ESET MAIL SECURITY

ДЛЯ MICROSOFT EXCHANGE SERVER

Инструкция по установке и руководство пользователя

Microsoft® Windows® Server 2000 / 2003 / 2008 / 2008 R2

Щелкните здесь, чтобы загрузить актуальную версию этого документа

ESET MAIL SECURITY

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

Международная служба поддержки клиентов: www.eset.eu/support
Служба поддержки клиентов в Северной Америке: www.eset.com/support

Версия 1/9/2012

Содержание

1. Введение

ESET Mail Security 4 для Microsoft Exchange Server — это интегрированное решение, которое защищает почтовые ящики от различных типов вредоносных программ, в том числе вложений в сообщения электронной почты, зараженных червями и троянскими программами, документов, в которых содержатся вредоносные сценарии, 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.

ESET Mail Security поддерживает Microsoft Exchange Server версий 5.5 и более поздних, а также Microsoft Exchange Server в кластерной среде. В более новых версиях (Microsoft Exchange Server 2007 и более поздние версии) также поддерживаются конкретные роли (почтовый ящик, концентратор, пограничный сервер). Можно удаленно управлять ESET Mail Security в больших сетях с помощью ESET Remote Administrator.

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

1.1 Новые возможности в версии 4.3

По сравнению с версией ESET Mail Security 4.2 в версии 4.3 были добавлены следующие нововведения и усовершенствования.

- Добавлены новые журналы для модуля защиты от спама и работы с «серыми» списками, в которых приводится подробная информация о сообщениях, обработанных соответствующим модулем. В журнале защиты от спама также подробно указываются причины, по которым сообщения были классифицированы как СПАМ.

- Автоматические исключения улучшают общую стабильность и непрерывность работы сервера. Теперь достаточно одного щелчка мыши, чтобы задать целые комплекты исключений из сканирования защитой от вирусов для конкретных серверных приложений и файлов операционной системы.

- Классификация сообщений по значению оценки нежелательности. Теперь администраторы могут указывать собственные диапазоны оценки нежелательности, которые будут определять, какие именно сообщения будут классифицироваться как спам, для точной настройки фильтрации защиты от спама.

- Объединение лицензий. ESET Mail Security позволяет использовать несколько лицензий, тем самым увеличивая количество защищаемых почтовых ящиков.

1.2 Системные требования

Поддерживаемые операционные системы

- Microsoft Windows NT 4.0 с пакетом обновления SP6, SP6a
- Microsoft Windows 2000 Server
- Microsoft Windows Server 2003 (x86 и x64)
- Microsoft Windows Server 2008 (x86 и x64)
- Microsoft Windows Server 2008 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)

Поддерживаемые версии Microsoft Exchange Server

- Microsoft Exchange Server 5.5 с пакетом обновления SP3, SP4
- Microsoft Exchange Server 2000 с пакетом обновления SP1, SP2, SP3
- 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

Требования к оборудованию зависят от используемых версий операционной системы и Microsoft Exchange Server. Рекомендуется ознакомиться с документацией на Microsoft Exchange Server для получения дополнительных сведений о требованиях к оборудованию.

1.3 Используемые методы

Для сканирования сообщений электронной почты используется два независимых метода.

Сканирование почтовых ящиков с помощью VSAPI 6
Фильтрация сообщений на уровне SMTP-сервера 7

1.3.1 Сканирование почтовых ящиков с помощью VSAPI

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 Фильтрация сообщений на уровне SMTP-сервера

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* 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.

1.4 Типы защиты

Существует три типа защиты.

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 злонамеренным кодом, модуль защиты от вирусов может устранить ее, сначала заблокировав, а затем очистив, удалив или поместив на карантин 82.

1.4.2 Защита от спама

Для защиты от спама используется ряд технологий («черные» списки реального времени, DNSBL, идентификация крупных объемов данных по их фрагментам, проверка репутации, анализ содержимого, байесовский фильтр, правила, работа с «белыми» и «черными» списками вручную и т. д.) для обеспечения максимально качественного обнаружения угроз в электронной почте. Модуль сканирования защиты от спама формирует значение вероятности спама для конкретного сообщения электронной почты в процентах (от 0 до 100).

Другим компонентом модуля защиты от спама является метод работы с «серыми» списками (отключен по умолчанию). Данный метод основан на спецификации RFC 821, в которой говорится о том, что в связи с тем, что SMTP считается ненадежным методом передачи, каждый агент передачи сообщений должен повторно пытаться доставить сообщение после временного сбоя доставки. Большая часть спама представляет собой однократно отправляемые сообщения (с помощью специализированных средств) по автоматически созданному списку адресов электронной почты. Сервер, применяющий работу с «серыми» списками, вычисляет 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.

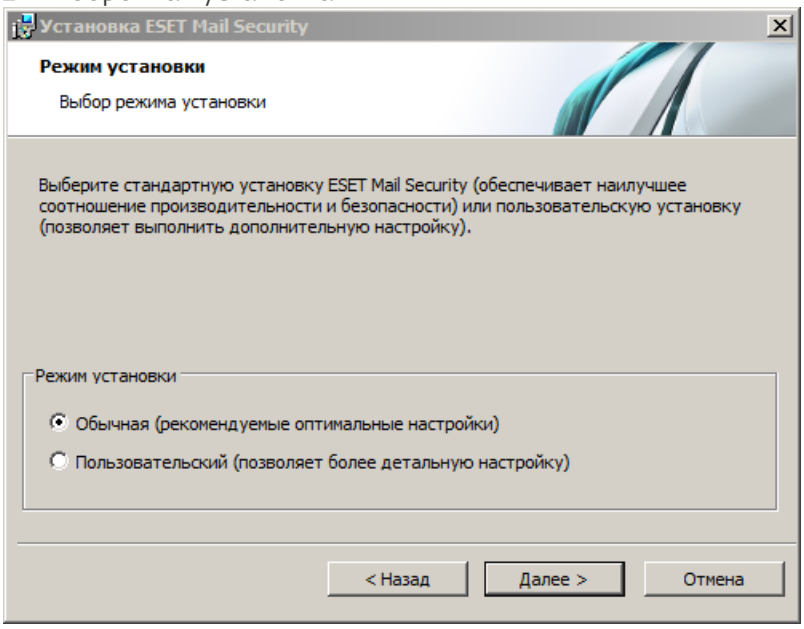
1.5 Интерфейс пользователя

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 пользователя существует также и **дерево расширенных параметров**, которое можно открыть с любой страницы программы, нажав клавишу F5. После нажатия клавиши F5 открывается окно дерева расширенных параметров, в котором отображается перечень настраиваемых функций программы. В этом окне можно конфигурировать параметры в соответствии со своими потребностями. Древовидная структура разбита на два раздела: **Защита сервера** и **Защита компьютера**. В разделе **Защита сервера** содержатся элементы, относящиеся к тем параметрам ESET Mail Security, которые регулируют защиту сервера Microsoft Exchange Server. В разделе **Защита компьютера** содержатся настраиваемые элементы для защиты самого сервера.

2. Установка

После приобретения ESET Mail Security установочный файл можно загрузить с веб-сайта ESET (www.eset.com) в виде пакета с расширением .msi. После запуска этого файла мастер установки поможет установить программу. Существует два типа установки, которые отличаются уровнями выбора параметров.

1. Обычная установка
2. Выборочная установка

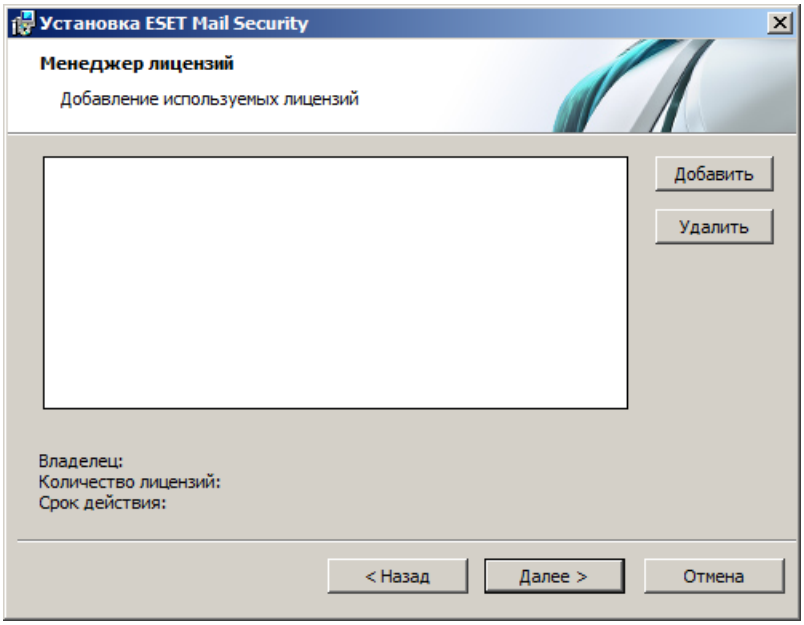


ПРИМЕЧАНИЕ: Настоятельно рекомендуется устанавливать ESET Mail Security в только что установленной и сконфигурированной операционной системе, если это возможно. Однако при возникновении необходимости в установке программного продукта на существующей системе лучше всего удалить предыдущую версию ESET Mail Security, перезапустить сервер и установить ESET Mail Security 4.5 после этого.

2.1 Обычная установка

Режим обычной установки позволяет быстро установить ESET Mail Security, выполнив в процессе установки лишь минимальные изменения конфигурации. Обычная установка — это режим установки по умолчанию; при отсутствии особых требований не рекомендуется выбирать другой режим. После установки ESET Mail Security на компьютере можно в любой момент изменить параметры и конфигурацию программы. В настоящем руководстве пользователя эти параметры и функциональность описываются подробно Параметры, активируемые в режиме обычной установки, обеспечивают отличный уровень безопасности в сочетании с удобством использования и высокой производительностью компьютера.
После выбора режима установки и нажатия кнопки «Далее» предлагается ввести имя пользователя и пароль. Этот этап играет важную роль в обеспечении постоянной защиты компьютера, так как имя пользователя и пароль делают возможным автоматическое обновление 70 базы данных сигнатур вирусов. Введите имя пользователя и пароль, полученные после покупки или регистрации программного продукта, в соответствующие поля. Если имени пользователя и пароля пока нет, их можно будет ввести непосредственно в программе позднее.

На следующем этапе, в окне **Диспетчер лицензий**, добавьте файл лицензии, который получили по электронной почте после покупки программного продукта.

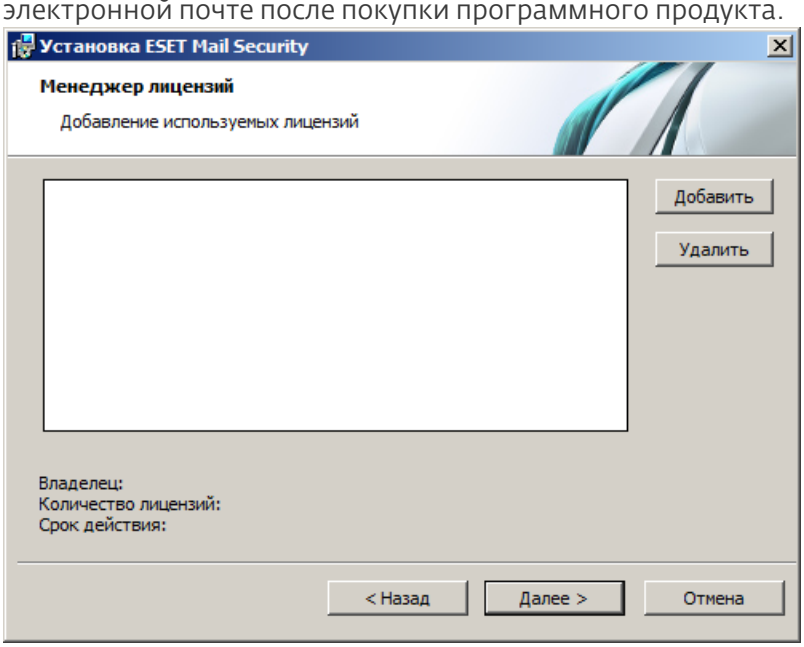


На следующем этапе конфигурируется система своевременного обнаружения ThreatSense.Net. Система своевременного обнаружения ThreatSense.Net предназначена для немедленного непрерывного информирования компании ESET о новых заражениях, что позволяет быстро реагировать и защищать пользователей. Эта система предусматривает отправку новых угроз в лабораторию ESET, где они анализируются, обрабатываются и добавляются в базу данных сигнатур вирусов. По умолчанию флажок **Включить систему своевременного обнаружения ThreatSense.Net** установлен. Для изменения расширенных параметров отправки подозрительных файлов нажмите **Дополнительные настройки...**.
Следующим этапом установки является конфигурирование **обнаружения потенциально нежелательных приложений**. Потенциально нежелательные приложения не обязательно являются вредоносными, но часто негативно влияют на работу операционной системы.
Такие приложения часто поставляются в пакете с другими программами, и их установку бывает трудно заметить при установке всего пакета. Хотя при установке таких приложений обычно на экран выводится уведомление, они вполне могут быть установлены без согласия пользователя.
Рекомендуется выбрать параметр **«Включить обнаружение потенциально нежелательного ПО»**, чтобы разрешить приложению ESET Mail Security выявлять угрозы такого типа. Если использовать эту функцию не следует, установите флажок **Выключить обнаружение потенциально нежелательного ПО**.
Последним этапом обычной установки является подтверждение установки. Для этого нажмите кнопку **Установить**.

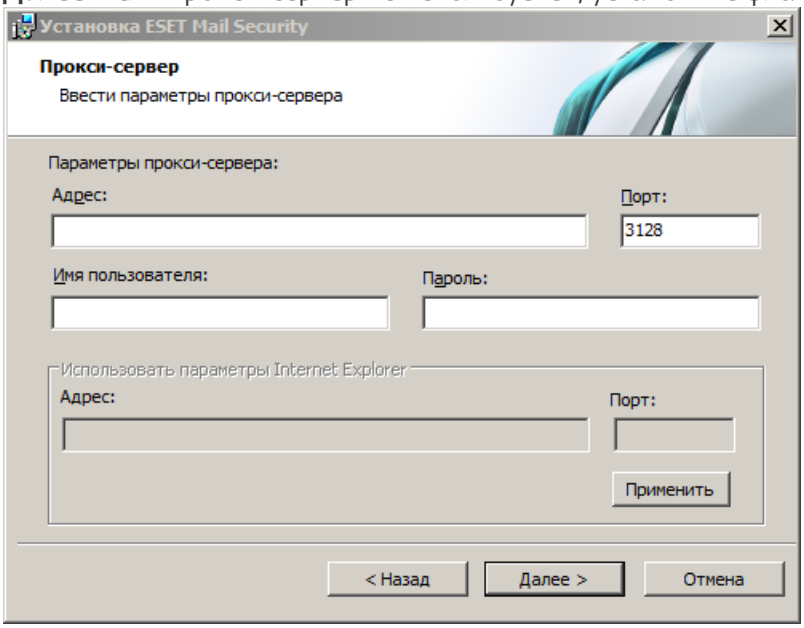
2.2 Выборочная установка

Выборочная установка предназначена для тех пользователей, которые хотят сконфигурировать программное обеспечение ESET Mail Security в ходе процесса установки.
После выбора режима установки и нажатия кнопки **Далее** пользователю будет предложено выбрать папку для установки. По умолчанию программа устанавливается в папку *C:\Program Files\ESET\ESET Mail Security*.
Нажмите кнопку **Обзор...**, чтобы изменить папку (не рекомендуется).
Затем заполните поля **Имя пользователя** и **Пароль**. Это действие аналогично соответствующему действию в режиме обычной установки (см. Обычная установка 9).

На следующем этапе, в окне **Диспетчер лицензий**, добавьте файл лицензии, который получили по электронной почте после покупки программного продукта.

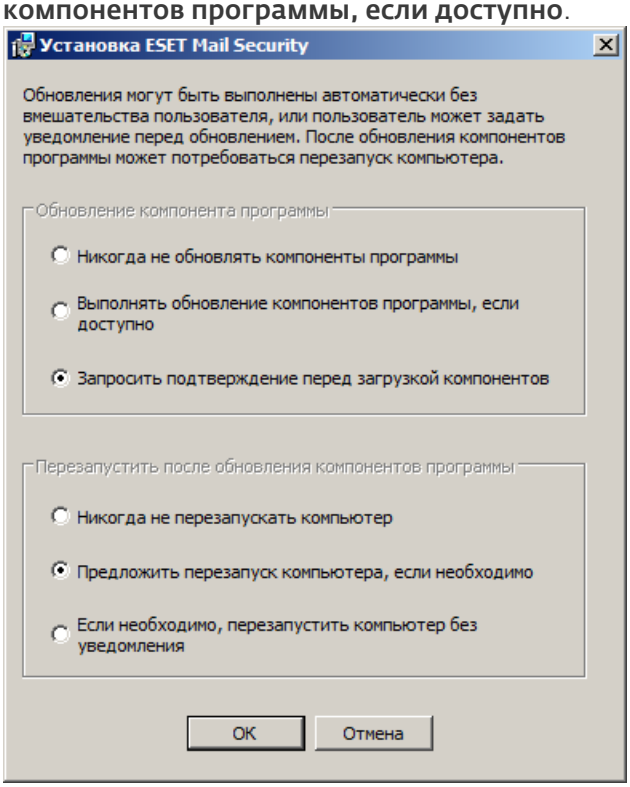


После ввода имени пользователя и пароля нажмите кнопку **Далее**, чтобы перейти к окну **Настройте подключение к Интернету**.
Если используется прокси сервер, он должен быть корректно сконфигурирован для обеспечения нормальной работы обновления сигнатур вирусов. Если нужно сконфигурировать прокси-сервер автоматически, не меняйте параметр по умолчанию **Я не уверен, используется ли прокси-сервер. Я хочу использовать те же параметры, какие использует Internet Explorer (рекомендуется)** и нажмите кнопку **Далее**. Если прокси-сервер не используется, установите флажок **Я не использую прокси-сервер**.



Если же вы предпочитаете ввести данные прокси-сервера самостоятельно, его параметры можно сконфигурировать вручную. Для конфигурирования параметров прокси-сервера выберите вариант **Я использую прокси-сервер** и нажмите кнопку **Далее**. Введите IP-адрес или URL-адрес прокси-сервера в

поле **Адрес**. В поле **Порт** укажите порт, по которому этот прокси-сервер принимает запросы на соединение (по умолчанию 3128). Если прокси-сервер требует аутентификации, введите правильные **имя пользователя** и **пароль** для доступа к нему. Параметры прокси-сервера также по желанию могут быть скопированы из параметров Internet Explorer. После ввода сведений прокси-сервера нажмите кнопку **Применить** и подтвердите свой выбор.
Нажмите **Далее**, чтобы перейти к окну **Настроить параметры автоматического обновления**. На этом этапе можно задать, как в системе будет обрабатываться автоматическое обновление компонентов программы. Нажмите **Изменить...** для доступа к расширенным параметрам.
Если нет необходимости обновлять компоненты программы, выберите вариант **Никогда не обновлять компоненты программы**. Установите флажок **Запросить подтверждение перед загрузкой компонентов**, чтобы перед загрузкой компонентов программы на экран выводилось окно подтверждения. Для автоматической загрузки обновлений компонентов программы выберите вариант **Выполнять обновление компонентов программы, если доступно**.



ПРИМЕЧАНИЕ: После обновления программных компонентов обычно нужно перезагрузить компьютер. Рекомендуется выбрать вариант **Никогда не перезапускать компьютер**. Полученные обновления компонентов будут активированы после следующего перезапуска сервера (вне зависимости от того, выполняется ли такой перезапуск по расписанию 80, вручную или как-либо иначе). Можно выбрать вариант **Предложить перезапуск компьютера, если необходимо**, если нужно, чтобы предлагалось перезапустить сервер после обновления компонентов. Если выбран этот параметр, то можно перезапустить сервер сразу же или отложить перезапуск и выполнить его позднее.
В следующем окне предлагается создать пароль для защиты параметров программы. Установите флажок **Защита параметров конфигурации паролем** и введите пароль в поля **Новый пароль** и **Подтвердить новый пароль**.
Следующие два этапа установки (**Система своевременного обнаружения ThreatSense.Net** и **Обнаружение потенциально нежелательных приложений**) совпадают с этапами режима обычной установки (см. раздел Обычная установка 9).
Нажмите **Установить** в окне **Все готово к установке**, чтобы завершить процесс установки.

2.3 Сервер терминалов

Если программное обеспечение ESET Mail Security установлено 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 106.

2.4 Обновление до новой версии

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

1. Автоматическое обновление путем обновления компонентов программы
   Поскольку обновления компонентов программы распространяются среди всех пользователей и могут повлиять на некоторые конфигурации компьютеров, они выпускаются только после длительного тестирования с целью обеспечения бесперебойного процесса обновления на всех возможных конфигурациях. Если нужно выполнить обновление до более новой версии сразу после ее выхода, нужно воспользоваться одним из описанных далее методов.
2. Обновление вручную путем загрузки и установки новой версии поверх предыдущей установленной
   В начале процесса установки можно принять решение о сохранении существующих параметров программы. Для этого нужно установить флажок **Использовать текущие параметры**.
3. Обновление вручную с автоматическим развертыванием в сетевой среде посредством ESET Remote Administrator.

2.5 Установка в кластерной среде

Кластер — это группа серверов (подключенный к кластеру сервер называется «узлом»), которые работают вместе как один сервер. Такой тип среды обеспечивает высокую доступность и надежность предоставляемых в ней служб. Если один из узлов кластера отказывает или становится недоступным, его функциональность начинает автоматически выполняться другим узлом кластера. ESET Mail Security обеспечивает полную поддержку серверов Microsoft Exchange Server, объединенных в кластер. Для корректной работы ESET Mail Security важно, чтобы у всех узлов кластера была одинаковая конфигурация. Этого можно добиться, применив политику с помощью ESET Remote Administrator (ERA). В следующих главах будет описано, как установить и сконфигурировать ESET Mail Security на серверах в кластерной среде, используя ERA.

Установка

В этой главе описывается метод автоматической установки, хотя это и не единственный способ установки программного продукта на нужный компьютер. Для получения сведений о дополнительных методах установки обратитесь к руководству пользователя ESET Remote Administrator.

1) Загрузите установочный пакет ESET Mail Security *msi* с веб-сайта ESET на тот компьютер, на котором установлено средство ERA. В ERA перейдите на вкладку **Удаленная установка** и в разделе **Компьютеры** щелкните правой кнопкой мыши любой компьютер в списке, после чего выберите в контекстном меню пункт **Управление пакетами**. В раскрывающемся меню **Тип** выберите **Пакет продуктов безопасности ESET** и нажмите кнопку **Добавить...**. В разделе **Источник** найдите загруженный установочный пакет ESET Mail Security и нажмите кнопку **Создать**.

2) В разделе **Изменение или выбор файла конфигурации для этого пакета** нажмите **Изменить** и сконфигурируйте параметры **ESET Mail Security** в соответствии со своими требованиями. Параметры ESET Mail Security находятся в следующих ветвях: **ESET Smart Security, ESET NOD32 Antivirus > Защита почтового сервера** и **Защита почтового сервера для Microsoft Exchange Server**. Также можно задать параметры других модулей, входящих в состав ESET Mail Security (например, модуль обновления, сканирование компьютера и т. д.). Рекомендуется экспортировать сконфигурированные параметры в файл в формате XML, который вы сможете использовать в дальнейшем (например, при создании установочного пакета, применении задачи конфигурации или политики).

