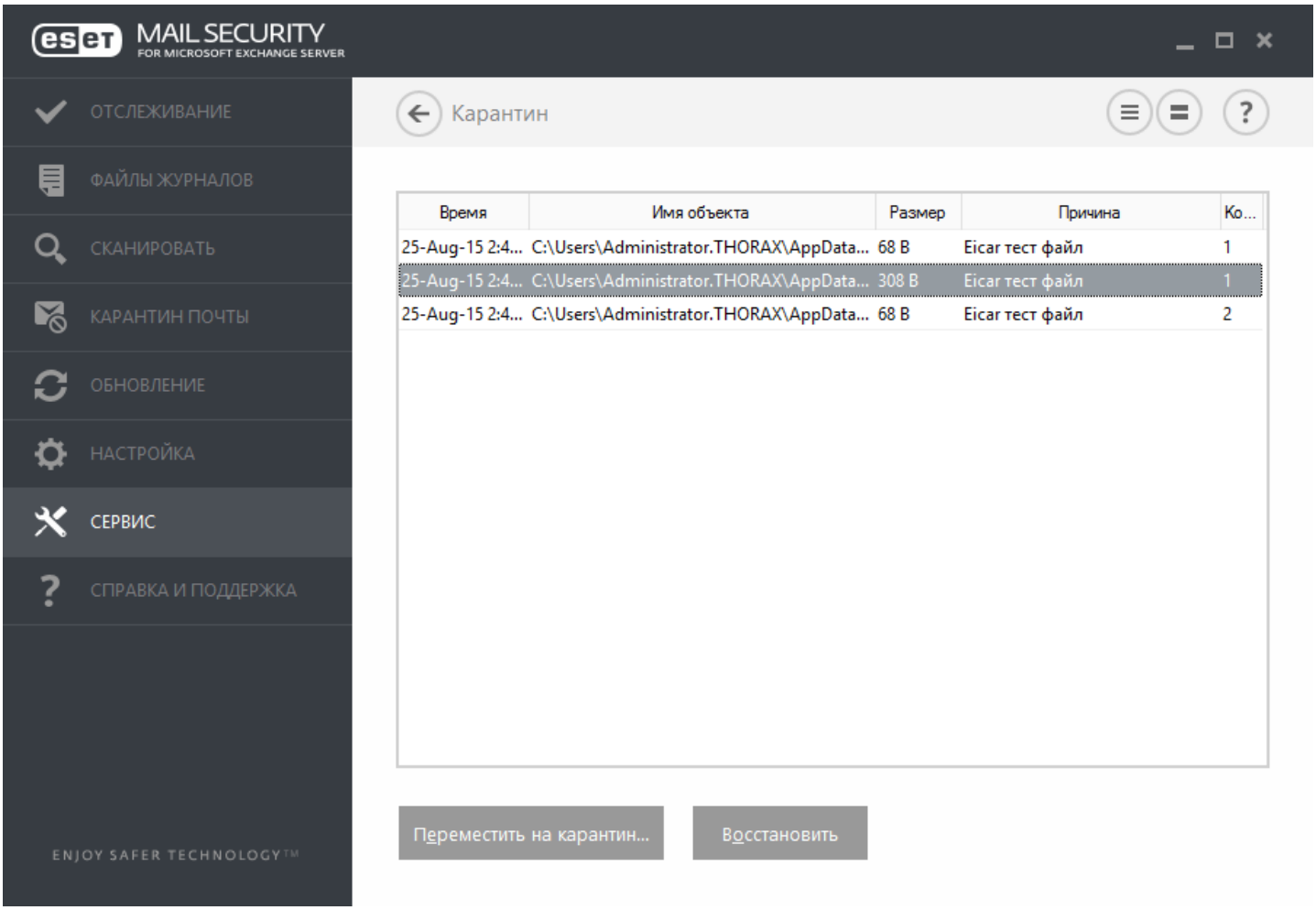
На следующем этапе отображается окно сводной информации о текущей планируемой задаче. После внесения необходимых изменений нажмите кнопку **Готово**.

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

5.11 Карантин

Карантин предназначен в первую очередь для изоляции и безопасного хранения зараженных файлов. Файлы следует помещать на карантин, если их нельзя вылечить или безопасно удалить либо если они отнесены программой ESET Mail 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 Mail 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 помещения файлов на карантин можно воспользоваться также контекстным меню. Щелкните правой кнопкой мыши в окне **Карантин** и выберите 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 по нужному файлу 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) и изолирован, передайте файл в вирусную лабораторию ESET. Чтобы отправить файл из карантина, щелкните его правой кнопкой мыши и выберите пункт **Передать на анализ**.

5.11.1 Помещение файлов на карантин

Программа ESET Mail 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**.

5.11.2 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 в карантин по ошибке, после восстановления исключите этот файл из задачи сканирования и отправьте его в службу поддержки клиентов ESET.

5.11.3 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**.

5.12 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.