3) Нажмите кнопку **Закрыть**. В следующем диалоговом окне (**Сохранить пакет на сервере?**) выберите ответ

Да и введите имя установочного пакета. Готовый установочный пакет (с именем и конфигурацией) будет сохранен на сервере. Чаще всего этот пакет используется для автоматической установки, но его также можно и сохранить как стандартный установочный пакет *msi* и использовать для непосредственной установки на сервере (**Редактор пакетов установки** > **Сохранить как...**).

4) Теперь установочный пакет готов, и можно инициировать удаленную установку на узлах в кластере. В ERA перейдите на вкладку **Удаленная установка** и в разделе **Компьютеры** выберите узлы, на которые следует установить ESET Mail Security (щелкайте левой кнопкой мыши, удерживая клавишу Ctrl или Shift). Правой кнопкой мыши нажмите любой из выбранных компьютеров и выберите пункт контекстного меню **Автоматическая установка**. С помощью кнопок **Задать**/**Задать все** задайте **имя пользователя** и **пароль** для учетной записи на целевом компьютере (это должна быть учетная запись с правами администратора). Нажмите кнопку **Далее**, чтобы выбрать установочный пакет, и запустите процесс удаленной установки, нажав кнопку **Готово**. Установочный пакет, содержащий ESET Mail Security и пользовательские параметры конфигурации, будет установлен на выбранных целевых компьютерах/узлах. Через некоторое время клиенты с ESET Mail Security появятся в ERA на вкладке **Клиенты**. Теперь можно удаленно управлять этими клиентами.

ПРИМЕЧАНИЕ: Для завершения процесса удаленной установки без каких-либо проблем необходимо, чтобы на целевых компьютерах были выполнены определенные условия, как и на сервере ERA Server. Для получения дополнительных сведений см. руководство пользователя ESET Remote Administrator.

Конфигурация

Для того чтобы программа ESET Mail Security корректно работала на узлах кластера, у узлов всегда должна быть одинаковая конфигурация. Это условие выполнено, если использовался описанный выше метод автоматической установки. Однако есть вероятность того, что конфигурация будет изменена по ошибке, что приведет к несоответствиям между программными продуктами ESET Mail Security в пределах кластера. Этого можно избежать, используя политику в ERA. Политика по сути очень схожа с обычной задачей конфигурации — она отправляет конфигурацию, определенную в редакторе конфигурации, клиентам. Отличается же политика от задачи конфигурации тем, что постоянно применяется к клиентам. Поэтому политику можно определить как конфигурацию, которая регулярно принудительно применяется к клиенту или группе клиентов.

В разделе ERA > **Служебные программы** > **Диспетчер политик...** есть ряд параметров, определяющих использование политики. Самым простым является использование варианта **Родительская политика по умолчанию**, которая также обычно служит в качестве **политики по умолчанию для главных клиентов**. Этот вид политики автоматически применяется ко всем подключенным в данный момент клиентам (в данном случае ко всем программным продуктам ESET Mail Security в пределах кластера). Можно сконфигурировать политику, нажав кнопку **Изменить...**, или использовать существующую конфигурацию, сохраненную в файле *xml*, если таковая уже была создана.

Вторым вариантом является создание новой политики (**Добавить новую дочернюю политику**) и использование функции **Добавить клиенты...**, чтобы назначить все программные продукты ESET Mail Security этой политике.

Такая конфигурация позволяет добиться того, что ко всем клиентам будет применена одна и та же политика с одинаковыми параметрами. Если нужно изменить существующие параметры сервера ESET Mail Security в кластере, достаточно изменить текущую политику. Изменения будут применены ко всем клиентам, назначенным данной политике.

ПРИМЕЧАНИЕ: Подробные сведения о политиках приводятся в руководстве пользователя ESET Remote Administrator.

2.6 Лицензия

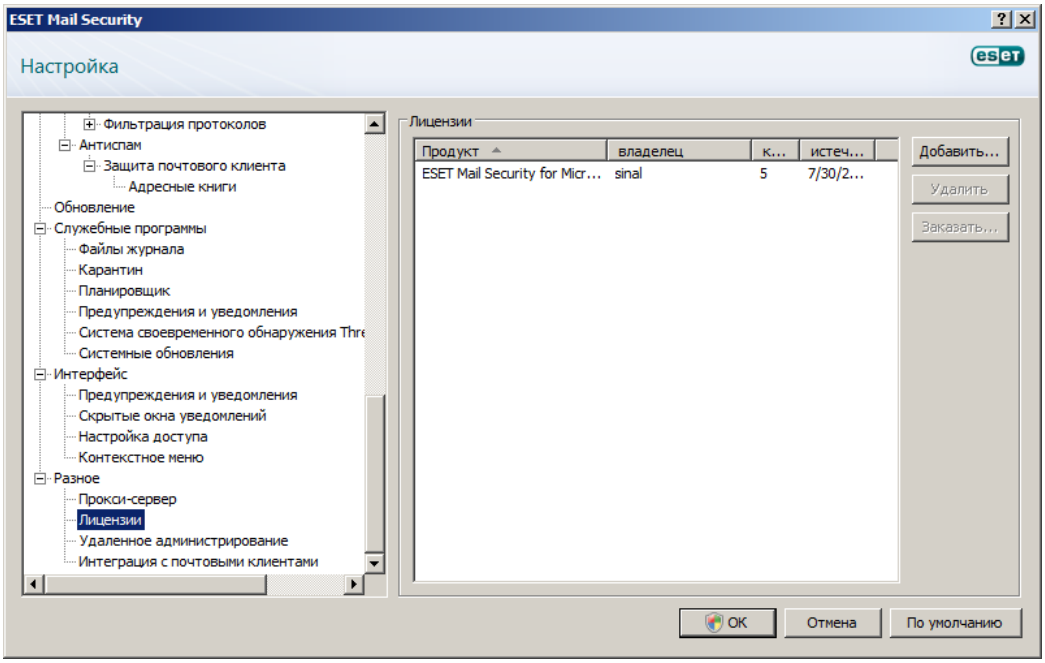
Очень важным этапом является ввод файла лицензии для ESET Mail Security для Microsoft Exchange Server. Без этого защита электронной почты на Microsoft Exchange Server будет работать некорректно. Если не добавить файл лицензии в ходе установки, это можно сделать позднее в дополнительных параметрах в разделе **Разное > Лицензии**.

ESET Mail Security позволяет использовать несколько лицензий одновременно путем их объединения, как описано далее.

1) Объединяются две или более лицензий, принадлежащих одному заказчику (т. е. лицензии, присвоенные одному и тому же имени заказчика), в результате чего соответствующим образом увеличивается количество сканируемых почтовых ящиков. В менеджере лицензий по-прежнему будут отображаться обе лицензии.

2) Объединяются две или более лицензий, принадлежащих разным заказчикам. Это происходит точно так же, как и в первом сценарии (пункт 1 выше) с тем отличием, что по меньшей мере у одной из таких лицензий должен быть особый атрибут. Этот атрибут необходим для объединения лицензий разных заказчиков. Если вам нужно использовать именно такую лицензию, обратитесь к своему местному дистрибьютору с просьбой о ее генерации.

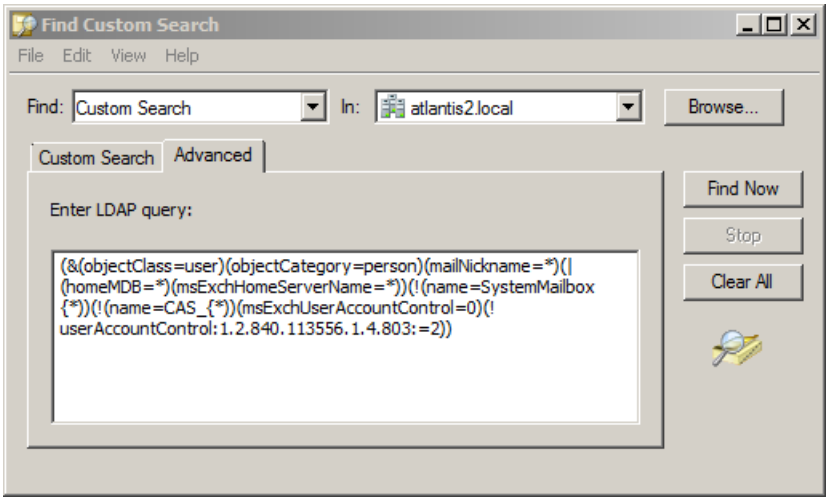
ПРИМЕЧАНИЕ. Срок действия вновь созданной лицензии определяется самой ранней из дат окончания срока действия входящих в нее лицензий.



ESET Mail Security для Microsoft Exchange Server (EMSX) сравнивает количество почтовых ящиков для службы Active Directory с имеющимся количеством лицензий. Проверяется служба Active Directory каждого сервера Exchange для определения общего количества почтовых ящиков. Системные почтовые ящики, деактивированные почтовые ящики и псевдонимы электронной почты не учитываются в общем количестве. В кластерной среде узлы с ролью почтового ящика в кластере также не учитываются в общем количестве.

Для определения имеющегося количества почтовых ящиков с поддержкой Exchange откройте на сервере **Пользователи и компьютеры Active Directory**. Щелкните домен правой кнопкой мыши и выберите **Найти...**. Затем в раскрывающемся меню **Найти** выберите пункт **Пользовательский поиск** и перейдите на вкладку **Дополнительно**. Вставьте из буфера обмена такой запрос по протоколу LDAP и нажмите кнопку **Найти сейчас**:

- `(&(objectClass=user)(objectCategory=person)(mailNickname=*)(|(homeMDB=*)(msExchHomeServerName=*))(!(name=SystemMailbox{*))(!(name=CAS_{*))(msExchUserAccountControl=0)(!userAccountControl:1.2.840.113556.1.4.803:=2))`



Если количество почтовых ящиков в службе Active Directory больше количества лицензий, в журнал Microsoft Exchange Server будет добавлено сообщение «Изменилось состояние защиты, так как превышено количество почтовых ящиков (количество), покрываемых вашей лицензией (количество)». ESET Mail Security также уведомит вас, изменив индикатор **Состояние защиты** на **ОРАНЖЕВЫЙ** и выведя на экран сообщение о том, что осталось 42 дня до отключения защиты. При получении этого уведомления обратитесь к работающему с вами агенту по продажам, чтобы приобрести дополнительные лицензии.

Если по прошествии 42 дней вы не добавили нужные лицензии на дополнительные почтовые ящики, индикатор **Состояние защиты** изменит цвет на **КРАСНЫЙ**. Вы получите сообщение об отключении защиты. При получении этого уведомления немедленно обратитесь к работающему с вами агенту по продажам, чтобы приобрести дополнительные лицензии.

2.7 Конфигурирование после установки

Существует ряд параметров, которые нужно сконфигурировать после установки программного продукта.

Настройка модуля защиты от спама

В этом разделе описываются параметры и методы, которые можно использовать для защиты сети от спама. Рекомендуется внимательно прочесть дальнейшие инструкции, прежде чем выбирать наиболее подходящее для вашей сети сочетание параметров.

Управление спамом
Для обеспечения высокого уровня защиты от спама нужно выбрать действия, которые следует применять к сообщениям, уже помеченным как спам.

Доступны три перечисленных ниже варианта.

1. **Удаление спама**

   Критерии, по которым сообщения помечаются как спам программой ESET Mail Security, установлены на достаточно высоком уровне, чтобы снизить вероятность удаления нормальных сообщений. Чем более точные параметры защиты от спама используются, тем меньше вероятность удаления нормальных сообщений. Среди преимуществ этого метода можно назвать низкое потребление системных ресурсов и меньший объем работ по администрированию. Недостаток же заключается в том, что при удалении нормального сообщения его нельзя восстановить локально.

2. **Карантин**

   Этот параметр исключает вероятность удаления нормальных сообщений. Сообщения можно восстановить и повторно направить изначальным получателям немедленно. К недостаткам же относятся более высокое потребление системных ресурсов и дополнительное время, необходимое на обслуживание карантина электронной почты. Для направления электронной почты на карантин можно использовать два метода.

   A. Внутренний карантин сервера Exchange (применяется к Microsoft Exchange Server 2007/2010)
   - Если нужно использовать внутренний карантин сервера, убедитесь в том, что поле **Обычный карантин сообщений** в правой панели меню дополнительных параметров (в разделе **Защита сервера** > **Карантин сообщений**) оставлено незаполненным. Также убедитесь в том, что в раскрывающемся меню в нижней части окна выбран вариант **Отправить сообщение в карантин системы почтового сервера**. Этот метод работает только тогда, когда существует внутренний карантин Exchange. По умолчанию этот внутренний карантин не активируется в Exchange. Если нужно активировать его, следует открыть командную консоль Exchange и ввести следующую команду:

   Set-ContentFilterConfig -QuarantineMailbox имя@домен.com

   (замените имя@домен.com на фактический почтовый ящик, который Microsoft Exchange следует использовать в качестве внутреннего почтового ящика карантина, например карантинexchange@компания.com)

   B. Пользовательский почтовый ящик карантина
   - Если ввести нужный почтовый ящик в поле **Обычный карантин сообщений**, ESET Mail Security будет перемещать все новые нежелательные сообщения в этот пользовательский почтовый ящик.

   Для получения дополнительных сведений о карантине и различных методах см. главу Карантин сообщений 26.

3. Пересылка спама

Спам будет пересылаться получателю. Однако ESET Mail Security заполнит соответствующий заголовок MIME значением вероятности нежелательной почты для каждого сообщения. На основе значения вероятности нежелательной почты интеллектуальным фильтром сообщений сервера Exchange будет выполнено соответствующее действие.

Фильтрация спама

Ядро защиты от спама
Для ядра защиты от спама существует три конфигурации: **Рекомендуемая**, **Наиболее точная** и **Самая быстрая**.
Если не нужно оптимизировать конфигурацию для обеспечения максимальной пропускной способности (например, при высокой нагрузке на сервер), рекомендуется выбрать вариант **Наиболее точная**. Если выбрана конфигурация **Рекомендуемая**, сервер автоматически настроит параметры на основе просканированных сообщений для балансировки нагрузки. Если активирован вариант **Наиболее точная**, параметры будут оптимизированы относительно ливневой скорости. Если выбрать **Выборочная** > **Открыть файл конфигурации**, можно изменить файл *spamcatcher.conf*. Этот параметр рекомендуется использовать только опытным пользователям.

Прежде чем приступать к полноценной эксплуатации, рекомендуется вручную сконфигурировать списки ограниченных и разрешенных IP-адресов. Для этого выполните следующие действия.

1) Откройте окно «Дополнительные параметры» и перейдите в раздел **Защита от спама.** Не забудьте установить флажок **Включить защиту сервера от спама**.
2) Перейдите в раздел **Ядро защиты от спама**.
3) Нажмите кнопку **Настройка...**, чтобы настроить списки **разрешенных, пропущенных** и **заблокированных IP-адресов**.
   - На вкладке **Заблокированные IP-адреса** содержится список ограниченных IP-адресов. Это значит, что в том случае, когда любой непропущенный IP-адрес из *заголовка полученного сообщения* совпадает с адресом из этого списка, сообщение получает оценку 100, а дальнейшие проверки не выполняются.
   - На вкладке **Разрешенные IP-адреса** перечисляются IP-адреса, которые являются разрешенными. Это значит, что в том случае, когда первый непропущенный IP-адрес из *заголовка полученного сообщения* совпадает с любым адресом из этого списка, сообщение получает оценку 0, а дальнейшие проверки не выполняются.
   - На вкладке **Игнорируемые IP-адреса** перечисляются адреса, которые следует пропускать *при проверках по «черным» спискам реального времени*. Этот список должен включать все внутренние IP-адреса, защищаемые файерволом, которые недоступны непосредственно через Интернет. Это позволяет избежать ненужных проверок и помогает отличить внешние выполняющие подключение IP-адреса от внутренних IP-адресов.

Работа с "серыми" списками
Работа с «серыми» списками — это метод защиты 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 неузнанного отправителя сообщение. Нормальный сервер попытается повторно доставить сообщение. Как правило, отправители спама не пытаются повторно доставить сообщения, так как они обычно обрабатывают тысячи адресов электронной почты одновременно и не могут тратить дополнительное время на повторную отправку.

При оценке источника сообщения этим методом учитываются конфигурации списков **Разрешенные IP-адреса**, **Игнорируемые IP-адреса**, **Надежные отправители** и **Разрешить IP** на сервере Exchange и параметры AntispamBypass для почтового ящика получателя. Работу с «серыми» списками следует тщательно сконфигурировать, потому что в противном случае возможны нежелательные сбои в работе (например, задержки доставки нормальных сообщений). Количество этих отрицательных последствий постепенно уменьшается, так как этот метод наполняет внутренний «белый» список доверенными соединениями. Если этот метод вам незнаком или вы считаете его отрицательные побочные эффекты неприемлемыми, рекомендуется отключить его в меню дополнительных параметров в разделе **Защита от спама** > **Microsoft Exchange Server** > **Транспортный агент** > **Включить работу с "серыми" списками**.

Рекомендуется отключить работу с «серыми» списками, если вы планируете протестировать основные функции программы, но не хотите конфигурировать ее расширенные функции.

ПРИМЕЧАНИЕ: Работа с «серыми» списками — это дополнительная мера защиты от спама, которая не влияет на возможности модуля защиты от спама по оценке спама.

Настройка защиты от вирусов

Карантин
В зависимости от типа используемого режима очистки рекомендуется сконфигурировать действие, которое следует применять к зараженным (неочищенным) сообщениям. Этот параметр можно настроить в окне «Дополнительные настройки» в разделе **Защита сервера** > **Защита от вирусов и шпионских программ** > **Microsoft Exchange Server** > **Транспортный агент**.
Если активирован параметр, задающий перемещение сообщений в карантин электронной почты, нужно сконфигурировать карантин в окне «Дополнительные настройки» в разделе **Защита сервера** > **Карантин сообщений**.

Производительность
Если нет никаких других ограничений, рекомендуется увеличить количество модулей сканирования ThreatSense в окне «Дополнительные настройки» (F5) в разделе **Защита сервера** > **Защита от вирусов и шпионских программ** > **Microsoft Exchange Server** > **VSAPI** > **Производительность**, воспользовавшись для этого такой формулой: *количество потоков сканирования = (количество физических ЦП x 2) + 1*. Также *количество потоков сканирования* должно быть равно *количеству модулей сканирования ThreatSense.* Сконфигурировать количество модулей сканирования можно в разделе **Защита компьютера** > **Защита от вирусов и шпионских программ** > **Производительность**. Ниже приведен пример.

Допустим, у вас есть сервер с 4 физическими ЦП. Для достижения наилучшей производительности по формуле выше у вас должно быть 9 потоков сканирования и 9 модулей сканирования.

ПРИМЕЧАНИЕ. Рекомендуется задавать количество модулей сканирования ThreatSense равным количеству используемых потоков сканирования. Использование большего количества потоков сканирования, чем модулей сканирования, не повлияет на производительность.

ПРИМЕЧАНИЕ. Если программное обеспечение ESET Mail Security используется на сервере Windows Server, который выступает в качестве сервера терминалов, и не нужно запускать графический интерфейс пользователя ESET Mail Security при каждом входе пользователя в систему, ознакомьтесь с конкретными инструкциями по его отключению в главе Отключение графического интерфейса пользователя на сервере терминалов 106.

3. ESET Mail Security — защита Microsoft Exchange Server

ESET Mail Security обеспечивает значительный уровень защиты сервера Microsoft Exchange Server. Существует три основных типа защиты: защита от вирусов, защита от спама и применение пользовательских правил. ESET Mail Security защищает от различных типов вредоносного содержимого, в том числе вложений в сообщения электронной почты, зараженных червями или троянскими программами, документов, в которых содержатся вредоносные сценарии, фишинга и спама. ESET Mail Security фильтрует вредоносное содержимое на уровне почтового сервера, прежде чем оно попадет в папку «Входящие» почтового клиента получателя. В следующих главах описываются все параметры, доступные для подробной настройки защиты Microsoft Exchange Server.

3.1 Общие настройки

В этом разделе описывается администрирование правил, файлов журнала, карантина сообщений и параметров производительности.

3.1.1 Microsoft Exchange Server

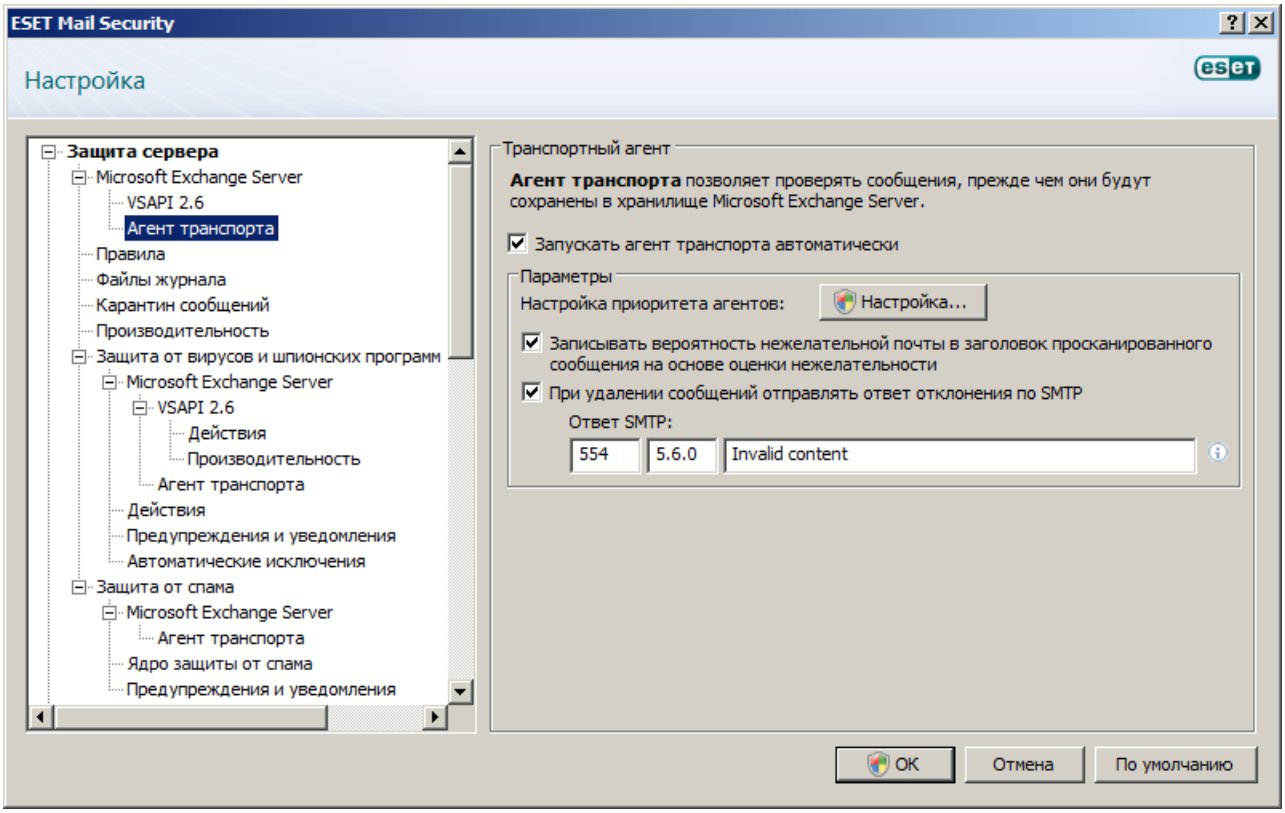
3.1.1.1 VSAPI (API поиска вирусов)

В Microsoft Exchange Server есть механизм, который обеспечивает сканирование каждого компонента сообщения с использованием текущей базы данных сигнатур вирусов. Если компонент сообщения не сканировался, соответствующий компонент отправляется в модуль сканирования, прежде чем сообщение будет передано клиенту. В каждой поддерживаемой версии Microsoft Exchange Server (5.5/2000/2003/2007/2010) предлагаются разные версии VSAPI.

Используйте флажок для включения и отключения автоматического запуска версии VSAPI, используемой вашим сервером Exchange.

3.1.1.2 Транспортный агент

В этом разделе можно сконфигурировать агент транспорта на автоматический запуск и задать приоритет загрузки агентов. В Microsoft Exchange Server 2007 и более поздних версиях можно установить агент транспорта только в том случае, если сервер имеет одну из двух ролей: *пограничный транспортный сервер* или *транспортный сервер-концентратор*.



ПРИМЕЧАНИЕ. Агент транспорта недоступен в Microsoft Exchange Server 5.5 (VSAPI 1.0).

В меню **Настройка приоритета агентов** можно задать приоритет агентов ESET Mail Security. Диапазон числовых значений приоритета агентов зависит от версии Microsoft Exchange Server (чем меньше число, тем выше приоритет).

Записывать вероятность нежелательной почты в заголовок просканированного сообщения на основе оценки нежелательности: вероятность нежелательной почты — это нормализованное значение, присваиваемое сообщению, которое показывает вероятность того, что данное сообщение является спамом (вычисляется на основе характеристик заголовка сообщения, его темы, содержимого и т. д.). Рейтинг 0 показывает, что сообщение крайне маловероятно является спамом, тогда как значение 9 — что сообщение с очень высокой вероятностью является спамом. Значения вероятности нежелательной почты могут далее обрабатываться интеллектуальным фильтром сообщений Microsoft Exchange Server (или агентом фильтрации содержимого). Для получения дополнительных сведений обратитесь к документации на Microsoft Exchange Server.

Параметр **При удалении сообщений отправлять ответ отклонения по SMTP**

- Если этот флажок снят, сервер отправляет ответ «OK» по протоколу SMTP агенту передачи почты отправителя в формате «250 2.5.0 - Requested mail action okay, completed», а затем выполняет необъявленную потерю.

- Если же флажок установлен, по SMTP отправляется ответ отклонения агенту передачи почты отправителя. Можно ввести ответное сообщение в следующем формате.

Основной код ответа	Дополнительный код состояния	Описание
250	2.5.0	Requested mail action okay, completed (Запрошенное действие с почтой в порядке, завершено)
451	4.5.1	Requested action aborted: (Запрошенное действие прервано:) local error in processing (локальная ошибка при обработке)
550	5.5.0	Requested action not taken: (Запрошенное действие не выполнено:) mailbox unavailable (почтовый ящик недоступен)

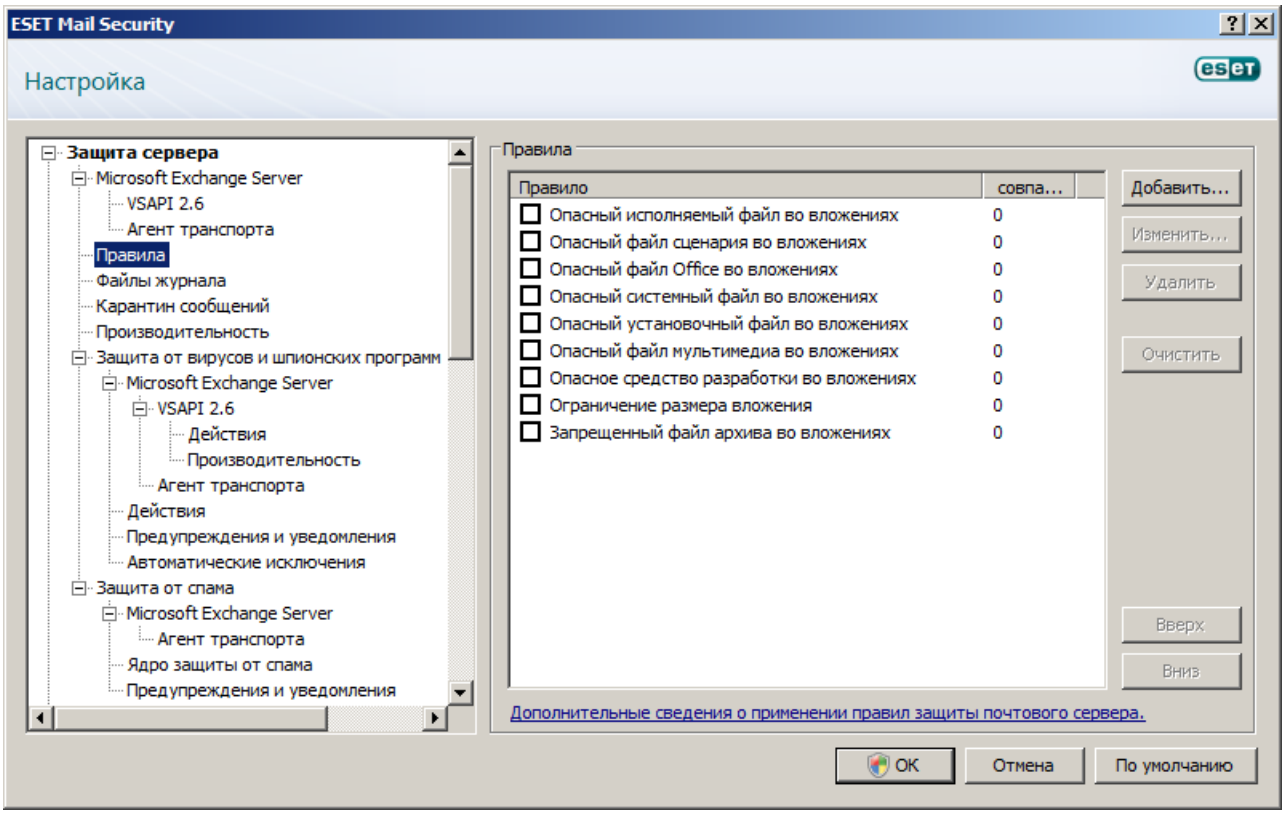
Внимание: Неверный синтаксис кодов ответа по SMTP может привести к некорректной работе компонентов программы и снизить ее эффективность.

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

3.1.2 Правила

Пункт меню **Правила** позволяет администраторам вручную задавать условия фильтрации электронной почты и действия, которые необходимо выполнить с отфильтрованными сообщениями. Правила применяются в соответствии с набором совместно используемых условий. Несколько условий объединяются логическим оператором AND, то есть правило применяется только в случае, если все условия выполнены. В столбце **Номер** (рядом с именем каждого правила) отображается количество случаев успешного применения данного правила.

Правила проверяются для сообщения во время его обработки агентом транспорта или 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 каждой части сообщения по отдельности (тело, вложение), то есть правила последовательно применяются к каждой из таких частей. Правила также применяются во время фонового сканирования (например, повторное сканирование хранилища почтового ящика после обновления базы данных сигнатур вирусов), что также может увеличивать значение счетчика.



- **Добавить...**: добавление нового правила.
- **Изменить...**: изменение существующего правила.
- **Удалить**: удаление выделенного правила.
- **Очистить**: сброс счетчика правила (столбец **Номер**).
- **Вверх**: перемещение выделенного правила вверх по списку.
- **Вниз**: перемещение выделенного правила вниз по списку.

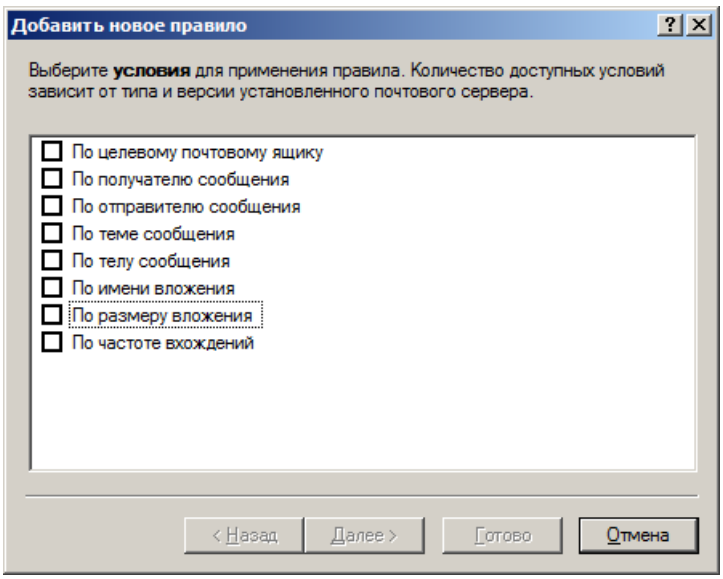
Снятие флажка (слева от имени каждого правила) отключает текущее правило Это позволяет повторно активировать правило в случае необходимости.

ПРИМЕЧАНИЕ: Можно также использовать системные переменные (например, *%PATHEXT%*) при настройке правил.

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

3.1.2.1 Добавление нового правила

Этот мастер помогает добавить пользовательские правила с сочетанием различных условий.



ПРИМЕЧАНИЕ: Не все условия применяются, когда сообщение сканируется агентом транспорта.

- **По целевому почтовому ящику**: условие применяется к имени почтового ящика (VSAPI).
- **По получателю сообщения**: условие применяется к сообщению, отправленному указанному получателю (VSAPI + агент транспорта)
- **По отправителю сообщения**: условие применяется к сообщению от указанного отправителя (VSAPI + агент транспорта)
- **По теме сообщения**: условие применяется к сообщению с определенной темой (VSAPI + агент транспорта)
- **По телу сообщения**: условие применяется к сообщению, в теле которого есть указанный текст (VSAPI)
- **По имени вложения**: условие применяется к сообщению с указанным именем вложения (VSAPI)
- **По размеру вложения**: условие применяется к сообщению, размер вложения которого превышает указанный (VSAPI)
- **По частоте вхождений**: условие применяется к объектам (тело сообщения электронной почты и вложения), для которых количество вхождений в течение указанного периода времени превышает заданное число (VSAPI + агент транспорта). Это особенно удобно, если вы постоянно получаете нежелательные сообщения, имеющие одинаковое тело сообщения или одно и то же вложение.

При указании перечисленных выше условий (за исключением **По размеру вложения**) достаточно указать фразу лишь частично, если не установлен флажок **Только слова целиком**. В значениях не учитывается регистр при условии, что не установлен флажок **С учетом регистра**. Если в значениях есть символы, отличные от буквенно-цифровых знаков, используйте круглые скобки и кавычки. Также можно создавать условия при помощи логических операторов AND, OR и NOT.

ПРИМЕЧАНИЕ. Набор доступных правил зависит от установленной версии Microsoft Exchange Server.

ПРИМЕЧАНИЕ. Microsoft Exchange Server 2000 (VSAPI 2.0) оценивает только отображаемые имена отправителя и получателя, но не адрес электронной почты. Адреса электронной почты оцениваются, начиная с Microsoft Exchange Server 2003 (VSAPI 2.5).

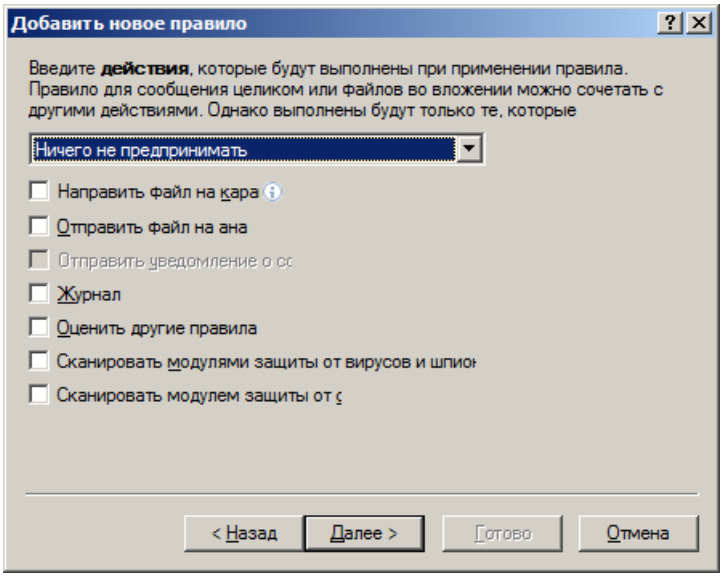
Примеры ввода условий

По целевому почтовому ящику	smith
По отправителю сообщения:	smith@mail.com
По получателю сообщения:	"J.Smith" or "smith@mail.com"
По теме сообщения:	" "
По имени вложения:	".com" OR ".exe"

По телу сообщения: ("бесплатно" OR "лотерея") AND ("выигрыш" OR "купить")

3.1.2.2 Действия, выполняемые при применении правил

В этом разделе можно выбрать действия, которые следует выполнять с сообщениями и/или вложениями, соответствующими условиям, определенным в правилах. Можно ничего не предпринимать, пометить сообщение как содержащее угрозу или спам или удалить его целиком. Когда сообщение или его вложения соответствуют условиям правила, по умолчанию оно не сканируется модулями защиты от вирусов и от спама, если сканирование не активировано принудительно путем установки соответствующих флажков в нижней части окна (выполняемое действие в таком случае зависит от параметров модулей защиты от вирусов и от спама).



- **Ничего не предпринимать**: никакие действия в отношении сообщения не выполняются.
- **Предпринять действие для неочищенной угрозы**: сообщение будет помечено как содержащее неочищенную угрозу (независимо от того, содержало ли оно действительно угрозу).
- **Предпринять действие для нежелательной почты**: сообщение будет помечено как спам (независимо от того, является ли оно спамом). Этот параметр недоступен, если используется ESET Mail Security без модуля защиты от спама.
- **Удалить сообщение**: удаляется целиком сообщение вместе с содержанием, которое соответствует условиям.

- **Направить файл на карантин**: вложения направляются на карантин.

ПРИМЕЧАНИЕ. Не следует путать эту функцию с карантином почты (см. главу Карантин сообщений 26)

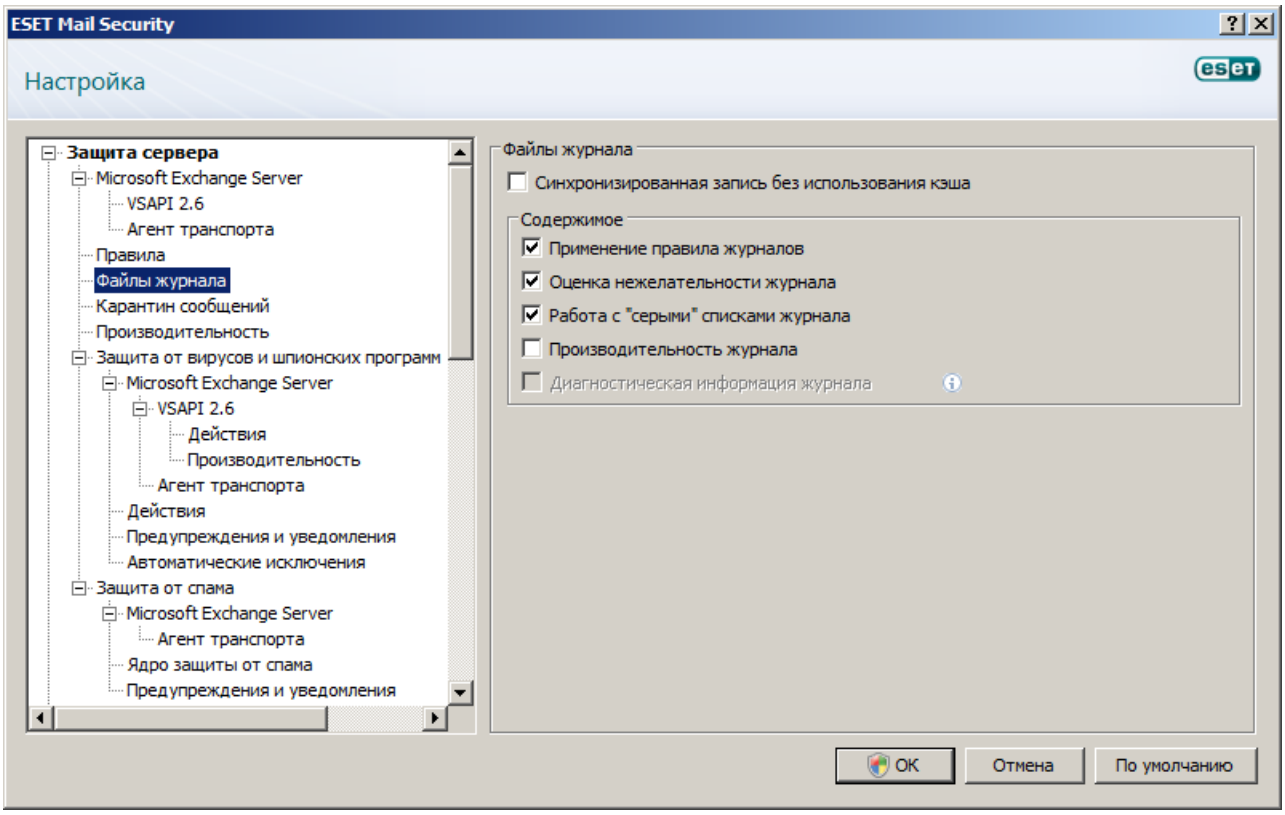
- **Отправить файл на анализ**: подозрительные вложения отправляются в лабораторию ESET на анализ.
- **Отправить уведомление о событии**: администратору отправляется уведомление (в зависимости от параметров, выбранных в разделе **Служебные программы > Предупреждения и уведомления**).
- **Журнал**: информация о применяемом правиле регистрируется в журнале программы.
- **Оценить другие правила**: позволяет оценить также и другие правила, что дает пользователю возможность задать несколько наборов условий и разные применяемые действия в зависимости от условий.
- **Сканировать модулями защиты от вирусов и шпионских программ**: сообщение и его вложения сканируются на наличие угроз.
- **Сканировать модулем защиты от спама**: сообщение сканируется на наличие спама.

ПРИМЕЧАНИЕ. Данная функция доступна только для Microsoft Exchange Server 2000 и более поздних версий с включенным агентом транспорта.

Последним этапом мастера создания нового правила является присвоение имени каждому созданному правилу. Также можно добавить **Комментарий правила**. Эта информация будет сохранена в журнале Microsoft Exchange Server.

3.1.3 Файлы журнала

Параметры файлов журнала позволяют выбрать, как будет формироваться файл журнала. В более подробном протоколе может быть представлено больше информации, но при этом он может снижать производительность сервера.



Если установлен флажок **Синхронизированная запись без использования кэша**, все записи журнала немедленно будут записываться в файл журнала без хранения в кэше журнала. По умолчанию компоненты ESET Mail Security, работающие на сервере Microsoft Exchange Server, хранят сообщения журнала в собственном внутреннем кэше и отправляют их в журнал приложения через определенные промежутки времени для снижения влияния на производительность. Однако в этом случае диагностические записи в журнале могут быть расположены не по порядку. Рекомендуется оставить этот параметр выключенным, если нет особой необходимости включить его для диагностики. Можно указать тип информации, хранящейся в файлах журнала, в меню **Содержимое**.

- **Применение правила журналов**: если этот параметр активирован, ESET Mail Security записывает имена всех активированных правил в файл журнала.

- **Оценка нежелательности журнала**: используйте этот вариант, чтобы связанная со спамом активность записывалась в журнал защиты от спама 84. Когда почтовый сервер получает нежелательное сообщение, информация об этом записывается в журнал с указанием таких сведений, как время/дата, отправитель, получатель, тема, оценка нежелательности, причина и действие. Это полезно, когда нужно проследить, какие нежелательные сообщения были получены, когда и какие действия были применены.

- **Работа с "серыми" списками журнала**: активируйте этот параметр, если следует записывать активность, связанную с работой с «серыми» списками, в журнал работы с «серыми» списками 84. В нем указывается такая информация, как время/дата, домен HELO, IP-адрес, отправитель, получатель, действие и т. д. **ПРИМЕЧАНИЕ**: Этот параметр работает только в том случае, если работа с «серыми» списками активирована в параметрах агента транспорта 39 в разделе **Защита сервера** > **Защита от спама** > **Microsoft Exchange Server** > **Транспортный агент** дерева расширенных параметров (F5).

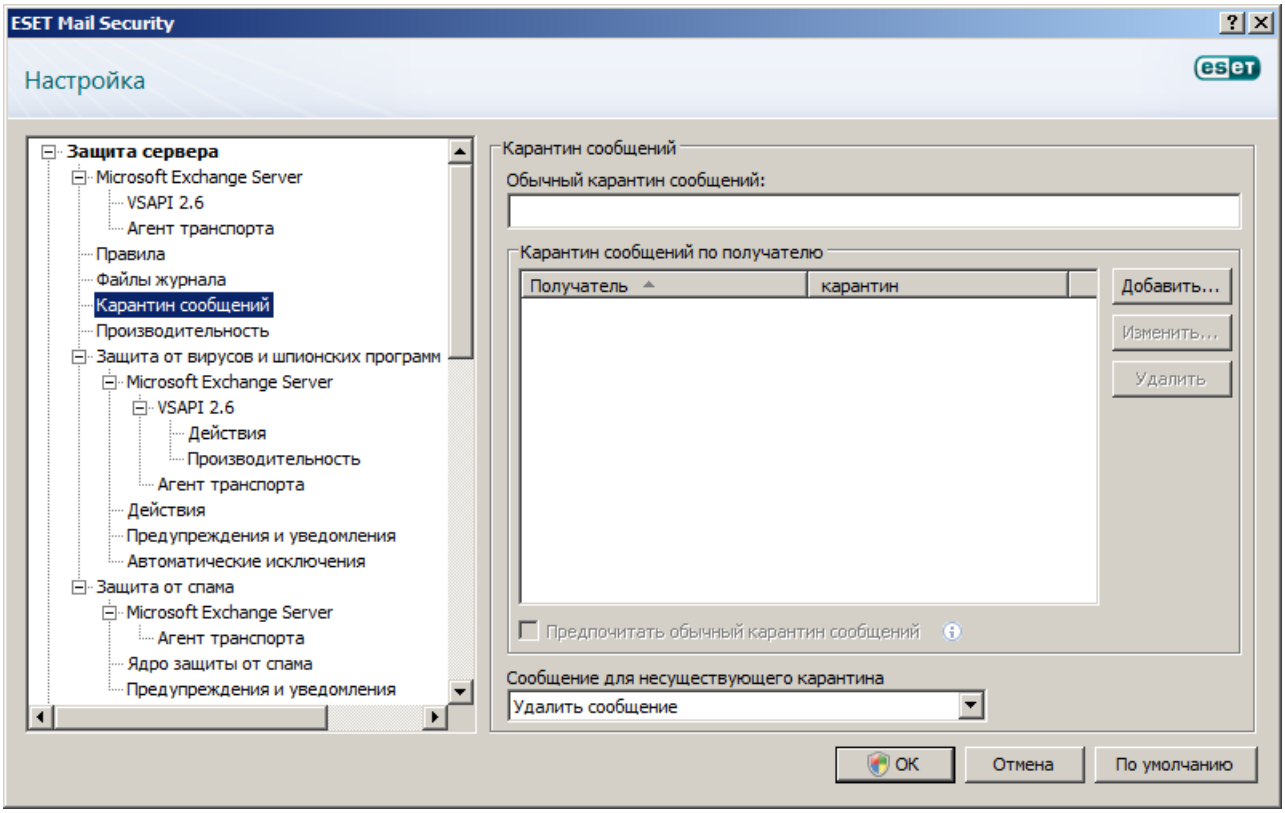
- **Производительность журнала**: регистрируется информация о периоде времени выполненной задачи, размере просканированного объекта, скорости передачи (КБ/с) и оценке производительности.