6. Глоссарий

6.1 Типы заражений

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

6.1.1 Вирусы

Компьютерный вирус — это 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» к заражаемому файлу. 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 возможных 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.

6.1.2 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.

6.1.3 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.

6.1.4 Руткиты

Руткитом называется вредоносная программа, которая предоставляет злоумышленникам полный доступ к компьютеру, не проявляя при этом своего присутствия в системе. После получения доступа к системе (обычно путем использования ее уязвимостей) руткиты используют функции операционной системы, чтобы избежать обнаружения программным обеспечением защиты от вирусов: используются механизмы маскировки процессов, файлов и данных 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 Mail Security есть преимущества технологии Anti-Stealth, которая позволяет обнаружить и устранить активные руткиты.

6.1.5 Рекламные программы

Под рекламной программой понимается программное обеспечение, существующее за счет рекламы. Программы, демонстрирующие пользователю рекламные материалы, относятся к этой категории. Рекламные приложения часто автоматически открывают всплывающие окна с рекламой в веб-браузере или изменяют домашнюю страницу. 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.

6.1.6 Шпионские программы

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

Авторы шпионских программ утверждают, что эти технологии служат для изучения требований и интересов пользователей и позволяют создавать рекламные материалы, более соответствующие целевой аудитории. Проблема заключается в том, что нет четкой границы между полезными и вредоносными приложениями и никто не гарантирует, что получаемая информация не будет использована во вред. Данные, полученные шпионскими программами, могут содержать защитные коды, PIN-коды, номера 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 шпионских программ во время установки основной программы, чтобы поощрить их к приобретению платной версии.

Примерами хорошо известного бесплатного программного обеспечения, вместе с которым поставляется шпионское, могут служить клиенты 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.

6.1.7 Упаковщики

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

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

6.1.8 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 Live Grid. 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).

6.1.9 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.

6.1.10 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 Mail Security помогает 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.

6.1.11 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.

6.2 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.

6.2.1 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.

6.2.2 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 в получателях страх, неуверенность и мнительность, побуждая их верить в то, что «не поддающийся обнаружению вирус» удаляет их файлы, крадет пароли или выполняет какие-либо другие крайне нежелательные действия с компьютерами.

Некоторые мистификации работают, предлагая получателям переслать сообщение своим знакомым, 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.

6.2.3 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.

6.2.4 Распознавание мошеннических сообщений

Вообще существует несколько признаков, которые могут помочь распознать спам (нежелательные сообщения) в почтовом ящике. Сообщение, наиболее вероятно, является нежелательным, если оно соответствует хотя бы нескольким из следующих критериев:

- Адрес отправителя отсутствует в адресной книге получателя.
- Предлагается получить большую сумму денег, но сначала нужно оплатить небольшую сумму.
- Под разными предлогами (проверка данных, финансовые операции) предлагается предоставить какие-либо личные данные, такие как номера банковских счетов, имя пользователя, пароль и т. д.
- Сообщение написано на иностранном языке.
- Предлагается купить продукцию, в которой получатель не заинтересован. Однако если вы все же решите совершить покупку, следует убедиться, что отправитель сообщения является надежным продавцом (например, проконсультироваться с производителем продукции).
- Некоторые из слов намеренно написаны с ошибками, чтобы обмануть фильтр спама. Например, «веагро» вместо «виагра» и т. п.

6.2.4.1 Правила

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

1) условие (например, получение сообщения с определенного адреса);

2) действие (например, удаление сообщения, перемещение его в указанную папку).

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

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

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

6.2.4.2 Байесовский фильтр

Фильтрация спама Байеса является эффективным методом фильтрации электронной почты, который применяется в большинстве приложений для защиты от спама. Он позволяет идентифицировать нежелательные сообщения с высокой точностью и может настраиваться для каждого пользователя отдельно.

Метод основан на следующих принципах. На первом этапе происходит процесс обучения. Пользователь вручную помечает достаточное количество сообщений как нормальные или спам (обычно 200 и 200). Фильтр анализирует обе категории и узнает, например, что в спаме часто содержатся слова «Ролекс» или «Виагра», тогда как нормальные сообщения отправляются членами семьи или корреспондентами из адресной книги пользователя. После обработки достаточного количества сообщений фильтр Байеса может присвоить каждому сообщению определенный «индекс спама», показывающий, является ли данное сообщение спамом.

Основным преимуществом фильтра Байеса является гибкость. Например, если пользователь по профессии биолог, всем входящим сообщениям, содержимое которых может быть отнесено к биологии и другим близким сферам знаний, обычно будет присвоен более низкий индекс вероятности. Если сообщение содержит слова, которые обычно позволяют классифицировать его как нежелательное, но при этом оно было отправлено корреспондентом из адресной книги пользователя, оно будет помечено как нормальное. Это происходит потому, что наличие отправителя в адресной книге уменьшает общую вероятность спама.

6.2.4.3 «Белый» список

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

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

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

6.2.4.4 «Черный» список

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

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

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

6.2.4.5 Контроль на стороне сервера

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

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