- **Диагностическая информация журнала**: регистрируется диагностическая информация, необходимая для точной настройки программы в соответствии с протоколом; этот параметр предназначен

преимущественно для отладки и выявления проблем. Не рекомендуется активировать этот параметр. Для просмотра диагностической информации, формируемой этой функцией, нужно выбрать для параметра «Минимальная степень детализации журнала» значение **Диагностические записи** в разделе **Служебные программы** > **Файлы журнала** > **Минимальная степень детализации журнала**.

3.1.4 Карантин сообщений

Карантин сообщений — это особый почтовый ящик, задаваемый системным администратором для хранения потенциально зараженных сообщений и спама. Сообщения, хранящиеся на карантине, могут быть проанализированы или очищены позднее при помощи более новой базы данных сигнатур вирусов.



Существует два типа систем карантина сообщений, которые можно использовать.

Первый вариант заключается в использовании системы карантина Microsoft Exchange (применяется только для Microsoft Exchange Server 2007/2010). В этом случае внутренний механизм Exchange используется для хранения потенциально зараженных сообщений и спама. Кроме того, можно добавить отдельный почтовый ящик карантина (или несколько почтовых ящиков) для конкретных получателей, если это необходимо. Это значит, что потенциально зараженные сообщения, которые изначально были отправлены определенному получателю, будут доставлены в отдельный почтовый ящик карантина, а не во внутренний почтовый ящик карантина Exchange. Это может быть полезно в некоторых ситуациях, чтобы упорядочивать зараженные сообщения и спам.

Другим вариантом, который можно использовать, является **Обычный карантин сообщений**. Если используется более ранняя версия Microsoft Exchange Server (5.5, 2000 или 2003), то просто указывается **Обычный карантин сообщений**, который представляет собой почтовый ящик, предназначенный для хранения потенциально зараженных сообщений. В этом случае не используется внутренняя система карантина Exchange. Вместо этого используется почтовый ящик, указанный системным администратором. Как и в первом случае, можно добавить отдельный почтовый ящик карантина (или несколько почтовых ящиков) для конкретных получателей. В результате потенциально зараженные сообщения доставляются в отдельный почтовый ящик, а не в обычный карантин сообщений.

- **Обычный карантин сообщений**: здесь можно указать адрес обычного карантина сообщений (например, основной_карантин@компания.com) или задать использование внутренней системы карантина Microsoft Exchange Server 2007/2010, оставив это поле пустым и выбрав пункт **Отправить сообщение в карантин системы почтового сервера** (при условии, что карантин Exchange существует в вашей среде) в раскрывающемся меню в нижней части окна. В этом случае сообщения электронной почты доставляются в карантин с применением внутреннего механизма Exchange и его собственных параметров.
  ПРИМЕЧАНИЕ: По умолчанию этот внутренний карантин не активируется в Exchange. Если нужно активировать его, следует открыть командную консоль Exchange и ввести следующую команду:

  Set-ContentFilterConfig -QuarantineMailbox имя@домен.com

  (замените имя@домен.com на фактический почтовый ящик, который Microsoft Exchange следует использовать в качестве внутреннего почтового ящика карантина, например карантинexchange@компания.com)

- **Карантин сообщений по получателю**: применение этого параметра позволяет задать почтовые ящики карантина сообщений для нескольких получателей. Каждое правило карантина можно включить и отключить, установив или сняв флажок в его строке.

  Добавить...: можно добавить новое правило карантина, указав адрес электронной почты нужного получателя и адрес электронной почты карантина, куда будет направлено сообщение.
  Изменить...: изменение выделенного правила карантина.
  Удалить: удаление выделенного правила карантина.

  Предпочитать обычный карантин сообщений: если данный параметр активирован, сообщение будет доставлено в указанный обычный карантин, если выполняется более одного правила карантина (например, если сообщение имеет несколько получателей, причем некоторые из них указаны в нескольких правилах карантина).

- **Сообщение для несуществующего карантина сообщений** (если не задан обычный карантин сообщений, существуют описанные далее варианты действий, которые будут применяться к потенциально зараженным сообщениям и спаму)

  Ничего не предпринимать: сообщение будет обработано стандартным образом, то есть доставлено получателю (не рекомендуется)
  Удалить сообщение: сообщение будет удалено, если оно предназначено получателю, для которого не существует правило карантина, а обычный карантин сообщений не задан; это означает, что все потенциально зараженные сообщения и спам будут автоматически удаляться без хранения где-либо.
  Отправить сообщение в карантин системы почтового сервера: сообщение будет доставлено и сохранено во внутреннем карантине системы Exchange (недоступно для Microsoft Exchange Server 2003 и более ранних версий)

ПРИМЕЧАНИЕ. Можно также использовать системные переменные (например, *%USERNAME%*) при настройке параметров карантина сообщений.

3.1.4.1 Добавление нового правила карантина

Введите нужный адрес электронной почты получателя и адрес электронной почты карантина в соответствующие поля.

Если нужно удалить сообщение электронной почты, предназначенное получателю, для которого не применяется правило карантина, можно выбрать вариант **Удалить сообщение** в раскрывающемся меню **Сообщение для несуществующего карантина сообщений**.

3.1.5 Производительность

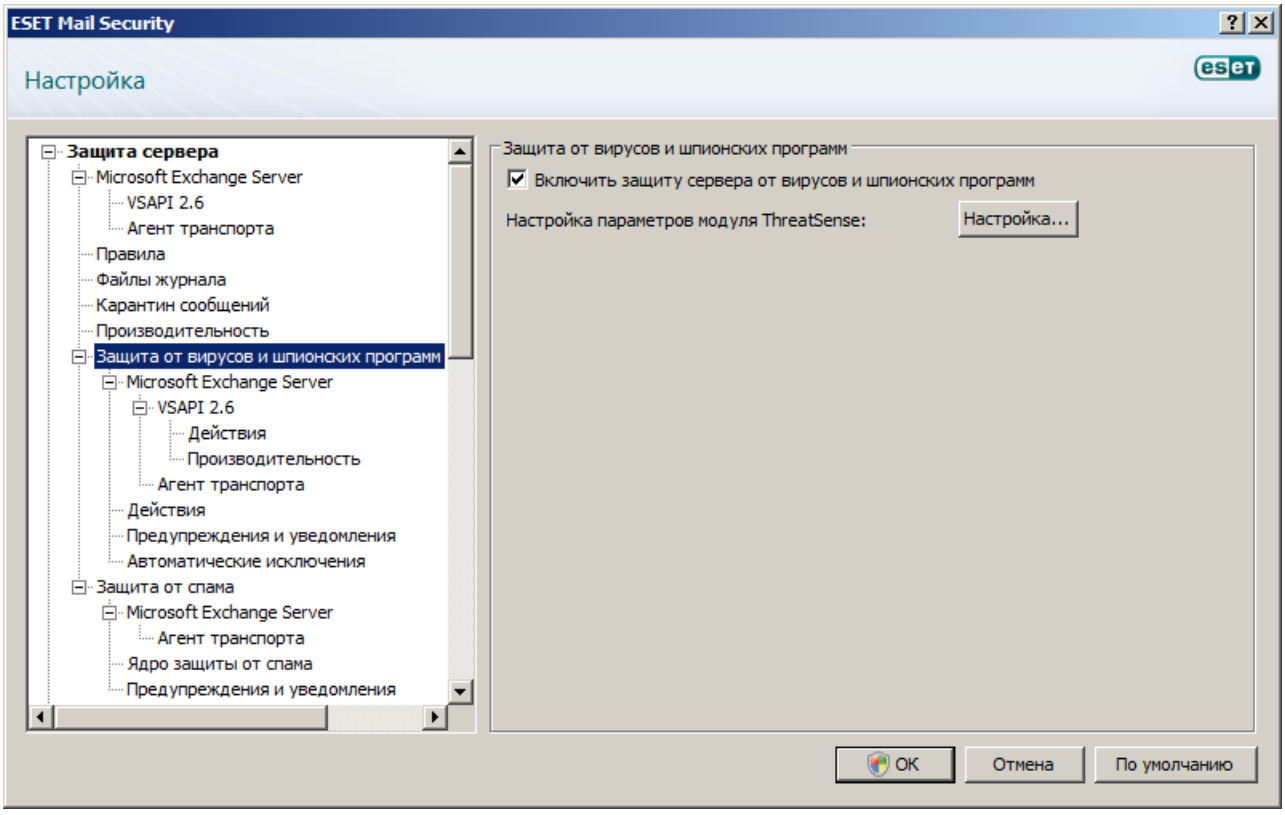
В этом разделе можно выбрать папку для хранения временных файлов для улучшения производительности программы. Если папка не указана, ESET Mail Security будет создавать временные файлы во временной папке системы.

ПРИМЕЧАНИЕ. Для сокращения возможного влияния операций ввода-вывода и фрагментации рекомендуется разместить временную папку не на том жестком диске, на котором установлен сервер Microsoft Exchange Server. Настоятельно не рекомендуется выбирать временную папку на съемных носителях, таких как гибкие диски, USB-устройства, DVD-диски и т. п.

ПРИМЕЧАНИЕ. Можно использовать системные переменные (например, *%SystemRoot%\TEMP*) при настройке параметров производительности.

3.2 Параметры защиты от вирусов и шпионских программ

Можно включить защиту почтового сервера от вирусов и шпионских программ, установив флажок **Включить защиту сервера от вирусов и шпионских программ**. Имейте в виду, что защита от вирусов и шпионских программ включается автоматически после каждого перезапуска службы или компьютера. Настроить параметры модуля ThreatSense можно, нажав кнопку **Настройка...**.



3.2.1 Microsoft Exchange Server

Когда речь идет о защите от вирусов и шпионских программ, ESET Mail Security для Microsoft Exchange Server применяет два типа сканирования. Первый тип сканирует сообщения через VSAPI, тогда как второй использует агент транспорта.

- В рамках защиты с применением VSAPI 29 сообщения сканируются непосредственно в хранилище сервера Exchange.

- Защитой агентом транспорта 35 сканируется трафик протокола SMTP вместо собственно хранилища сервера Exchange. Если этот тип защиты включен, это значит, что все сообщения и их компоненты сканируются при транспортировке, еще до того, как они попадают в хранилище сервера Exchange или отправляются по протоколу SMTP. 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» Microsoft Exchange Server.

ПРИМЕЧАНИЕ: Агент транспорта недоступен в Microsoft Exchange Server 5.5, но доступен во всех более новых версиях Microsoft Exchange Server (начиная с версии 2000).

Защита от вирусов и шпионских программ с помощью VSAPI и агента транспорта могут работать одновременно (это используемая по умолчанию рекомендуемая конфигурация). Или же можно выбрать использовать только один тип защиты (либо VSAPI, либо агент транспорта). Они могут включаться и отключаться независимо друг от друга. Рекомендуется использовать оба типа для обеспечения максимально качественной защиты от вирусов и шпионских программ. Не рекомендуется отключать оба типа.

3.2.1.1 API поиска вирусов (VSAPI)

В Microsoft Exchange Server есть механизм, который обеспечивает сканирование каждого компонента сообщения с использованием текущей базы данных сигнатур вирусов. Если сообщение не сканировалось ранее, соответствующие его компоненты отправляются в модуль сканирования, прежде чем сообщение будет передано клиенту. В каждой поддерживаемой версии Microsoft Exchange Server (5.5/2000/2003/2007/2010) предлагаются разные версии VSAPI.

3.2.1.1.1 Microsoft Exchange Server 5.5 (VSAPI 1.0)

В состав этой версии Microsoft Exchange Server входит VSAPI версии 1.0.

Если активирован параметр **Фоновое сканирование**, можно сканировать все сообщения в фоновом режиме системы. 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.

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 задачи она появляется в списке запланированных и, как и с другими задачами, можно изменить ее параметры, удалить ее или временно отключить.

3.2.1.1.1.1 Действия

В этом разделе можно задать действия, которые следует выполнять, если сообщение и/или вложение оценивается как зараженное.

В поле **Действие, если очистка невозможна** можно выбрать один из вариантов: **Блокировать** зараженное содержимое, **Удалить** сообщение или **Ничего не предпринимать** к зараженному содержимому сообщения. Это действие будет применено, только если в результате автоматической очистки (задается в разделе **Настройка параметров модуля ThreatSense** > Очистка 67) не удалось очистить сообщение.

В поле **Удаление** можно задать **метод удаления вложения**, выбрав один из перечисленных далее вариантов.

- **Усечь файл до нулевой длины**: ESET Mail Security урезает вложение до нулевого размера и позволяет получателю видеть имя файла и тип вложения.
- **Заменить вложение информацией действия**: ESET Mail Security заменяет зараженный файл на протокол вируса или описание правила.

Если нажать кнопку **Повторное сканирование**, то можно выполнить еще одно сканирование сообщений и файлов, которые уже были просканированы ранее.

3.2.1.1.1.2 Производительность

При сканировании Microsoft Exchange Server позволяет ограничить время на открытие вложений в сообщения. Это время задается в поле **Предельное время ответа (мс)** и представляет собой период, по окончании которого клиент повторит попытку доступа к файлу, который ранее был недоступен из-за сканирования.

3.2.1.1.2 Microsoft Exchange Server 2000 (VSAPI 2.0)

В состав этой версии Microsoft Exchange Server входит VSAPI версии 2.0.

Если снять флажок **Включить защиту от вирусов и шпионских программ VSAPI 2.0**, 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 39, а также будут применяться правила 22.

Если активирован параметр **Упреждающее 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 сканироваться до остальных ожидающих сообщений.

Параметр **Фоновое сканирование** позволяет сканировать все сообщения в фоновом режиме системы. 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.

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 задачи она появляется в списке запланированных и, как и с другими задачами, можно изменить ее параметры, удалить ее или временно отключить.

Если нужно сканировать сообщения в формате обычного текста, установите флажок **Сканировать тело сообщений в формате обычного текста**.

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

3.2.1.1.2.1 Действия

В этом разделе можно задать действия, которые следует выполнять, если сообщение и/или вложение оценивается как зараженное.

В поле **Действие, если очистка невозможна** можно выбрать один из вариантов: **Блокировать** зараженное содержимое, **Удалить** сообщение или **Ничего не предпринимать** к зараженному содержимому сообщения. Это действие будет применено, только если в результате автоматической очистки (задается в разделе **Настройка параметров модуля ThreatSense >** Очистка 67) не удалось очистить сообщение.

Параметр **Удаление** позволяет задать **метод удаления сообщения** и **метод удаления вложения**.

В качестве значений параметра **Метод удаления сообщения** можно выбрать один из следующих вариантов.

- **Удалить тело сообщения**: удаляется тело зараженного сообщения; получателю будут доставлены пустое сообщение и все незараженные вложения.
- **Заменить тело сообщения информацией действия**: тело зараженного сообщения заменяется информацией о выполненных действиях.

В качестве значений параметра **Метод удаления вложения** можно выбрать один из следующих вариантов.

- **Усечь файл до нулевой длины**: ESET Mail Security урезает вложение до нулевого размера и позволяет получателю видеть имя файла и тип вложения.
- **Заменить вложение информацией действия**: ESET Mail Security заменяет зараженный файл на протокол вируса или описание правила.

Если нажать кнопку **Повторное сканирование**, то можно выполнить еще одно сканирование сообщений и файлов, которые уже были просканированы ранее.

3.2.1.1.2.2 Производительность

В этом разделе можно задать количество независимых потоков сканирования, используемых одновременно. Большее количество потоков на многопроцессорных компьютерах может увеличить скорость сканирования. Для обеспечения максимальной производительности программы рекомендуется использовать одинаковое количество модулей сканирования ThreatSense и потоков сканирования.

В поле **Предельное время ответа (с)** можно задать максимальное время, в течение которого поток ждет завершения сканирования сообщения. Если в течение этого времени сканирование не завершается, Microsoft Exchange Server запретит клиенту доступ к электронной почте. Сканирование не будет прервано, а по его окончании все остальные попытки получить доступ к файлу будут успешны.

СОВЕТ: Для определения **количества потоков сканирования**, рекомендуемых поставщиком Microsoft Exchange Server, нужно использовать формулу: [количество физических процессоров] x 2 + 1.

ПРИМЕЧАНИЕ: Производительность не увеличивается существенно, если количество модулей сканирования ThreatSense больше потоков сканирования.

3.2.1.1.3 Microsoft Exchange Server 2003 (VSAPI 2.5)

В состав этой версии Microsoft Exchange Server входит VSAPI версии 2.5.

Если снять флажок **Включить защиту от вирусов и шпионских программ VSAPI 2.5**, 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 39, а также будут применяться правила 22.

Если активирован параметр **Упреждающее 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 сканироваться до остальных ожидающих сообщений.

Параметр **Фоновое сканирование** позволяет сканировать все сообщения в фоновом режиме системы. 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.

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 задачи она появляется в списке запланированных и, как и с другими задачами, можно изменить ее параметры, удалить ее или временно отключить.

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

Параметр **Сканировать переносимые сообщения** активирует сканирование сообщений, которые не хранятся на локальном сервере Microsoft Exchange Server и доставляются на другие серверы электронной почты через локальный сервер Microsoft Exchange Server. Сервер Microsoft Exchange Server можно сконфигурировать в качестве шлюза, который затем передает сообщения на другие серверы электронной почты. Если активировано сканирование переносимых сообщений, ESET Mail Security также сканирует эти сообщения. Этот параметр доступен только тогда, когда отключен агент транспорта.

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

3.2.1.1.3.1 Действия

В этом разделе можно задать действия, которые следует выполнять, если сообщение и/или вложение оценивается как зараженное.

В поле **Действие, если очистка невозможна** можно выбрать один из вариантов: **Блокировать** зараженное содержимое, **Удалить** зараженное содержимое сообщения, **Удалить сообщение целиком** или **Ничего не предпринимать**. Это действие будет применено, только если в результате автоматической очистки (задается в разделе **Настройка параметров модуля ThreatSense >** Очистка 67) не удалось очистить сообщение.

Параметр **Удаление** позволяет задать **метод удаления сообщения** и **метод удаления вложения**.

В качестве значений параметра **Метод удаления сообщения** можно выбрать один из следующих вариантов.

- **Удалить тело сообщения**: удаляется тело зараженного сообщения; получателю будут доставлены пустое сообщение и все незараженные вложения.
- **Заменить тело сообщения информацией действия**: тело зараженного сообщения заменяется информацией о выполненных действиях.
- **Удалить сообщение целиком**: удаляется сообщение целиком вместе с вложениями; можно также выбрать, какое действие следует предпринять при удалении вложений.

В качестве значений параметра **Метод удаления вложения** можно выбрать один из следующих вариантов.

- **Усечь файл до нулевой длины**: ESET Mail Security урезает вложение до нулевого размера и позволяет получателю видеть имя файла и тип вложения.
- **Заменить вложение информацией действия**: ESET Mail Security заменяет зараженный файл на протокол вируса или описание правила.
- **Удалить сообщение целиком**: удаляется сообщение целиком вместе с вложениями; можно также выбрать, какое действие следует предпринять при удалении вложений.

Если нажать кнопку **Повторное сканирование**, то можно выполнить еще одно сканирование сообщений и файлов, которые уже были просканированы ранее.

3.2.1.1.3.2 Производительность

В этом разделе можно задать количество независимых потоков сканирования, используемых одновременно. Большее количество потоков на многопроцессорных компьютерах может увеличить скорость сканирования. Для обеспечения максимальной производительности программы рекомендуется использовать одинаковое количество модулей сканирования ThreatSense и потоков сканирования.

В поле **Предельное время ответа (с)** можно задать максимальное время, в течение которого поток ждет завершения сканирования сообщения. Если в течение этого времени сканирование не завершается, Microsoft Exchange Server запретит клиенту доступ к электронной почте. Сканирование не будет прервано, а по его окончании все остальные попытки получить доступ к файлу будут успешны.

СОВЕТ. Для определения **количества потоков сканирования**, рекомендуемых поставщиком Microsoft Exchange Server, нужно использовать формулу: [количество физических процессоров] x 2 + 1.

ПРИМЕЧАНИЕ. Производительность не увеличивается существенно, если количество модулей сканирования ThreatSense больше потоков сканирования.

3.2.1.1.4 Microsoft Exchange Server 2007/2010 (VSAPI 2.6)

В состав этой версии Microsoft Exchange Server входит VSAPI версии 2.6.

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 39, а также будут применяться правила 22.

Если активирован параметр **Упреждающее 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 сканироваться до остальных ожидающих сообщений.

Параметр **Фоновое сканирование** позволяет сканировать все сообщения в фоновом режиме системы. 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 вложением** 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 месяцев**
- **Сообщения, полученные за последние 3 месяца**
- **Сообщения, полученные за последний месяц**
- **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 задачи она появляется в списке запланированных и, как и с другими задачами, можно изменить ее параметры, удалить ее или временно отключить.

Установка флажка **Сканировать тело 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.

3.2.1.1.4.1 Действия

В этом разделе можно задать действия, которые следует выполнять, если сообщение и/или вложение оценивается как зараженное.

В поле **Действие, если очистка невозможна** можно выбрать один из вариантов: **Блокировать** зараженное содержимое, **Удалить объект** для удаления зараженного содержимого сообщения, **Удалить сообщение целиком** или **Ничего не предпринимать**. Это действие будет применено, только если в результате автоматической очистки (задается в разделе **Настройка параметров модуля ThreatSense** > Очистка 67) не удалось очистить сообщение.

Как описано выше, можно выбрать одно из следующих значений для параметра **Действие, если очистка невозможна**.

- **Ничего не предпринимать**: не предпринимать никаких действий к зараженному содержимому сообщения.
- **Блокировать**: заблокировать сообщение, прежде чем оно будет получено, в хранилище Microsoft Exchange Server.
- **Удалить объект**: удалить зараженное содержимое сообщения.
- **Удалить сообщение целиком**: удалить все сообщение вместе с зараженным содержимым.

Параметр **Удаление** позволяет задать **метод удаления тела сообщения** и **метод удаления вложения**.

В качестве значений параметра **Метод удаления тела сообщения** можно выбрать один из следующих вариантов.

- **Удалить тело сообщения**: удаляется тело зараженного сообщения; получателю будут доставлены пустое сообщение и все незараженные вложения.
- **Заменить тело сообщения информацией действия**: тело зараженного сообщения заменяется информацией о выполненных действиях.
- **Удалить сообщение целиком**: удаляется сообщение целиком вместе с вложениями; можно также выбрать, какое действие следует предпринять при удалении вложений.

В качестве значений параметра **Метод удаления вложения** можно выбрать один из следующих вариантов.

- **Усечь файл до нулевой длины**: ESET Mail Security урезает вложение до нулевого размера и позволяет получателю видеть имя файла и тип вложения.
- **Заменить вложение информацией действия**: ESET Mail Security заменяет зараженный файл на протокол вируса или описание правила.
- **Удалить сообщение целиком**: вложение удаляется.

Если активирован параметр **Использовать карантин VSAPI**, зараженные сообщения будут храниться в карантине сервера электронной почты. Обратите внимание, что это карантин VSAPI под управлением сервера (не карантин клиента или почтовый ящик карантина). Зараженные сообщения, хранящиеся на карантине почтового сервера, будут недоступны до очистки с применением самой актуальной базы данных сигнатур вирусов.

Если нажать кнопку **Повторное сканирование**, то можно выполнить еще одно сканирование сообщений и файлов, которые уже были просканированы ранее.

3.2.1.1.4.2 Производительность

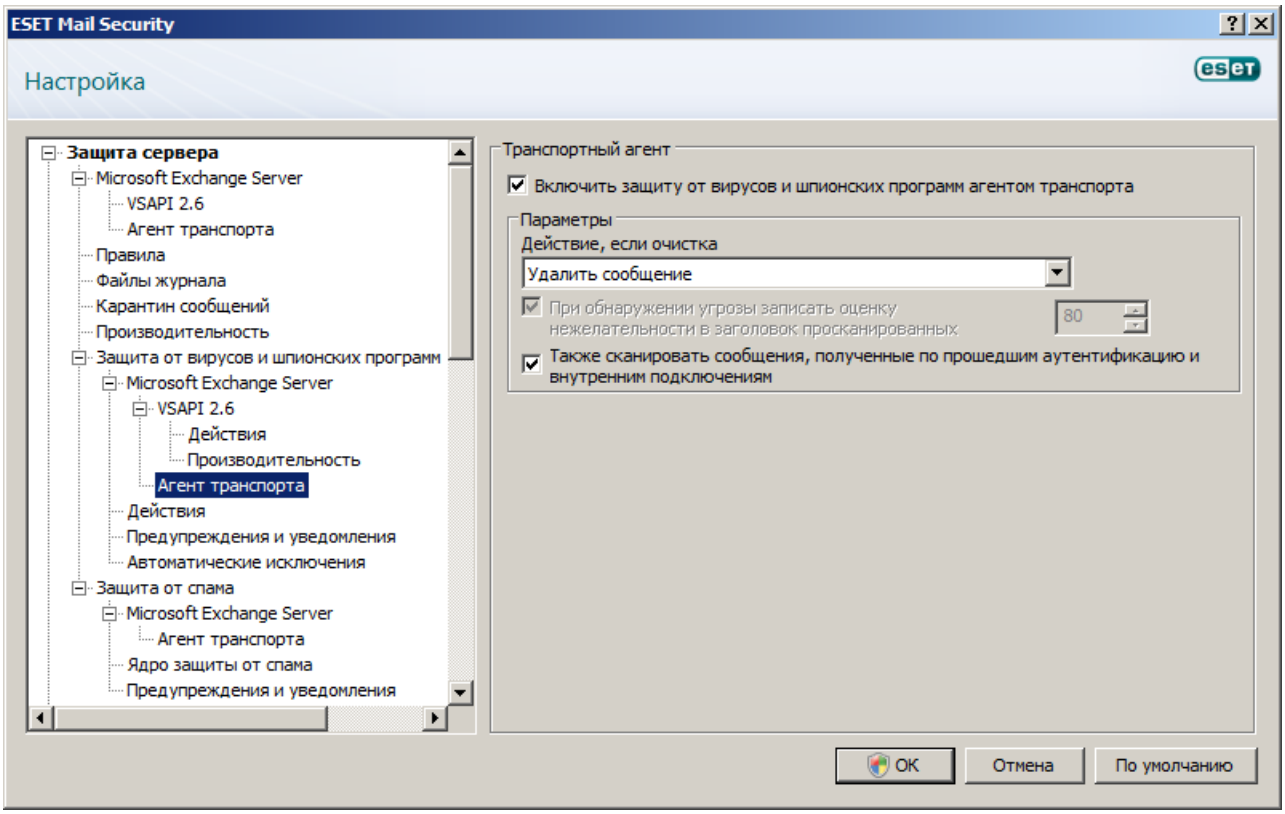
В этом разделе можно задать количество независимых потоков сканирования, используемых одновременно. Большее количество потоков на многопроцессорных компьютерах может увеличить скорость сканирования. Для обеспечения максимальной производительности программы рекомендуется использовать одинаковое количество модулей сканирования ThreatSense и потоков сканирования.

СОВЕТ. Для определения **количества потоков сканирования**, рекомендуемых поставщиком Microsoft Exchange Server, нужно использовать формулу: [количество физических процессоров] x 2 + 1.

ПРИМЕЧАНИЕ. Производительность не увеличивается существенно, если количество модулей сканирования ThreatSense больше потоков сканирования.

3.2.1.1.5 Транспортный агент

В этом разделе можно включить или отключить защиту от вирусов и шпионских программ, осуществляемую агентом транспорта. Для Microsoft Exchange Server 2007 и более поздних версий можно установить агент транспорта только в том случае, если сервер имеет одну из двух ролей: *пограничный транспортный сервер* или *транспортный сервер-концентратор*.



Если существует сообщение, которое невозможно очистить, оно будет обработано в соответствии с параметрами в разделе «Транспортный агент». Это сообщение можно удалить, отправить в почтовый ящик карантина или сохранить.

Если снять флажок **Включить защиту от вирусов и шпионских программ агентом транспорта**, 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 39, а также будут применяться правила 22 .

Если установить флажок **Включить защиту от вирусов и шпионских программ агентом транспорта**, также можно выбрать **Действие, если очистка невозможна**.

- **Сохранить сообщение**: зараженное сообщение, которое не удалось очистить, сохраняется.
- **Направить сообщение на карантин**: зараженное сообщение отправляется в почтовый ящик карантина.
- **Удалить сообщение**: зараженное сообщение удаляется.

При обнаружении угрозы записать оценку нежелательности в заголовок просканированных сообщений (в %): оценке нежелательности (вероятность того, что сообщение является спамом) присваивается заданное значение в процентах.

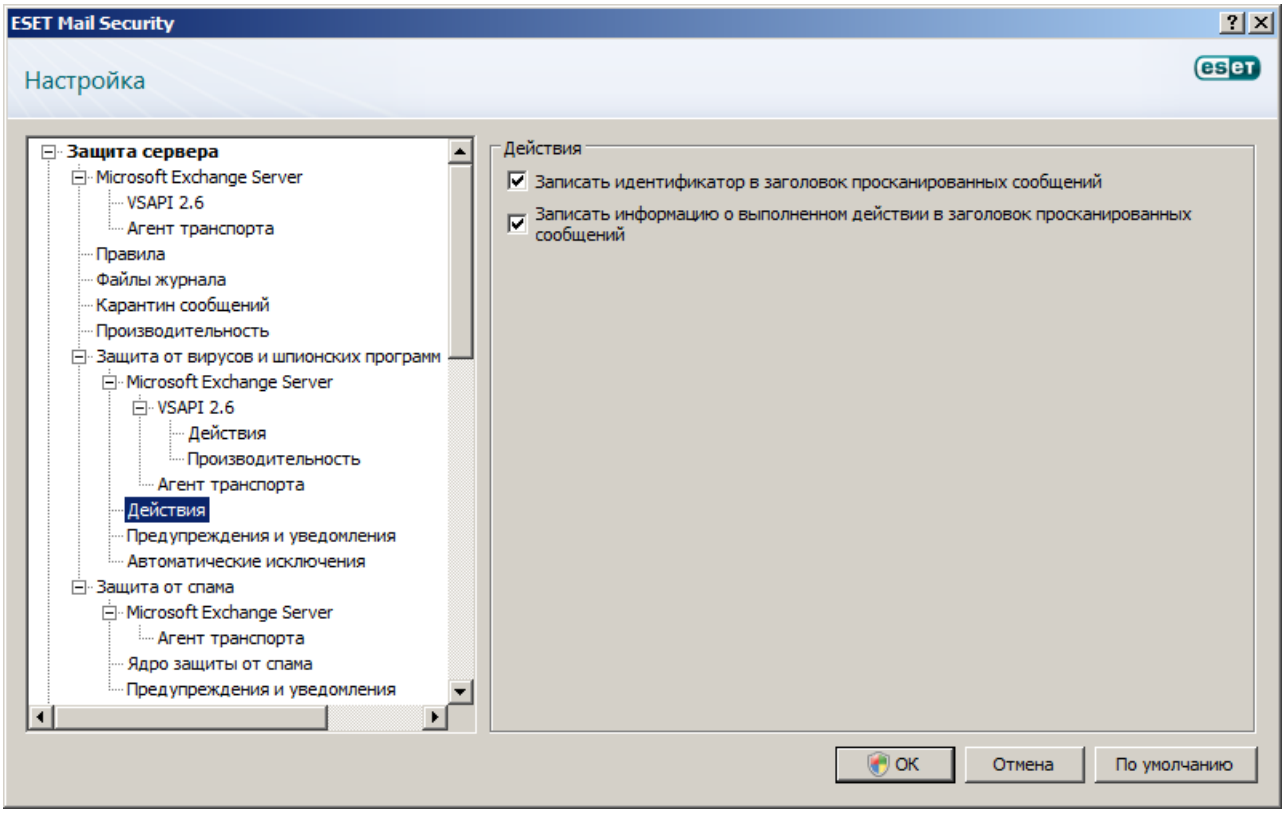
Это значит, что при обнаружении угрозы оценка нежелательности (заданное значение в процентах) будет записана в просканированное сообщение. Поскольку большая часть зараженных сообщений рассылаются ботнетами, распространяемые таким образом сообщения можно классифицировать как спам. Для обеспечения эффективной работы этой функции нужно активировать параметр **Записывать вероятность нежелательной почты в просканированные сообщения на основе оценки нежелательности** в разделе **Защита сервера**> **Microsoft Exchange Server** > Транспортный агент 20.

Если активирован параметр **Также сканировать сообщения, полученные по прошедшим**

аутентификацию и внутренним подключениям, ESET Mail Security также выполняет сканирование сообщений, полученных от прошедших аутентификацию источников или локальных серверов. Рекомендуется сканировать такие сообщения, так как это делает защиту еще более надежной, но это не обязательно.

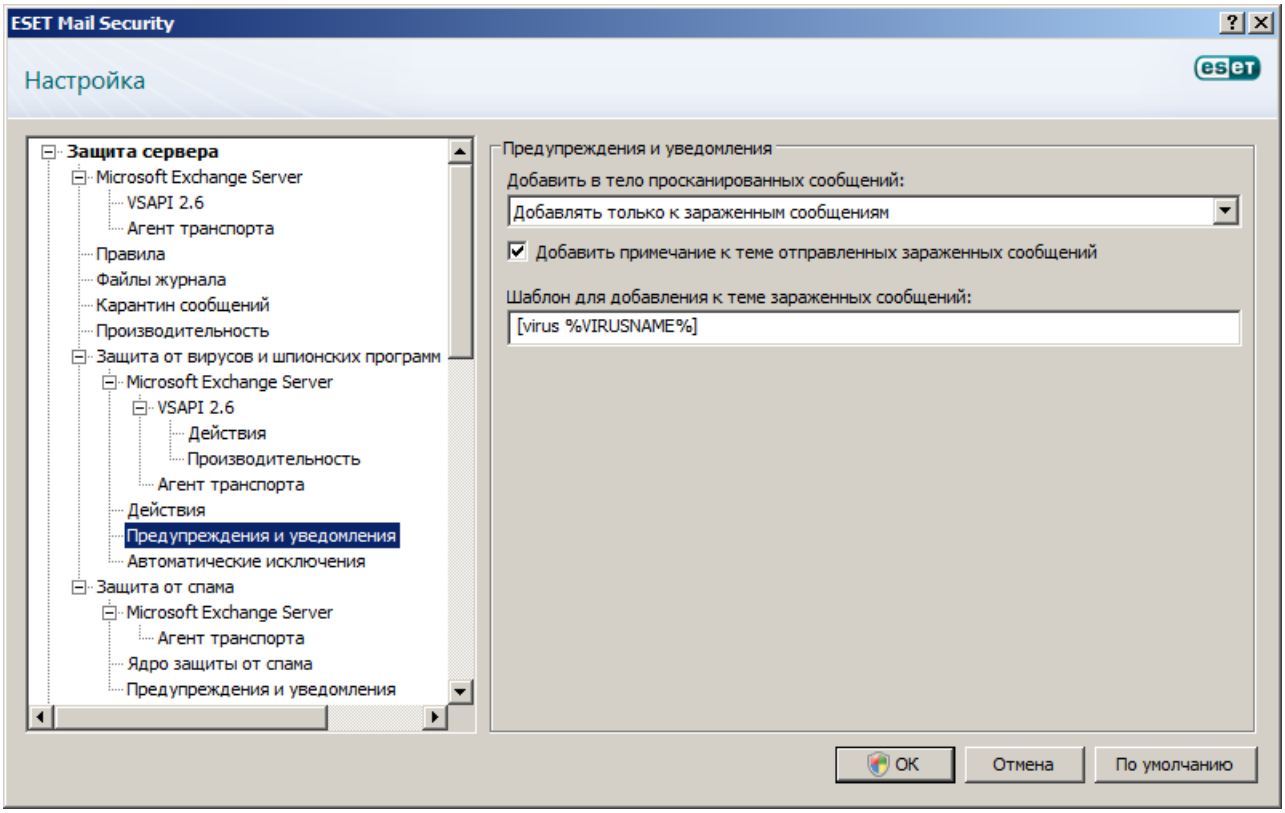
3.2.2 Действия

В этом разделе можно выбрать, следует ли добавлять идентификатор задачи сканирования и/или информацию о результатах сканирования в заголовок просканированных сообщений.



3.2.3 Предупреждения и уведомления

ESET Mail Security позволяет добавить текст в исходную тему или тело зараженного сообщения.



Добавить в тело просканированных сообщений: позволяет использовать один из трех описанных далее вариантов.

- Не добавлять к сообщениям
- Добавлять только к зараженным сообщениям
- Добавлять ко всем просканированным сообщениям

Если выбрать вариант **Добавить к теме зараженных сообщений**, ESET Mail Security будет добавлять уведомление в тему сообщения. Значение такого уведомления задается в текстовом поле **Шаблон для добавления к теме зараженных сообщений** (по умолчанию [*virus %VIRUSNAME%*]). Описанные выше изменения могут автоматизировать фильтрацию электронной почты путем переноса сообщений с определенной темой (если это поддерживается почтовым клиентом) в отдельную папку.

ПРИМЕЧАНИЕ. Также можно использовать системные переменные при добавлении шаблона в тему сообщения.

3.2.4 Автоматические исключения

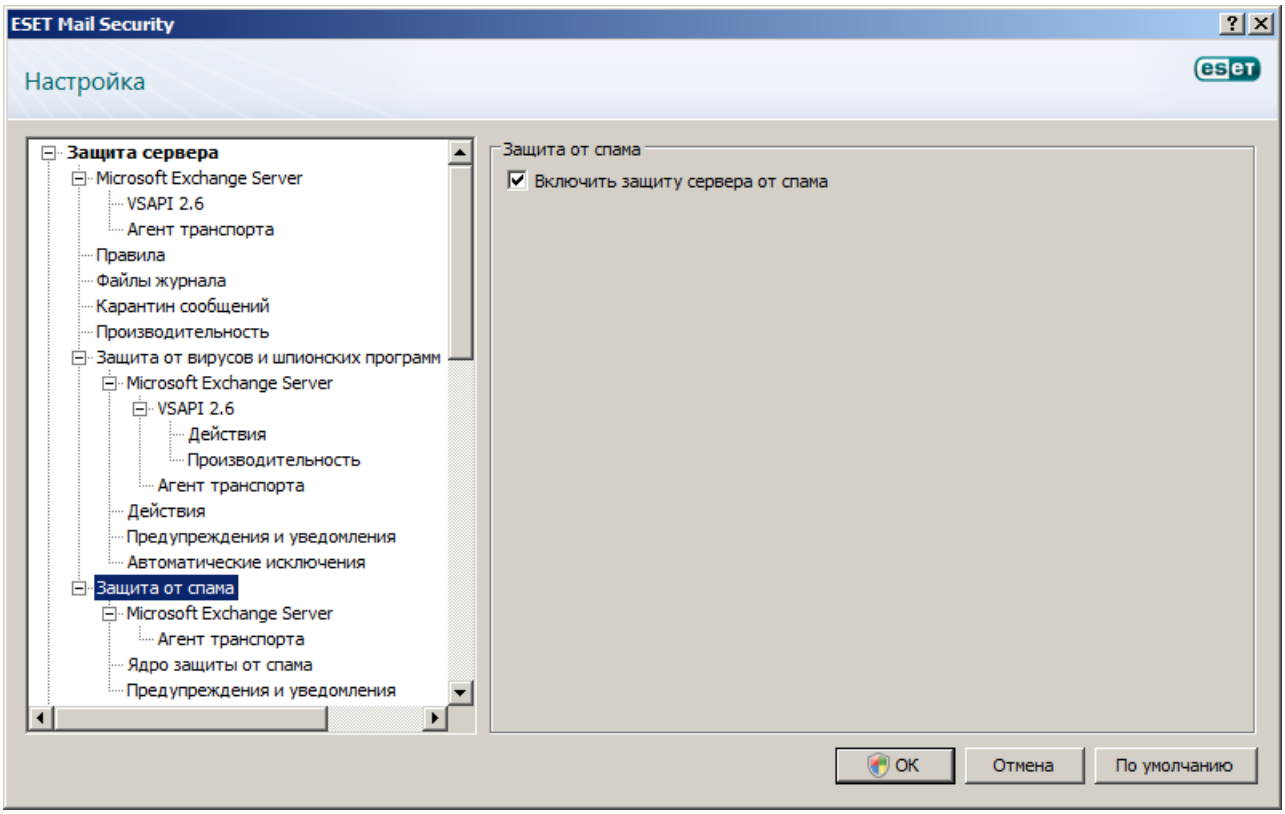
Разработчики серверных приложений и операционных систем рекомендуют исключать наборы критических рабочих файлов и папок из антивирусного сканирования для большинства таких программных продуктов. Антивирусное сканирование может отрицательно повлиять на производительность сервера, привести к конфликтам 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.
ESET Mail Security выявляет критические файлы серверных приложений и серверных операционных система и автоматически добавляет их в список Исключения. После добавления в список серверный процесс или приложение может быть включено (по умолчанию) путем установки соответствующего флажка или же отключено его снятием. В результате ситуация будет развиваться следующим образом.

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** > **Защита компьютера** > **Защита от вирусов и шпионских программ** > **Исключения**). 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 рекомендованных 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** > **Защита компьютера** > **Защита от вирусов и шпионских программ** > **Исключения**). Однако они не будут автоматически проверяться и восстанавливаться в списке **Исключения** при каждом перезапуске сервера (см. пункт 1 выше). Эту настройку рекомендуется применять только опытным пользователям, которым нужно удалить или изменить какие-либо из стандартных исключений. Если нужно удалить исключения из списка без перезапуска сервера, их следует удалить вручную (**Дополнительные настройки** > **Защита компьютера** > **Защита от вирусов и шпионских программ** > **Исключения)**.

Описанные выше настройки никак не влияют на любые пользовательские исключения, введенные вручную в разделе **Дополнительные настройки** > **Защита компьютера** > **Защита от вирусов и шпионских программ** > **Исключения**.
Автоматические исключения для серверных приложений и операционных систем выбираются на основе рекомендаций Microsoft. Для получения дополнительных сведений воспользуйтесь следующими ссылками.
http://support.microsoft.com/kb/822158
http://support.microsoft.com/kb/245822
http://support.microsoft.com/kb/823166
http://technet.microsoft.com/en-us/library/bb332342%28EXCHG.80%29.aspx
http://technet.microsoft.com/en-us/library/bb332342.aspx

3.3 Защита от спама

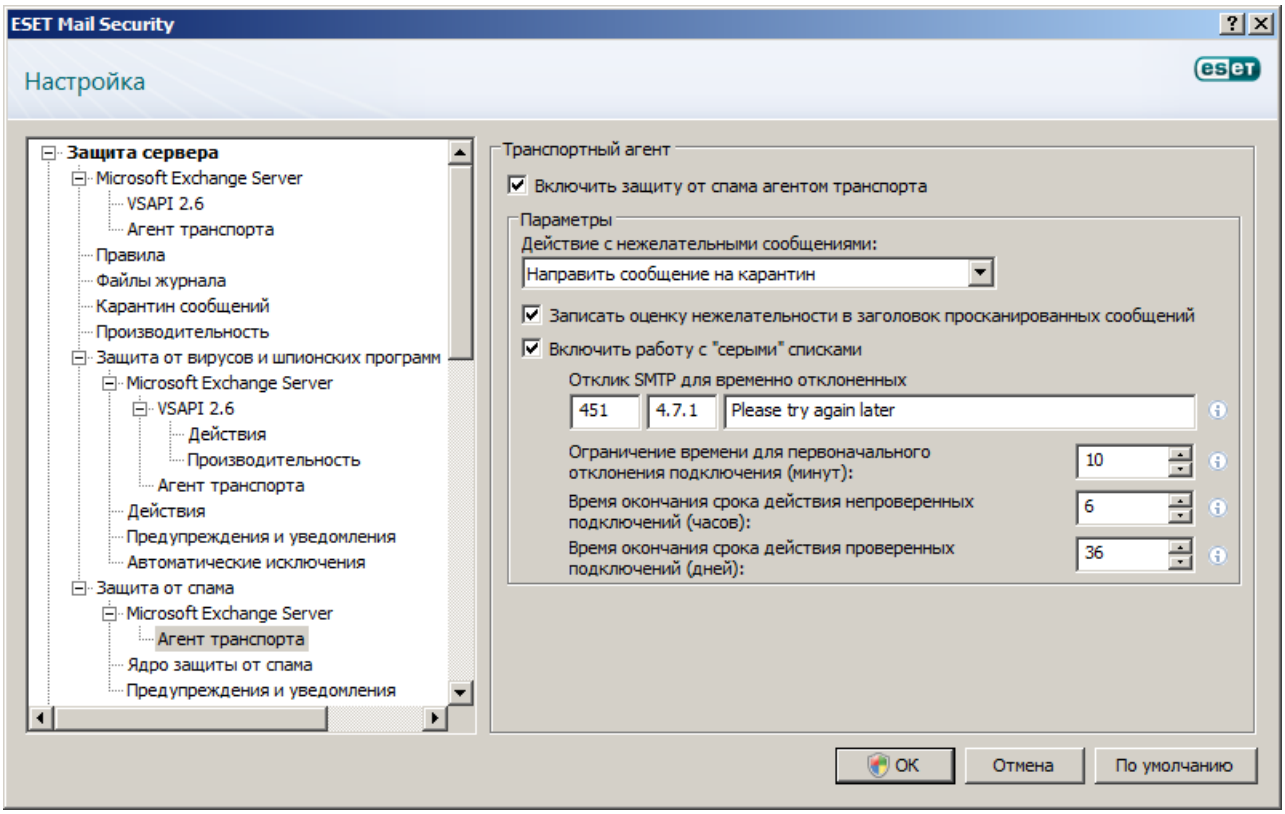
В разделе **Защита от спама** можно включать и отключать защиту от спама для установленного почтового сервера, конфигурировать параметры ядра защиты от спама и задавать другие уровни защиты.



3.3.1 Microsoft Exchange Server

3.3.1.1 Транспортный агент

В этом разделе можно задать параметры защиты от спама с использованием агента транспорта.



ПРИМЕЧАНИЕ. Агент транспорта недоступен в Microsoft Exchange Server 5.5.

При активации параметра **Включить защиту от спама агентом транспорта** пользователь настраивает перечисленные далее параметры как **Действие с нежелательными сообщениями**.

- **Сохранить сообщение**: сообщение сохраняется, даже если оно помечено как спам.
- **Направить сообщение на карантин**: помеченное как спам сообщение отправляется в почтовый ящик карантина.
- **Удалить сообщение**: помеченное как спам сообщение удаляется.

Если нужно включить в заголовок сообщения информацию о его оценке нежелательности, установите флажок **Записать оценку нежелательности в заголовок просканированных сообщений**.

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 не от известного 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 спама.
При оценке источника сообщения этим методом учитываются конфигурации списков **Разрешенные IP-адреса**, **Игнорируемые IP-адреса**, **Надежные отправители** и **Разрешить IP** на сервере Exchange и параметры AntispamBypass для почтового ящика получателя. Сообщения электронной почты, поступающие от IP-адресов/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.

В поле **Отклик SMTP для временно отклоненных подключений** задается ответ о временном отклонении, отправляемый SMTP-серверу, если сообщение отклоняется.

Пример отправляемого по SMTP ответного сообщения

Основной код ответа	Дополнительный код состояния	Описание
451	4.7.1	Requested action aborted: (Запрошенное действие прервано:) local error in processing (локальная ошибка при обработке)

Внимание: 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.

Ограничение времени для первоначального отклонения подключения (минут): 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.

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

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

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

3.3.2 Ядро защиты от спама

Здесь можно сконфигурировать параметры **ядра защиты от спама**. Это можно сделать, нажав кнопку **Настроить...**. Откроется окно, в котором можно сконфигурировать перечисленные далее параметры ядра защиты от спама 41.

Классификация сообщений

Ядро защиты от спама ESET Mail Security присваивает каждому просканированному сообщению оценку нежелательности в диапазоне от 0 до 100. Изменяя предельные значения диапазона оценок нежелательности в этом разделе, можно влиять на следующие факторы.

1) Классификация сообщения как СПАМА или как НЕ СПАМА. Все сообщения, имеющие оценку нежелательности, равную или превышающую значение параметра **Оценка нежелательности для обработки сообщения как спама** , считаются СПАМОМ. В результате к таким сообщениям будут применены действия, заданные в разделе Транспортный агент 39.

2) Запись сообщения в журнал защиты от спама 84 (**Служебные программы** > **Файлы журнала** > **Защита от спама**). Все сообщения, имеющие оценку нежелательности, равную или превышающую значение параметра **Пороговое значение оценки нежелательности, при котором сообщение обрабатывается как возможный спам или разрешенное сообщение** , записываются в журнал.

3) Один из перечисленных далее разделов статистики защиты от спама, в котором будет учтено данное сообщение (**Состояние защиты > Статистика > Защита почтового сервера от спама**).

Сообщения, классифицированные как спам: оценка нежелательности сообщения равна или больше значения, заданного в параметре **Оценка нежелательности для обработки сообщения как спама**.

Сообщения, классифицированные как возможный спам: оценка нежелательности сообщения равна или больше значения, заданного в параметре **Пороговое значение оценки нежелательности, при котором**

сообщение обрабатывается как возможный спам или разрешенное сообщение.

Сообщения, классифицированный как возможный не спам: оценка нежелательности сообщения ниже значения, заданного в параметре **Пороговое значение оценки нежелательности, при котором сообщение обрабатывается как возможный спам или разрешенное сообщение**.

Сообщения, классифицированные как не спам: оценка нежелательности сообщения равна или меньше значения, заданного в параметре **Оценка нежелательности для обработки сообщения как не спама**.

3.3.2.1 Настройка параметров ядра защиты от спама

Настройка параметров ядра защиты от спама
Можно выбрать профиль из набора предварительно сконфигурированных профилей (**Рекомендуемая**, **Наиболее точная**, **Самая быстрая**, **Выборочная**). Список профилей загружается из модуля защиты от спама. Для каждого из указанных профилей из файла *spamcatcher.conf* загружаются различные конкретные параметры, а другая конкретная подгруппа параметров загружается непосредственно из программы, причем вновь они будут разными для каждого отдельного профиля. Даже если выбран вариант **Выборочная**, некоторые параметры применяются непосредственно из программы, а не из файла *spamcatcher.conf*, т. е. параметры прокси-сервера из файла *spamcatcher.conf* не будут применены, если прокси-сервер был сконфигурирован через графический интерфейс пользователя ESET Mail Security, поскольку параметры из программы всегда имеют более высокий приоритет по сравнению с параметрами из файла *spamcatcher.conf*. Параметр автоматического обновления ядра защиты от спама каждый раз будет менять состояние на отключенное вне зависимости от изменений в файле *spamcatcher.conf*.

Профиль **Рекомендуемая** состоит из рекомендуемых параметров и представляет собой наиболее рациональное сочетание безопасности и влияния на производительность системы.
Единственной целью профиля **Наиболее точная** является безопасность почтового сервера. Этот профиль потребляет больше системных ресурсов по сравнению с рекомендуемым.
Профиль **Самая быстрая** предварительно сконфигурирован для обеспечения минимального потребления системных ресурсов, что достигается за счет отключения некоторых функций сканирования.
Раздел **Выборочная** > **Открыть файл конфигурации** дает пользователю возможность изменить файл *spamcatcher.conf*. Этот вариант рекомендован тем системным администраторам, которым нужно полностью самостоятельно выбрать все параметры системы (при необходимости). Но первые три варианта профилей должны быть достаточны в большинстве ситуаций. Если нужно использовать выборочный профиль, ознакомьтесь с главой Файл конфигурации 44 для получения дополнительных сведений о доступных параметрах и их влиянии на систему. Необходимо помнить, что есть ряд параметров, которые применяются непосредственно из программы, а потому имеют более высокий приоритет по сравнению с параметрами из файла *spamcatcher.conf*. Это нужно, чтобы предотвратить неправильное конфигурирование важнейших компонентов, которое могло бы привести к некорректной работе ESET Mail Security.

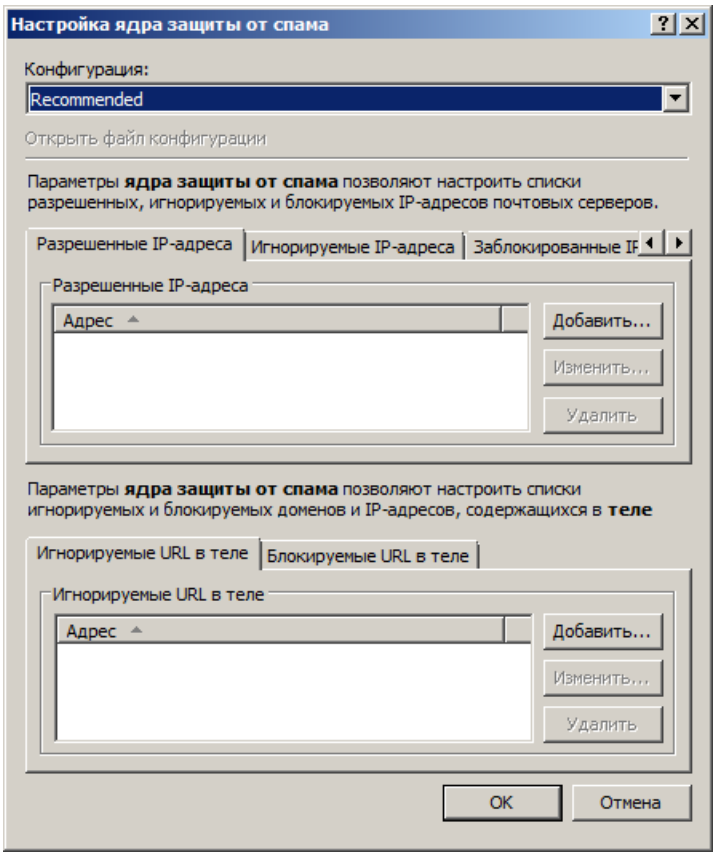
Изменить параметры в файле *spamcatcher.conf* можно двумя способами. Первый способ заключается в использовании графического интерфейса пользователя ESET Mail Security, для чего нужно выбрать профиль **Выборочная** в раскрывающемся меню **Конфигурация**. Затем следует нажать ссылку **Открыть файл конфигурации** непосредственно под раскрывающимся меню профиля. В результате файл *spamcatcher.conf* будет открыт в «Блокноте» для редактирования. Второй способ заключается в том, чтобы открыть файл *spamcatcher.conf* непосредственно в любом другом текстовом редакторе. Файл *spamcatcher.conf* находится в папке *C:\Documents and Settings\All Users\Application Data\ESET\ESET Mail Security\MailServer* в Windows Server 2000 и 2003, а для Windows Server 2008 в папке *C:\ProgramData\ESET\ESET Mail Security\MailServer*.

После внесения в файл *spamcatcher.conf* нужных параметров нужно перезапустить ядро защиты от спама, чтобы в него попали изменения из программы и из файла конфигурации. Если файл *spamcatcher.conf* изменялся через графический интерфейс пользователя, можно просто закрыть диалоговое окно, нажав кнопку «OK». При этом будет перезапущено ядро защиты от спама. Также при этом станет неактивной ссылка **Перезагрузка параметров ядра защиты от спама**. Это значит, что ядро защиты от спама было перезапущено.

Если же изменения в файл *spamcatcher.conf* вносились непосредственно в текстовом редакторе (не через графический интерфейс пользователя), то необходимо перезапустить ядро защиты от спама, чтобы изменения попали в программу. Существует несколько способов перезапуска ядра защиты от спама. Можно оставить ядро защиты от спама для перезапуска в следующий раз (например, при обновлении базы данных сигнатур) или при необходимости перезапустить его вручную через древовидную структуру расширенного меню (F5) **Защита сервера** > **Защита от спама** > **Ядро защиты от спама**, где нужно нажать ссылку **Перезагрузка параметров ядра защиты от спама**. Также перезапустить ядро защиты от спама можно путем отключения и повторного включения защиты от спама через главное окно ESET Mail Security. Для этого нужно перейти в раздел **Настройка** > **Защита от спама**, где нажать **Временно отключить защиту от спама** в нижней части окна, а затем нажать **Включить защиту от спама**.

После этого ядром защиты от спама будет использоваться новая конфигурация.

ПРИМЕЧАНИЕ. Можно использовать измененный файл *spamcatcher.conf* вместе с профилем конфигурации, отличным от **Выборочная** (например, с профилем **Наиболее точная**). В этом случае некоторые параметры используются в соответствии с конфигурацией в файле *spamcatcher.conf* , а некоторые — так, как задано в графическом интерфейсе пользователя. Если значения параметров отличаются, параметры из графического интерфейса пользователя всегда имеют преимущество перед параметрами из файла *spamcatcher.conf* (за исключением некоторых важнейших компонентов системы, которые задаются программой вне зависимости от того, что указано в графическом интерфейсе пользователя или в файле *spamcatcher.conf*).



На вкладке **Разрешенные IP-адреса** можно указать IP-адреса, которые следует разрешать. Это значит, что в том случае, когда первый непропущенный IP-адрес из заголовка полученного сообщения совпадает с любым адресом из этого списка, сообщение получает оценку 0, а дальнейшие проверки не выполняются.

На вкладке **Игнорируемые IP-адреса** можно указать IP-адреса, которые следует пропускать при проверках по «черным» спискам реального времени. Следует включить в этот список все внутренние IP-адреса, защищаемые файерволом, которые недоступны непосредственно через Интернет. Это позволяет избежать ненужных проверок и помогает определить фактические IP-адреса, которые выполняют подключение. Внутренние IP-адреса уже пропускаются ядром (192.168.x.y и 10.x).

На вкладке **Заблокированные IP-адреса** можно указать IP-адреса, которые следует блокировать. Это значит, что в том случае, когда любой непропущенный IP-адрес из заголовка полученного сообщения совпадает с адресом из этого списка, сообщение получает оценку 100, а дальнейшие проверки не

выполняются.

На вкладке **Пропущенные домены** можно указать домены, используемые в теле сообщения, которые всегда следует исключать из проверок DNSBL и MSBL и пропускать.

На вкладке **Заблокированные домены** можно указать домены, используемые в теле сообщения, которые всегда следует блокировать.

ПРИМЕЧАНИЕ. В отличие от IP-адресов при добавлении доменов нельзя использовать подстановочные знаки.

Технологии защиты от спама и работы с «серыми» списками также позволяют использовать так называемую работу с «белым» списком.

Возможности применения работы с «белым» списком для работы с «серыми» списками

Microsoft Exchange 2003
- список разрешенных IP-адресов в интеллектуальном фильтре сообщений Exchange (**Фильтрация подключений > Глобальный список разрешенных адресов**)
- список разрешенных и пропущенных IP-адресов в параметрах ESET Mail Security

Microsoft Exchange 2007/2010
- список разрешенных и пропущенных IP-адресов в параметрах ESET Mail Security
- список надежных отправителей для конкретного получателя
- параметр AntispamBypassEnabled для конкретного почтового ящика
- список разрешенных IP-адресов в Microsoft Exchange
- параметр AntispamBypassEnabled для конкретного подключения по SMTP

Возможности применения работы с «белым» списком для защиты от спама

Общие
- список разрешенных IP-адресов в параметрах ESET Mail Security
- список доменов почты в файле *approvedsenders*
- фильтрация на основе правил

Microsoft Exchange 2003
- список разрешенных IP-адресов в интеллектуальном фильтре сообщений Exchange (**Фильтрация подключений > Глобальный список разрешенных адресов**)

Microsoft Exchange 2007/2010
- список надежных отправителей для конкретного получателя
- параметр AntispamBypassEnabled для конкретного почтового ящика
- список разрешенных IP-адресов в Microsoft Exchange
- параметр AntispamBypassEnabled для конкретного подключения по SMTP

ПРИМЕЧАНИЕ: Общей характеристикой технологий защиты от спама и работы с «серыми» списками является то, что сообщения от прошедших аутентификацию и внутренних источников не проверяются на предмет спама.

3.3.2.1.1 Файл конфигурации

Файл конфигурации *spamcatcher.conf* позволяет изменить ряд дополнительных параметров, которые не доступны в графическом интерфейсе пользователя ESET Mail Security. Параметры в файле *spamcatcher.conf* явным образом структурированы и описаны.

Имя — имя параметра
Аргументы — значения, которые могут быть присвоены параметру, а также их синтаксис
По умолчанию — значение параметра по умолчанию
Описание — подробное описание параметра

Пустые строки и строки, начинающиеся с символа решетки («#»), опускаются.

Перечень самых важных параметров, присутствующих в файле *spamcatcher.conf*, приведен далее.

Имя параметра	Описание
approved_ip_list	Перечень одобренных IP-адресов. Нет необходимости добавлять список в файл *spamcatcher.conf*. Сформировать его можно в графическом интерфейсе пользователя программы (см. главу Настройка параметров ядра защиты от спама 41).
blocked_ip_list	Перечень заблокированных IP-адресов. Нет необходимости добавлять список в файл *spamcatcher.conf*. Сформировать его можно в графическом интерфейсе пользователя программы (см. главу Настройка параметров ядра защиты от спама 41).
ignored_ip_list	Перечень пропущенных IP-адресов. Нет необходимости добавлять список в файл *spamcatcher.conf*. Сформировать его можно в графическом интерфейсе пользователя программы (см. главу Настройка параметров ядра защиты от спама 41).
rbl_list	Перечень серверов «черных» списков реального времени, которые следует использовать при оценке сообщений. Запрос к «черным» спискам реального времени проверяет наличие конкретного IP-адреса на данном сервере. Таким проверкам подвергаются IP-адреса из раздела «Получено» в заголовке сообщения. Используется такой формат ввода: `rbl_list=сервер:ответ:коррекция,сервер2:ответ2:коррекция2,...` Значение параметров описывается далее. 1) Сервер — имя сервера «черных» списков реального времени. 2) Ответ — ответ сервера «черных» списков реального времени, если обнаружен IP-адрес (стандартными являются ответы 127.0.0.2, 127.0.0.3, 127.0.0.4 и т. п.). Этот параметр является необязательным, при его отсутствии будут учитываться все ответы. 3) Коррекция — значение от 0 до 100, которое влияет на общую оценку нежелательности. Стандартным значением является 100, т. е. в случае положительного результата проверки сообщению присваивается оценка нежелательности 100, а само сообщение считается спамом. Отрицательные значения снижают общую оценку нежелательности сообщения. Также следует ожидать значения 0 при обработке сообщений от отправителей из файла *approvedsenders* и значения 100, если сообщения поступили от отправителей из файла *blockedsenders* (см. ниже). Пример 1. `rbl_list=ent.adbl.org` Для проверки в «черных» списках реального времени используется сервер `ent.adbl.org`. Если результат проверки положительный, сообщению будет присвоено стандартное значение коррекции 100, а само сообщение будет помечено как спам. Пример 2. `rbl_list=ent.adbl.org::60` Для проверки в «черных» списках реального времени используется сервер `ent.adbl.org`. Если результат проверки положительный, сообщению будет присвоено значение коррекции 60, которое увеличивает общую оценку нежелательности. Пример 3. `rbl_list=bx9.dbl.com::85, list.dnb.org:127.0.0.4:35, req.gsender.org::-75` Для проверки в «черных» списках реального времени используются заданные серверы (слева направо). При положительном результате проверки по серверу `bx9.dbl.com` будет добавлено значение коррекции 85. Если проверка по серверу `list.dnb.org` будет положительной с ответом 127.0.0.4, будет использоваться значение коррекции 35. Коррекция не будет применяться, если ответы будут отличны от 127.0.0.4. При

	положительном результате проверки по серверу `req.gsender.org` оценка нежелательности будет уменьшена на 75 пунктов (отрицательное значение).
rbl_max_ips	Максимальное количество IP-адресов, которые могут быть отправлены для проверки на сервер «черных» списков реального времени. Общее количество запросов на сервер «черных» списков реального времени равняется общему количеству IP-адресов в разделах «Получено» заголовка сообщения (до заданного в rbl_maxcheck_ips ограничения), умноженному на количество серверов «черных» списков реального времени, заданных в параметре rbl_list. Значение 0 означает, что не существует ограничений по максимальному количеству IP-адресов, которые могут проверяться. IP-адреса в параметре ignored_ip_list (т. е. список **Пропущенные IP-адреса** в параметрах ESET Mail Security). Этот параметр применяется только в том случае, если включен параметр rbl_list (т. е. в нем есть хотя бы 1 сервер).
approved_domain_list	Это список доменов и IP-адресов в теле сообщения электронной почты, которые следует считать разрешенными. Этот список не следует использовать для внесения в «белый» список адресов электронной почты по домену отправителя!
blocked_domain_list	Это список доменов и IP-адресов в теле сообщения электронной почты, которые следует считать постоянно заблокированными. Это не «черный» список адресов отправителей! Нет необходимости добавлять список в файл *spamcatcher.conf*. Сформировать его можно в графическом интерфейсе пользователя программы (см. главу Настройка параметров ядра защиты от спама 41).
ignored_domain_list	Список доменов в теле сообщения электронной почты, которые следует постоянно исключить из проверок DNSBL и игнорировать. Нет необходимости добавлять список в файл *spamcatcher.conf*. Сформировать его можно в графическом интерфейсе пользователя программы (см. главу Настройка параметров ядра защиты от спама 41).
dnsbl_list	Список серверов DNSBL, которые следует использовать для проверок доменов и IP-адресов в теле сообщения электронной почты. Используется следующий формат записи: `dnsbl_list=сервер:ответ:коррекция,сервер2:ответ2:коррекция2,...` Используемые параметры описаны далее. 1) Сервер — имя сервера DNSBL. 2) Ответ — ответ сервера DNSBL, если обнаружен IP-адрес или домен (стандартными являются ответы 127.0.0.2, 127.0.0.3, 127.0.0.4 и т. п.). Этот параметр является необязательным, при его отсутствии будут учитываться все ответы. 3) Коррекция — значение от 0 до 100, которое влияет на общую оценку нежелательности. Стандартным значением является 100, т. е. в случае положительного результата проверки сообщению присваивается оценка нежелательности 100, а само сообщение считается спамом. Отрицательные значения снижают общую оценку нежелательности сообщения. Также следует ожидать значения 0 при обработке сообщений от отправителей из файла *approvedsenders* и значения 100, если сообщения поступили от отправителей из файла *blockedsenders* (см. ниже). Проверки DNSBL могут отрицательно повлиять на производительность сервера в связи с тем, что каждый домен/IP-адрес из тела сообщения проверяется по всем заданным серверам DNSBL, причем для каждой проверки нужно обработать запрос к DNS-серверу. Сократить потребление системных ресурсов можно, развернув для этой цели DNS-сервер кэширования. По той же причине IP-адреса без поддержки маршрутизации (10.x.x.x, 127.x.x.x, 192.168.x.x) также опускаются при проверках DNSBL. Пример 1. `dnsbl_list=ent.adbl.org` Проверка DNSBL выполняется по серверу `ent.adbl.org` . При положительном результате проверки сообщению присваивается значение коррекции по умолчанию 100 (сообщение будет помечено как спам). Пример 2. `dnsbl_list=ent.adbl.org::60` Для проверки DNSBL используется сервер `ent.adbl.org` . Если результат проверки положительный, сообщению будет присвоено значение коррекции 60, которое увеличивает общую оценку нежелательности. Пример 3. `dnsbl_list=bx9.dbl.com::85, list.dnb.org:127.0.0.4:35, req.gsender.org::-75` Для проверки DNSBL используются заданные серверы (слева направо). При

	положительном результате проверки по серверу `bx9.dbl.com` будет добавлено значение коррекции 85. Если проверка по серверу `list.dnb.org` будет положительной с ответом `127.0.0.4` , то будет использоваться значение коррекции 35. Коррекция не будет применяться, если ответы будут отличны от 127.0.0.4. При положительном результате проверки по серверу `req.gsender.org` оценка нежелательности будет уменьшена на 75 пунктов (отрицательное значение).
home_country_list	Список стран, которые будут считаться страной проживания. Сообщения, маршрутизируемые через страну, отсутствующую в этом списке, будут оцениваться с использованием более жестких правил (будет применена более высокая оценка нежелательности). В качестве формата записи стран используется их двузначный код в соответствии с ISO 3166.
home_language_list	Список предпочтительных языков, т. е. тех языков, которые чаще всего используются в сообщениях электронной почты. Такие сообщения будут оцениваться с применением менее жестких правил (более низкая оценка нежелательности). В качестве формата записи языков используется их двузначный код в соответствии с ISO 639.
custom_rules_list	Позволяет задать пользовательские списки правил и хранить каждый список в отдельном файле. Каждое правило записывается в отдельной строке файла в следующем формате. **Фраза**, **тип**, **вероятность**, **УчетРегистра** **Фраза** — любой текст без запятых (,). **Тип**: может иметь одно из значений: SPAM, PHISH, BOUNCE, ADULT, FRAUD. Если ввести отличное от перечисленных значение, автоматически будет использоваться значение SPAM. Значение SPAM задает фразы, которые встречаются в типичных нежелательных сообщениях (предложения товаров и услуг). PHISH — это фразы, содержащиеся в мошеннических сообщениях (фишинг), целью которых является получение конфиденциальных данных (имена, пароли, номера кредитных карт и т. п.) от пользователей. BOUNCE — это фразы, используемые в автоматических ответах сервера, таких как уведомления о невозможности доставки (используются при подделках адреса отправителя). ADULT представляет фразы, часто встречающиеся в сообщениях, в которых предлагаются порнографические материалы. FRAUD обозначает фразы, используемые в мошеннических сообщениях электронной почты, в которых предлагаются подозрительные банковские операции (денежный перевод через счет пользователя и т. п.). Типичным примером такого типа спама являются так называемые нигерийские письма. **Вероятность** — значение от 0 до 100. Определяет вероятность принадлежности фразы к конкретной категории спама (одной из перечисленных выше). Если для типа PHISH вероятность составляет 90, очень высока вероятность того, что данная фраза используется в сообщениях фишинга. Чем выше вероятность, тем больше она влияет на общую оценку нежелательности сообщения. Существует особый случай, когда значение вероятности равно 100, причем оценка нежелательности сообщения также равна 100, т. е. сообщение будет помечено как спам с точностью 100 %. Точно так же в случае, когда данное значение равно 0, сообщение будет помечено как не спам. **УчетРегистра** — значение 0 или 1. Если 0, то фраза используется без учета регистра. 1 показывает, что фраза используется с учетом регистра. Примеры реплика, SPAM, 100, 0 Уважаемый пользователь eBay, PHISH, 90, 1 return to sender, BOUNCE, 80, 0

Дальнейшие параметры для работы с «черным и «белым» списками доступны в файлах *approvedsenders* и *blockedsenders*, которые находятся в папке C:*Documents and Settings\All Users\Application Data\ESET\ESET Mail Security\MailServer* в Windows Server 2000 и 2003 или в папке C:*ProgramData\ESET\ESET Mail Security\MailServer* в Windows Server 2008. В эти списки можно добавить адреса или домены отправителя, причем файл *approvedsenders* представляет собой список разрешенных адресов/доменов, а в файле *blockedsenders* перечисляются заблокированные адреса/домены.

Внимание: Поскольку очень часто используются методы подделки адресов отправителей (они изменяются так, чтобы сообщения казались отправленными тем, кто их якобы отправил), не рекомендуется

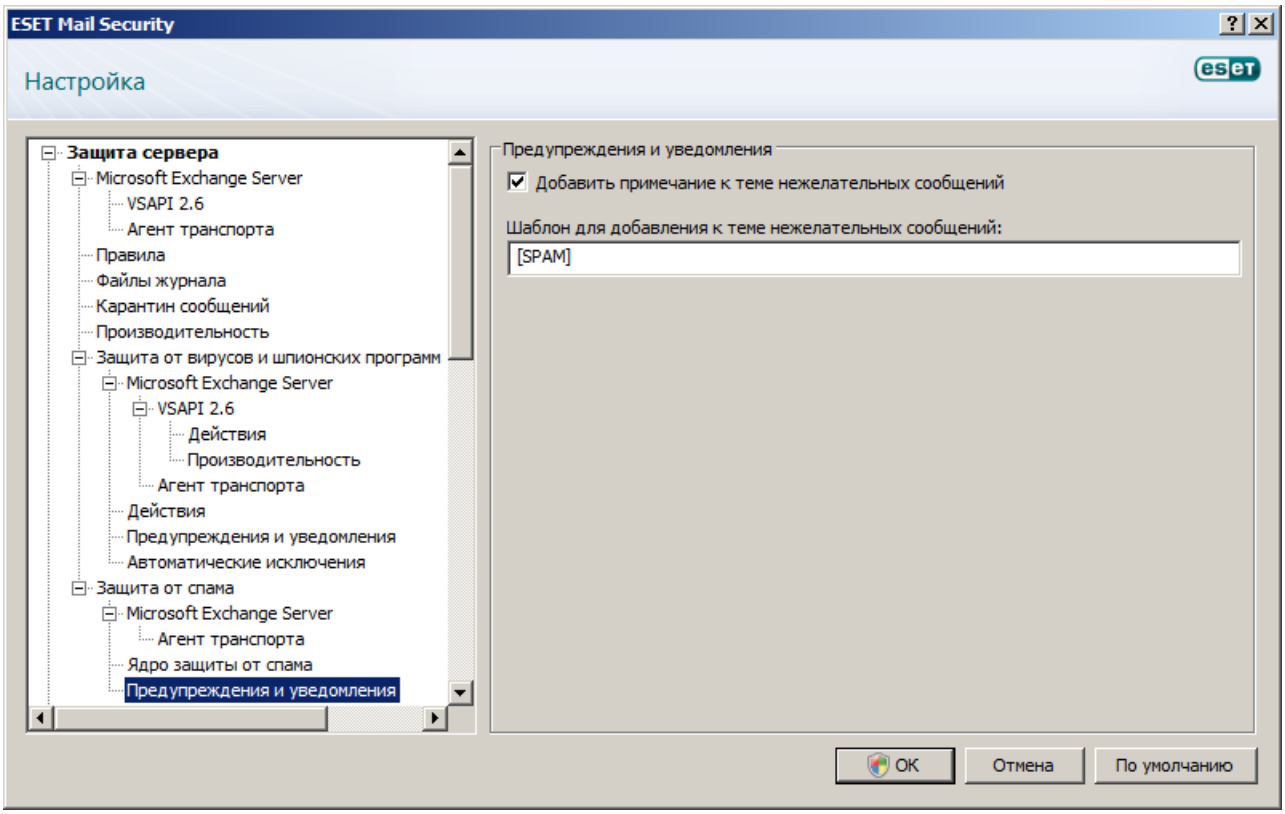
использовать файлы *approvedsenders* и *blockedsenders* как средства работы с «белым» и «черным» списками. В этих целях намного надежнее и безопаснее использовать разрешенные и заблокированные IP-адреса. Если нужно добавить отправителя в «белый» список по адресу/домену (файл *approvedsenders*), всегда следует применять дополнительный метод проверки сообщения (например, инфраструктуру политики отправителей).

Прочие параметры

enable_spf	Этот параметр включает/отключает проверку по инфраструктуре политики отправителей. Этот метод проверки проверяет общие правила домена (политику домена), чтобы определить, разрешено ли отправителю рассылать сообщения с этого домена.
enable_all_spf	Этот параметр определяет, могут ли домены, отсутствующие в параметре spf_list и файле Mailshell, обойти проверку по инфраструктуре политики отправителей. Для корректной работы этого параметра у параметра enable_realtime_spf должно быть значение «yes».
enable_realtime_spf	Если этот параметр активирован, DNS-запросы будут отправляться в режиме реального времени в ходе проверки по инфраструктуре политики отправителей. Это может негативно сказаться на производительности (задержки при оценке сообщений).
spf_list	Этот параметр позволяет назначить значимость конкретной записи инфраструктуры политики отправителей, тем самым повлияв на общую оценку нежелательности сообщения.
spf_*_weight	Символ «звездочка» (*) здесь представляет 14 возможных результатов проверки по инфраструктуре политики отправителей (дополнительные сведения см. в разделе *spamcatcher.conf*). Значение, введенное для этого параметра, представляет собой значение коррекции, которое затем применяется к оценке нежелательности в соответствии с конкретными типами результатов. Если проверка по инфраструктуре политики отправителей имеет результат «fail», будет применено значение коррекции из параметра spf_fail_weight. В зависимости от значения коррекции может увеличиться или уменьшиться итоговая оценка нежелательности.
spf_recursion_depth	Максимальная глубина вложенности (с применением механизма «include»). По норме RFC 4408 это ограничение равно 10 (для предотвращения атак типа «отказ в обслуживании»), но в некоторых записях инфраструктуры политики отправителей это ограничение больше не соблюдается, так как нужно применить большее количество уровней вложенности для выполнения запроса инфраструктуры политики отправителей.
enable_livefeed_sender_repute	Если этот параметр отключен, информация инфраструктуры политики отправителей из LiveFeed будет игнорироваться.

3.3.3 Предупреждения и уведомления

Каждое сообщение электронной почты, просканированное ESET Mail Security и помеченное как спам, может быть выделено путем добавления уведомления в тему сообщения. По умолчанию в качестве уведомления используется [*SPAM*], однако это может быть и пользовательская строка.



ПРИМЕЧАНИЕ. Также можно использовать системные переменные при добавлении шаблона в тему сообщения.

3.4 Часто задаваемые вопросы

В. После установки EMSX с модулем защиты от спама электронная почта перестала доставляться в почтовые ящики.
О. Если активирована работа с «серыми» списками, это нормально. В первые несколько часов полноценной эксплуатации сообщения электронной почты могут получаться с задержкой в несколько часов. Если проблема сохраняется в течение более длительного времени, рекомендуется отключить работу с «серыми» списками (или повторно конфигурировать).

В. Когда VSAPI сканирует вложения электронной почты, сканируется ли также тело сообщения?
О. В Microsoft Exchange Server 2000 с пакетом обновления SP2 и более поздней версии VSAPI сканирует также и тело сообщения.

В. Почему сканирование сообщений продолжается после отключения параметра VSAPI?
О. Изменения в параметры VSAPI выполняются асинхронно, то есть измененные параметры VSAPI должны быть запрошены Microsoft Exchange Server, чтобы они вступили в силу. Этот циклический процесс выполняется с интервалом примерно в одну минуту. То же относится и ко всем другим параметрам VSAPI.

В. Может ли VSAPI удалить целиком сообщение с зараженным вложением?
О. Да, VSAPI может удалить сообщение целиком. Однако для этого сначала нужно выбрать параметр **Удалить сообщение целиком** в разделе **Действия** параметров VSAPI. Этот параметр доступен в Microsoft Exchange Server версии 2003 и более поздних. Более ранние версии Microsoft Exchange Server не поддерживают удаление сообщений целиком.

В. Сканируется ли исходящая электронная почта также VSAPI на наличие вирусов?
О. Да, VSAPI сканирует исходящие сообщения электронной почты при условии, что в почтовом клиенте не сконфигурирован SMTP-сервер, отличный от Microsoft Exchange Server. Эта функция применяется в

Microsoft Exchange Server 2000 с пакетом обновления 3 и более поздних версий.

В. Можно ли добавить текст уведомления через VSAPI в каждое просканированное сообщение так же, как это делается при использовании агента транспорта?
О. Добавление текста в сообщения, просканированные VSAPI, не поддерживается в Microsoft Exchange Server.

В. Иногда я не могу открыть определенное сообщение электронной почты в Microsoft Outlook. С чем это связано?
О. Для параметра **Действие, если очистка невозможна** в параметрах VSAPI в разделе **Действия** скорее всего выбрано значение **Блокировать** или же вы создали правило, в котором используется действие **Блокировать**. При любом из этих вариантов зараженные сообщения и/или сообщения, отвечающие такому правилу, будут помечаться и блокироваться.

В. Что означает элемент **Предельное время ответа** в разделе **Производительность**?
О. Если используется Microsoft Exchange Server 2000 с пакетом обновления SP2 или более поздней версии, значение параметра **Предельное время ответа** показывает максимальное время в секундах, необходимое, чтобы завершить сканирование с помощью VSAPI одного потока. Если в течение этого времени сканирование не завершается, Microsoft Exchange Server запретит клиенту доступ к электронной почте. Сканирование не будет прервано, а по его окончании все остальные попытки получить доступ к файлу будут успешны. Если используется Microsoft Exchange Server 5.5 с пакетом обновления SP3 или SP4, это значение будет выражено в миллисекундах и представляет собой период, по окончании которого клиент повторит попытку доступа к файлу, который ранее был недоступен из-за сканирования.

В. Какой длины может быть список типов файлов в одном правиле?
О. Список расширений файлов может содержать не более 255 символов в одном правиле.

В. Я включил параметр **Фоновое сканирование** в VSAPI. До этого сообщения на сервере Microsoft Exchange Server всегда сканировались после каждого обновления базы данных сигнатур вирусов. Однако этого не случилось после последнего обновления. В чем заключается проблема?
О. Решение, следует ли сканировать все сообщения немедленно или при попытке пользователя открыть сообщение, зависит от нескольких факторов, среди которых нагрузка на сервер, время ЦП, необходимое для сканирования всех сообщений сразу, и общее количество сообщений. Microsoft Exchange Server будет сканировать каждое сообщение, прежде чем оно будет доставлено в папку «Входящие» клиента.

В. Почему значение счетчика правила увеличилось больше чем на единицу после получения одного сообщения?
О.Правила проверяются для сообщения во время его обработки агентом транспорта или VSAPI. Когда активирован и агент транспорта, и VSAPI, а сообщение отвечает условиям правила, счетчик может быть увеличен для правила на 2 и даже больше. VSAPI обращается к каждой части сообщения по отдельности (тело, вложение), то есть правила последовательно применяются к каждой из таких частей. Кроме того, правила также могут применяться во время фонового сканирования (например, повторное сканирование хранилища почтового ящика после обновления базы данных сигнатур вирусов), что также может увеличивать значение счетчика.

В. Совместимо ли программное обеспечение ESET Mail Security 4 для Microsoft Exchange Server с интеллектуальным фильтром сообщений?
О. Да, программное обеспечение ESET Mail Security 4 для Microsoft Exchange Server (EMSX) совместимо с интеллектуальным фильтром сообщений. В случае, если сообщение оценивается как спам, оно обрабатывается следующим образом.

- Если для модуля защиты от спама ESET Mail Security активирован параметр **Удалить сообщение** (или **Направить сообщение на карантин**), действие будет выполнено вне зависимости от того действия, которое настроено в интеллектуальном фильтре сообщений Microsoft Exchange.
- Если для модуля защиты от спама ESET Mail Security выбран вариант **Ничего не предпринимать**, будут использоваться параметры интеллектуального фильтра сообщений Microsoft Exchange и выполняться соответствующее действие (например, удаление, отклонение, архивация…). Должен быть активирован параметр **Записывать вероятность нежелательной почты в просканированные сообщения на основе оценки нежелательности** (в разделе **Защита сервера > Microsoft Exchange Server > Транспортный агент**), чтобы эта функция корректно работала.

В. Как настроить ESET Mail Security на перемещение нежелательных сообщений в выбранную пользователем папку спама Microsoft Outlook?
О. Использование параметров по умолчанию ESET Mail Security приводит к тому, что нежелательные сообщения хранятся в Microsoft Outlook в папке **Нежелательная почта**. Для включения этой функциональности установите флажок **Записать оценку нежелательности в заголовок просканированного сообщения** (в разделе **F5 > Защита сервера > Защита от спама > Microsoft Exchange Server > Транспортный агент**). Если нежелательные сообщения нужно хранить в другой папке, ознакомьтесь с приведенными далее инструкциями.

1) В ESET Mail Security
- Отключите параметр **Записать оценку нежелательности в заголовок просканированного сообщения**.
- Выберите **Ничего не предпринимать** в качестве действия для сообщений, помеченных как спам.
- Задайте текст, который будет добавляться к нежелательным сообщениям, например «[SPAM]» (в разделе **Защита сервера > Защита от спама > Предупреждения и уведомления**).

2) В Microsoft Outlook
- Настройте правило, чтобы сделать так, чтобы сообщения с определенным текстом в теме («[SPAM]») перемещались в выбранную папку.

В. В статистике защиты от спама многие сообщения находятся в категории **Не сканировалось**. Какая электронная почта не сканируется модулем защиты от спама?
О. В категории **Не сканировалось** есть следующие подкатегории.
Общие:
- Все сообщения, которые были просканированы, когда защита от спама была отключена на любом из уровней (почтовый сервер, агент транспорта).

Microsoft Exchange Server 2003:
- Все сообщения, поступающие с **IP-адреса**, который присутствует в интеллектуальном фильтре сообщений **глобального списка разрешенных адресов**.
- Сообщения от прошедших аутентификацию отправителей.

Microsoft Exchange Server 2007:
- Все сообщения, отправленные в пределах организации (все они будут сканироваться модулем защиты от вирусов).
- Сообщения от прошедших аутентификацию отправителей.
- Сообщения от пользователей, для которых выполнено конфигурирование на обход защиты от спама.
- Все сообщения, отправленные в почтовый ящик, для которого включен параметр **AntispamBypass**.
- Все сообщения от отправителей из списка **Надежные отправители**.

ПРИМЕЧАНИЕ. Адреса, перечисленные в «белом» списке и параметрах ядра защиты от спама, не попадают в категорию **Не сканировалось**, так как эта группа состоит исключительно из сообщений, которые никогда не обрабатывались модулем защиты от спама.

В. Пользователи загружают сообщения в свои почтовые клиенты по протоколу POP3 (в обход Microsoft Exchange Server), но почтовые ящики хранятся на сервере Microsoft Exchange Server. Будут ли такие сообщения электронной почты сканироваться модулями защиты от вирусов и защиты от спама ESET Mail Security?
О. При такой конфигурации ESET Mail Security будет сканировать сообщения электронной почты, хранящиеся на сервере Microsoft Exchange Server, только на наличие вирусов (через VSAPI). Сканирование модулем защиты от спама выполняться не будет, так как для этого нужен SMTP-сервер.

В. Можно ли задать значение оценки нежелательности, которое должно быть у сообщения, чтобы оно классифицировалось как спам?
О. Да, это ограничение можно задать в ESET Mail Security версии 4.3 и более поздних (см. главу Настройка параметров ядра защиты от спама 41).

В. Сканирует ли модуль защиты от спама ESET Mail Security также сообщения, которые загружаются через соединитель POP3?
О. Сообщения, загружаемые через соединитель POP3, сканируются на наличие спама только в SBS 2008.

4. ESET Mail Security — защита сервера

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

4.1 Защита от вирусов и шпионских программ

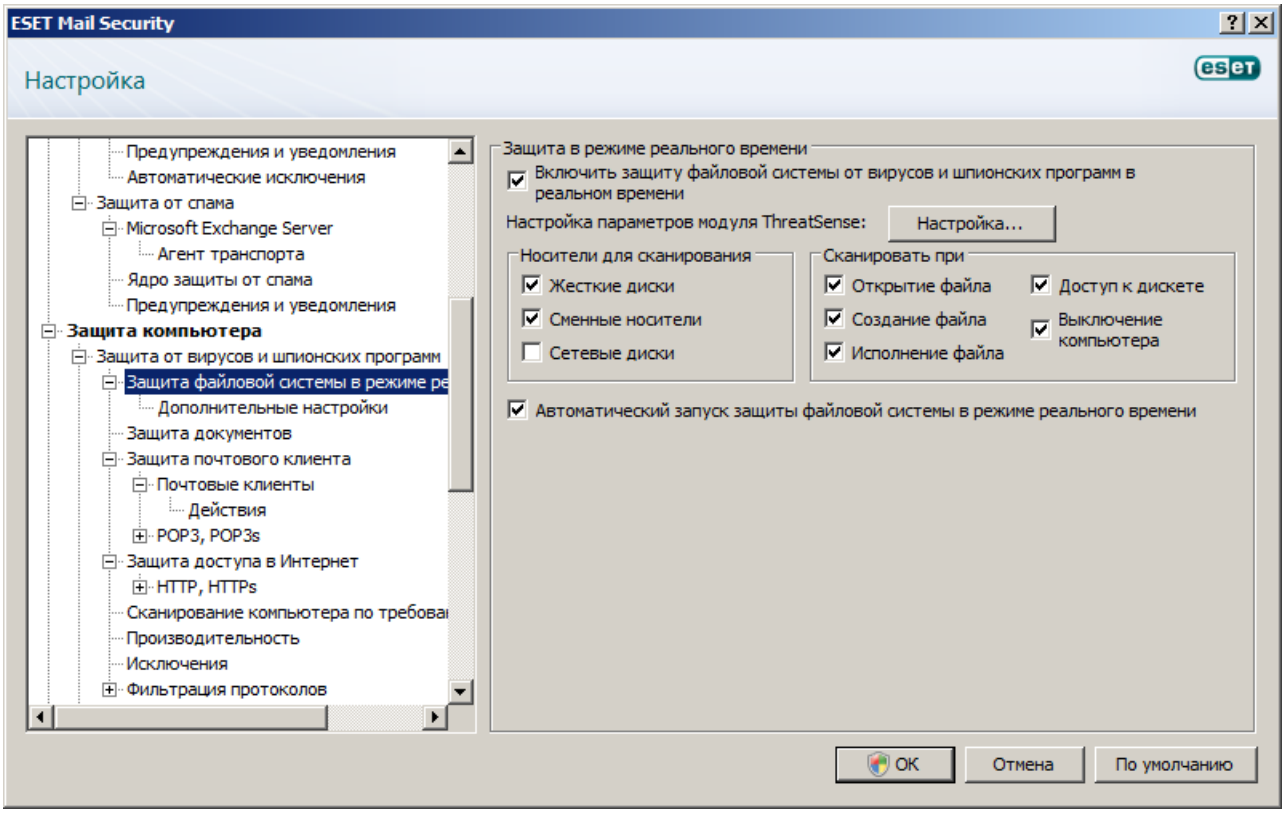
Защита от вирусов предотвращает вредоносные атаки на компьютер путем контроля файлов, электронной почты и связи через Интернет. Если обнаруживается содержащая злонамеренный код угроза, модуль защиты от вирусов может обезвредить ее, сначала заблокировав, а затем очистив, удалив или переместив на карантин.

4.1.1 Защита в режиме реального времени

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

4.1.1.1 Настройка управления

Защита файловой системы в режиме реального времени проверяет все типы носителей, причем контроль активируется различными событиями. За счет использования методов обнаружения ThreatSense (как описано в разделе Настройка параметров модуля ThreatSense 65) защита файловой системы в режиме реального времени может быть разной для вновь создаваемых и уже существующих файлов. Для вновь созданных файлов возможно применение более глубокого уровня контроля.
Для снижения влияния на производительность компьютера при использовании защиты в режиме реального времени файлы, которые уже сканировались, не сканируются повторно, пока не будут изменены. Файлы сканируются повторно сразу после каждого обновления базы данных сигнатур вирусов. Такое поведение конфигурируется с использованием оптимизации Smart. Если она отключена, все файлы сканируются каждый раз при доступе к ним. Для изменения этого параметра откройте окно «Дополнительные настройки» и нажмите **Защита от вирусов и шпионских программ** > **Защита файловой системы в режиме реального времени** в дереве расширенных параметров. Затем нажмите кнопку **Настройка...** рядом с пунктом **Настройка параметров модуля ThreatSense**, нажмите **Другое** и установите или снимите флажок **Включить оптимизацию Smart**.
По умолчанию защита в режиме реального времени запускается при загрузке системы и обеспечивает непрерывное сканирование. В особых случаях (например, в случае конфликта с другим модулем сканирования в режиме реального времени) защиту файловой системы в режиме реального времени можно отключить, сняв флажок **Автоматический запуск защиты файловой системы в режиме реального времени**.



4.1.1.1.1 Носители для сканирования

По умолчанию на наличие возможных угроз сканируются все типы носителей.
Жесткие диски: проверяются все жесткие диски, существующие в системе.
Съемные носители: дискеты, USB-устройства хранения и т. п.
Сетевые диски: сканируются все сопоставленные диски.
Рекомендуется оставить параметры по умолчанию, а изменять их только в особых случаях (например, если сканирование определенных носителей приводит к значительному замедлению обмена данными).

4.1.1.1.2 Сканировать при (сканирование по событию)

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.
Параметр **Доступ к дискете** позволяет контролировать загрузочный сектор дискеты, когда открывается такой диск. Параметр **Выключение компьютера** обеспечивает проверку загрузочных секторов жесткого диска при выключении компьютера. Хотя загрузочные вирусы в настоящее время встречаются редко, рекомендуется оставить эти флажки установленными, так как по-прежнему существует вероятность заражения таким вирусом из альтернативного источника.

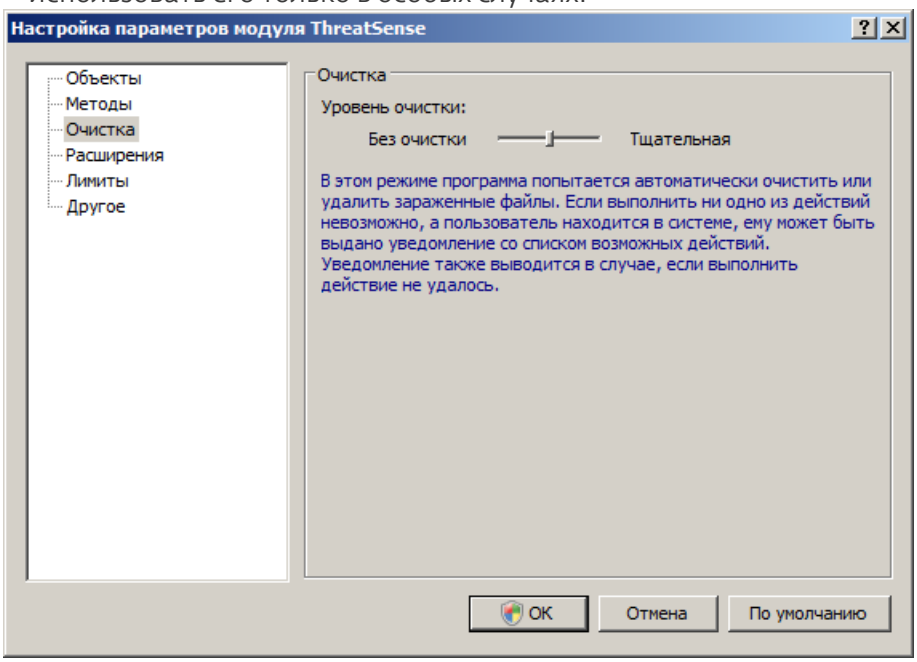
4.1.1.1.3 Расширенные параметры сканирования

Более подробную настройку можно выполнить в разделе **Защита компьютера** > **Защита от вирусов и шпионских программ** > **Защита в режиме реального времени** > **Дополнительные настройки**.
Дополнительные параметры модуля ThreatSense для новых и измененных файлов: вероятность заражения вновь созданных или измененных файлов выше по сравнению с существующими файлами. Именно поэтому программа проверяет эти файлы с дополнительными параметрами сканирования. Вместе с обычными методами сканирования, основанными на базе данных сигнатур вирусов, применяется расширенная эвристика, что значительно улучшает уровень обнаружения. В дополнение ко вновь созданным файлам выполняется также сканирование самораспаковывающихся файлов (.sfx) и упаковщиков (исполняемых файлов с внутренним сжатием). По умолчанию проверяются архивы с глубиной вложенности до 10 независимо от их фактического размера. Для изменения параметров сканирования архивов снимите флажок «Параметры сканирования архива по умолчанию».
Дополнительные параметры модуля ThreatSense.Net для исполняемых файлов: по умолчанию расширенная эвристика не применяется при исполнении файлов. Однако в некоторых случаев этот параметр может быть нужно включить (установив флажок **Расширенная эвристика запуска файлов**). Обратите внимание, что расширенная эвристика может замедлить выполнение некоторых программ из-за повышения системных требований.

4.1.1.2 Уровни очистки

Защита в режиме реального времени предусматривает три уровня очистки. Для выбора уровня очистки нажмите кнопку **Настройка...** в разделе **Защита файловой системы в режиме реального времени**, а затем выберите ветвь **Очистка**.

- При первом уровне, **Без очистки**, для каждого найденного заражения на экран выводится окно предупреждения с доступными для него действиями. Пользователь должен выбрать действие для каждого заражения отдельно. Этот уровень предназначен для более опытных пользователей, которые знают о действиях, которые следует предпринимать в случае заражения.
- При уровне по умолчанию автоматически выбирается и выполняется предварительно определенное действие (в зависимости от типа заражения). Обнаружение и удаление зараженных файлов сопровождается сообщением, выводимым в правом нижнем углу экрана. Автоматические действия не выполняются при обнаружении заражения в архиве (в котором также содержатся незараженные файлы), а также в случаях, когда для зараженных объектов нет предварительно заданного действия.
- Третий уровень, **Тщательная очистка**, является наиболее агрессивным: все зараженные объекты очищаются. Так как использование этого уровня может привести к потере нужных файлов, рекомендуется использовать его только в особых случаях.



4.1.1.3 Момент изменения конфигурации защиты в режиме реального времени

Защита в режиме реального времени является самой важной составляющей, необходимой для обеспечения безопасности компьютера. Поэтому необходимо быть внимательным при изменении ее параметров. Рекомендуется изменять параметры только в особых случаях. Например, при возникновении конфликтов с какими-либо приложениями или модулями сканирования в режиме реального времени других программ защиты от вирусов.
После установки ESET Mail Security все параметры оптимизированы для обеспечения максимального уровня безопасности системы для пользователей. Для восстановления параметров по умолчанию нажмите кнопку **По умолчанию**, расположенную в правом нижнем углу окна **Защита файловой системы в режиме реального времени** (**Дополнительные настройки** > **Защита от вирусов и шпионских программ** > **Защита файловой системы в режиме реального времени**).

4.1.1.4 Проверка защиты в режиме реального времени

Для проверки того, что защита в режиме реального времени действительно работает и обнаруживает вирусы, используйте проверочный файл eicar.com. Это специальный безвредный тестовый файл, который обнаруживается всеми программами защиты от вирусов. Файл создан компанией EICAR (Европейский институт антивирусных компьютерных исследований) для проверки функционирования программ защиты от вирусов. Файл eicar.com доступен для загрузки с веб-сайта http://www.eicar.org/download/eicar.com.
ПРИМЕЧАНИЕ. Перед осуществлением проверки защиты в режиме реального времени необходимо отключить файервол. Если файервол включен, он обнаружит данный файл и предотвратит его загрузку.

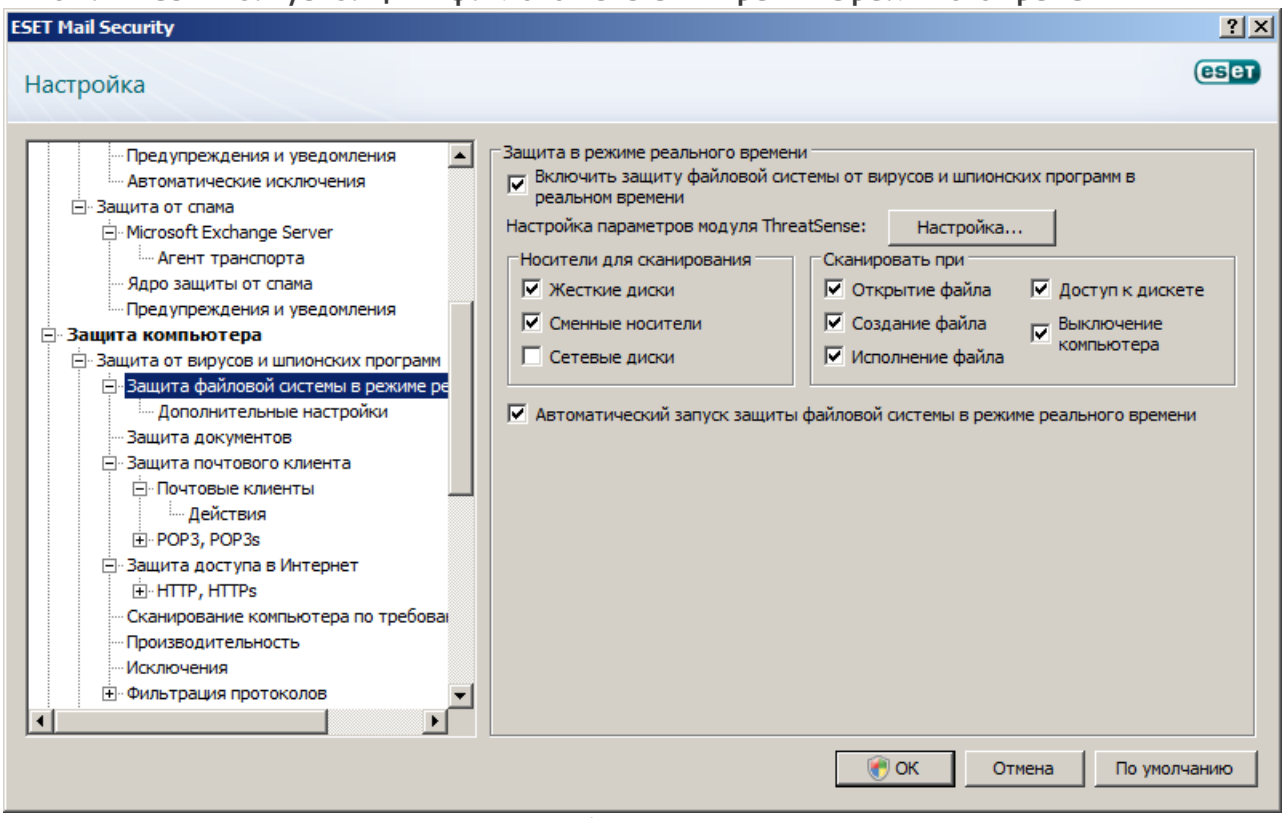
4.1.1.5 Решение проблем, возникающих при работе защиты файловой системы в режиме реального времени

В следующей главе рассказывается о проблемах, которые могут возникать при работе защиты в режиме реального времени, и о том, как их устранить.

Защита файловой системы в режиме реального времени отключена

Если защита в режиме реального времени непреднамеренно была отключена пользователем, ее нужно повторно активировать. Чтобы повторно активировать защиту файловой системы в режиме реального времени, в главном окне программы перейдите в раздел **Настройка** > **Защита от вирусов и шпионских программ** и щелкните ссылку **Включить защиту файловой системы в режиме реального времени**.

Если защита файловой системы в режиме реального времени не запускается при загрузке операционной системы, возможно, снят флажок **Автоматический запуск защиты файловой системы в режиме реального времени**. Чтобы установить этот флажок, перейдите в раздел «Дополнительные настройки» (F5) и нажмите **Защита файловой системы в режиме реального времени** в дереве расширенных параметров. Проверьте, что в разделе **Дополнительные настройки** в нижней части этого окна установлен флажок **Автоматический запуск защиты 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 в режиме реального времени могут возникнуть конфликты. Рекомендуется удалить все прочие программы защиты от вирусов с компьютера.

Защита в режиме реального времени на запускается

Если защита в режиме реального времени не запускается при загрузке операционной системы, но флажок **Автоматический запуск защиты файловой системы в режиме реального времени** установлен, возможно, возник конфликт с другими программами. В этом случае обратитесь за консультацией к специалистам службы поддержки клиентов ESET.

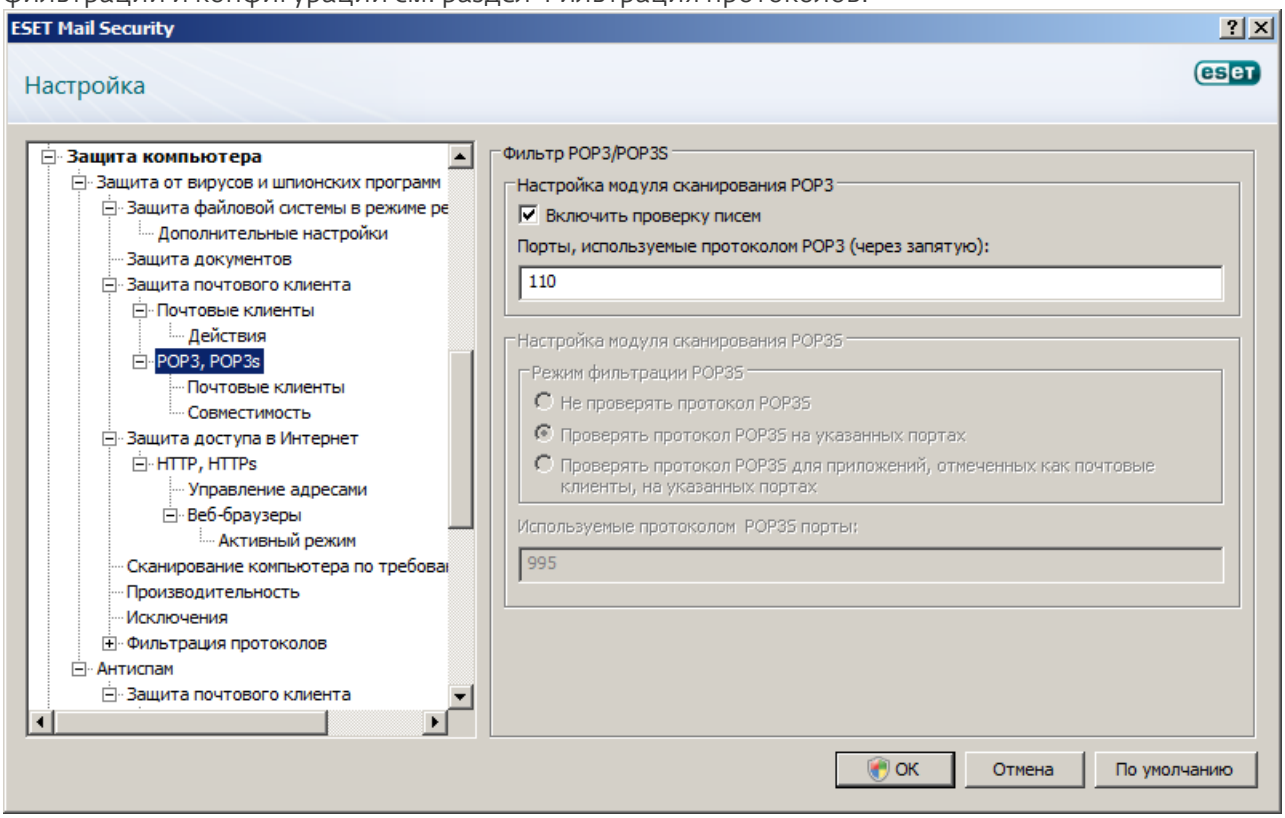
4.1.2 Защита почтового клиента

Защита электронной почты обеспечивает контроль обмена данными по электронной почте через протокол POP3. При использовании подключаемого модуля для Microsoft Outlook ESET Mail Security позволяет контролировать весь обмен данными, осуществляемый почтовым клиентом (по протоколам POP3, MAPI, IMAP, HTTP).

При проверке входящих сообщений программа использует все современные методы сканирования, обеспечиваемые модулем сканирования ThreatSense. Это позволяет обнаруживать вредоносные программы даже до того, как данные о них попадают в базу данных сигнатур вирусов. Сканирование соединений по протоколу POP3 не зависит от используемого почтового клиента.

4.1.2.1 Проверка POP3

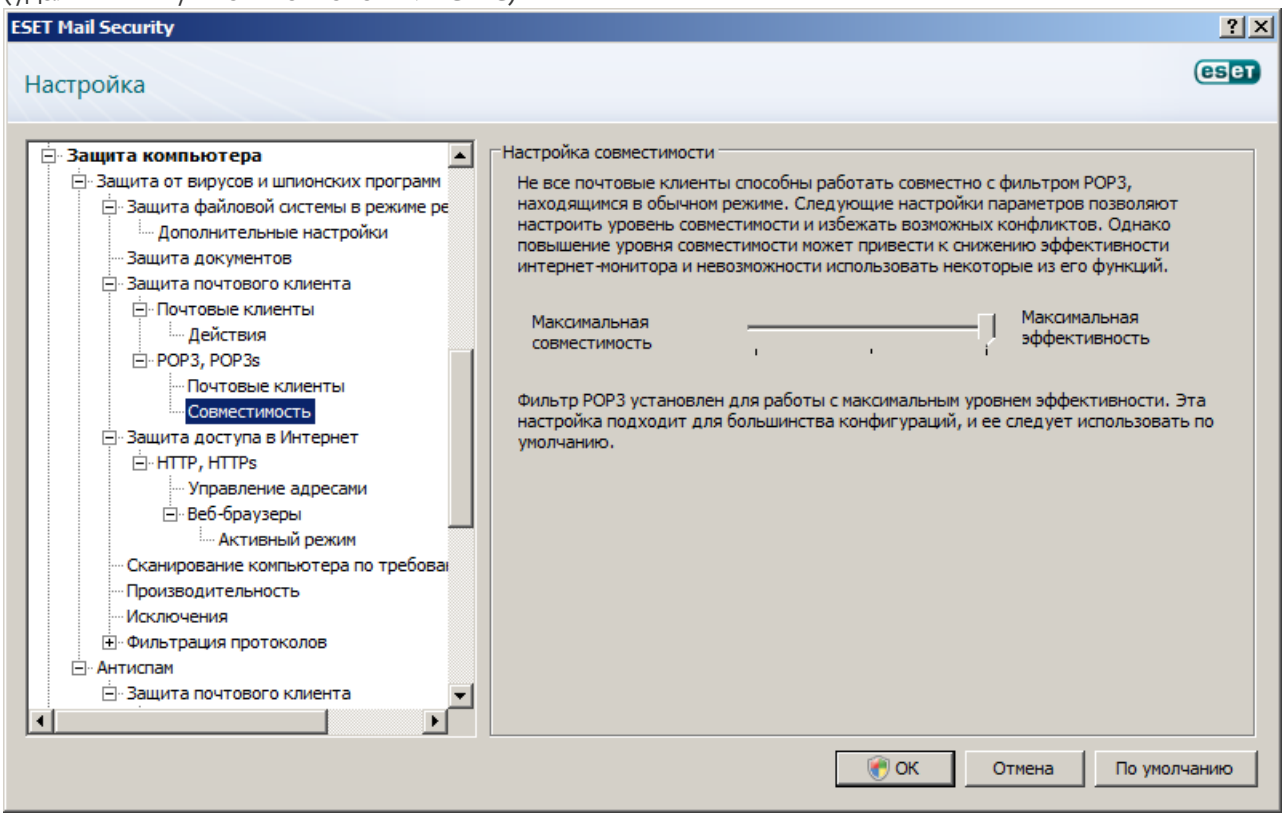
POP3 — самый распространенный протокол, используемый для получения электронной почты в почтовых клиентах. ESET Mail Security обеспечивает защиту этого протокола вне зависимости от используемого почтового клиента.
Модуль защиты, обеспечивающий эту функцию, автоматически инициируется при запуске операционной системы и остается активным в оперативной памяти. Для нормальной работы модуля убедитесь в том, что он включен. Проверка протокола POP3 осуществляется автоматически без необходимости в какой-либо дополнительной настройке конкретного почтового клиента. По умолчанию сканируются все соединения по порту 110, однако при необходимости могут быть добавлены и другие порты. Номера портов следует разделять запятыми.
Зашифрованное соединение не проверяется.
Для использования фильтрации протокола POP3/POP3S сначала нужно включить фильтрацию протоколов. Если параметры POP3/POP3S недоступны, перейдите в раздел **Защита компьютера** > **Защита от вирусов и шпионских программ** > **Фильтрация протоколов** из дерева расширенных параметров и установите флажок **Включить фильтрацию содержимого протоколов приложений**. Дополнительные сведения о фильтрации и конфигурации см. раздел Фильтрация протоколов.



4.1.2.1.1 Совместимость

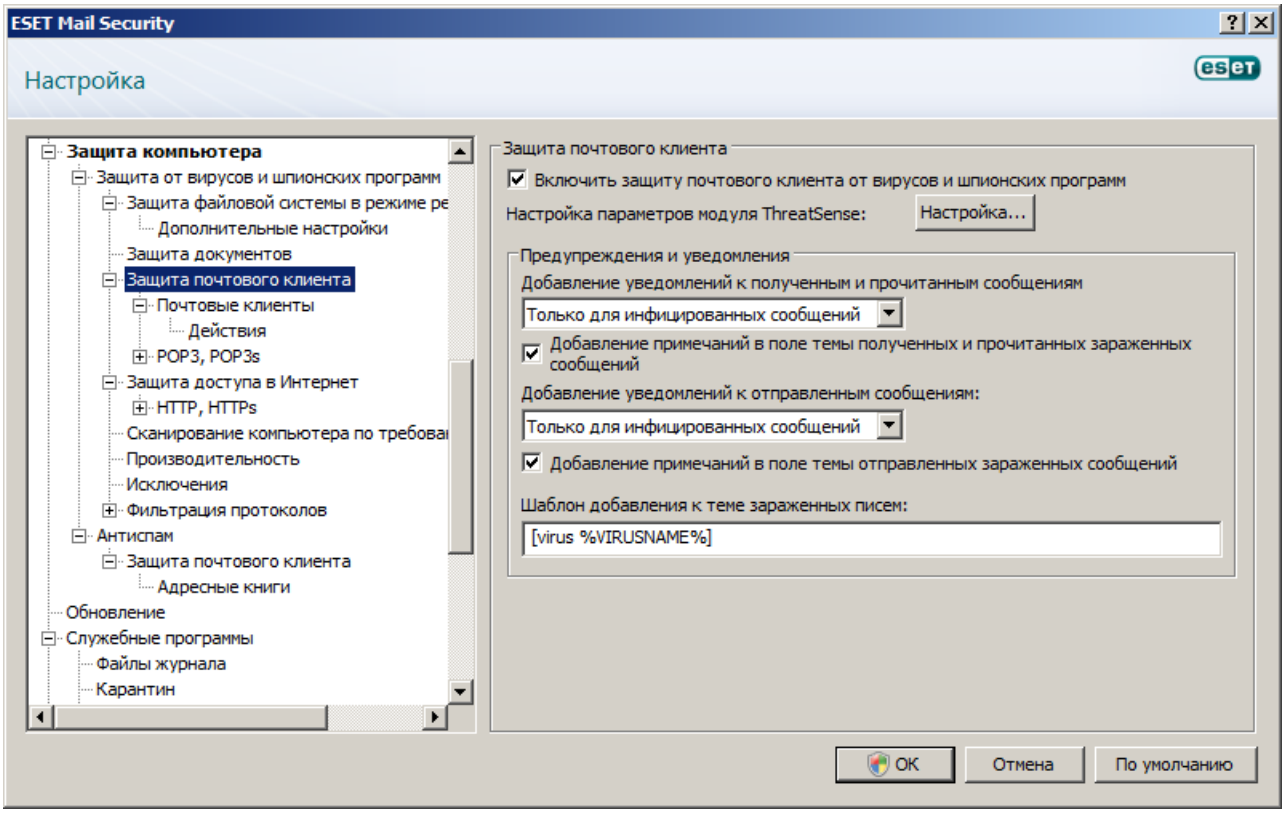
В некоторых программах для работы с электронной почтой могут возникать проблемы с фильтрацией POP3 (например, при медленном соединении с сервером в процессе получения сообщений могут возникать ошибки времени ожидания). В этом случае попробуйте изменить способ контроля трафика. Снижение уровня контроля может улучшить скорость процесса очистки. Для настройки уровня контроля при фильтрации POP3 из дерева расширенных параметров перейдите в раздел **Защита от вирусов и шпионских программ** > **Защита электронной почты** > **POP3, POP3s** > **Совместимость**.
Если используется вариант **Максимальная эффективность**, заражения удаляются из зараженных сообщений, а перед исходной темой сообщения вставляется информация о заражении (должен быть активирован вариант **Удалить** или **Очистить** или использоваться уровень очистки **Тщательная** или **По умолчанию**).
Режим **средней совместимости** изменяет способ получения сообщений. Сообщение постепенно отправляются в почтовый клиент. После передачи сообщения оно сканируется для выявления заражений. Однако при использовании такого уровня контроля возрастает риск заражения. Уровень очистки и применение уведомлений (текстовой информации, прикрепляемой к теме или телу сообщений) остаются теми же, что и для режима максимальной эффективности.
В режиме **максимальной совместимости** на экран выводится окно предупреждения, в котором пользователь информируется о получении зараженного сообщения. Никакая информация о зараженных файлах не добавляется в тему или тело доставленных сообщений, а заражения не удаляются автоматически

(удалять их нужно в почтовом клиенте).



4.1.2.2 Интеграция с почтовыми клиентами

Интеграция ESET Mail Security с почтовыми клиентами увеличивает уровень активной защиты от вредоносного кода в сообщениях электронной почты. Если используемый почтовый клиент поддерживается, такую интеграцию можно настроить в ESET Mail Security. Если интеграция активирована, панель инструментов защиты от спама ESET Mail Security вставляется непосредственно в почтовый клиент, обеспечивая более эффективную защиту электронной почты. Параметры интеграции доступны в разделе **Настройка** > **Ввод всего дерева расширенных параметров...** > **Разное** > **Интеграция с почтовыми клиентами**. Интеграция с почтовыми клиентами позволяет активировать интеграцию с поддерживаемыми почтовыми клиентами. В настоящий момент поддерживаются следующие почтовые клиенты: Microsoft Outlook, Outlook Express, почта Windows, почта Windows Live и Mozilla Thunderbird.
Установите флажок **Отключить проверку при изменении содержимого папки "Входящие"**, если при работе с почтовым клиентом наблюдается замедление работы системы. Такая ситуация может возникнуть при загрузке электронной почты из Kerio Outlook Connector Store.
Защита электронной почты активируется в разделе **Настройка** > **Ввод всего дерева расширенных параметров...** > **Защита от вирусов и шпионских программ** > **Защита почтового клиента**, где нужно выбрать вариант **Включить защиту почтового клиента от вирусов и шпионских программ**.



4.1.2.2.1 Добавление уведомлений в тело сообщения электронной почты

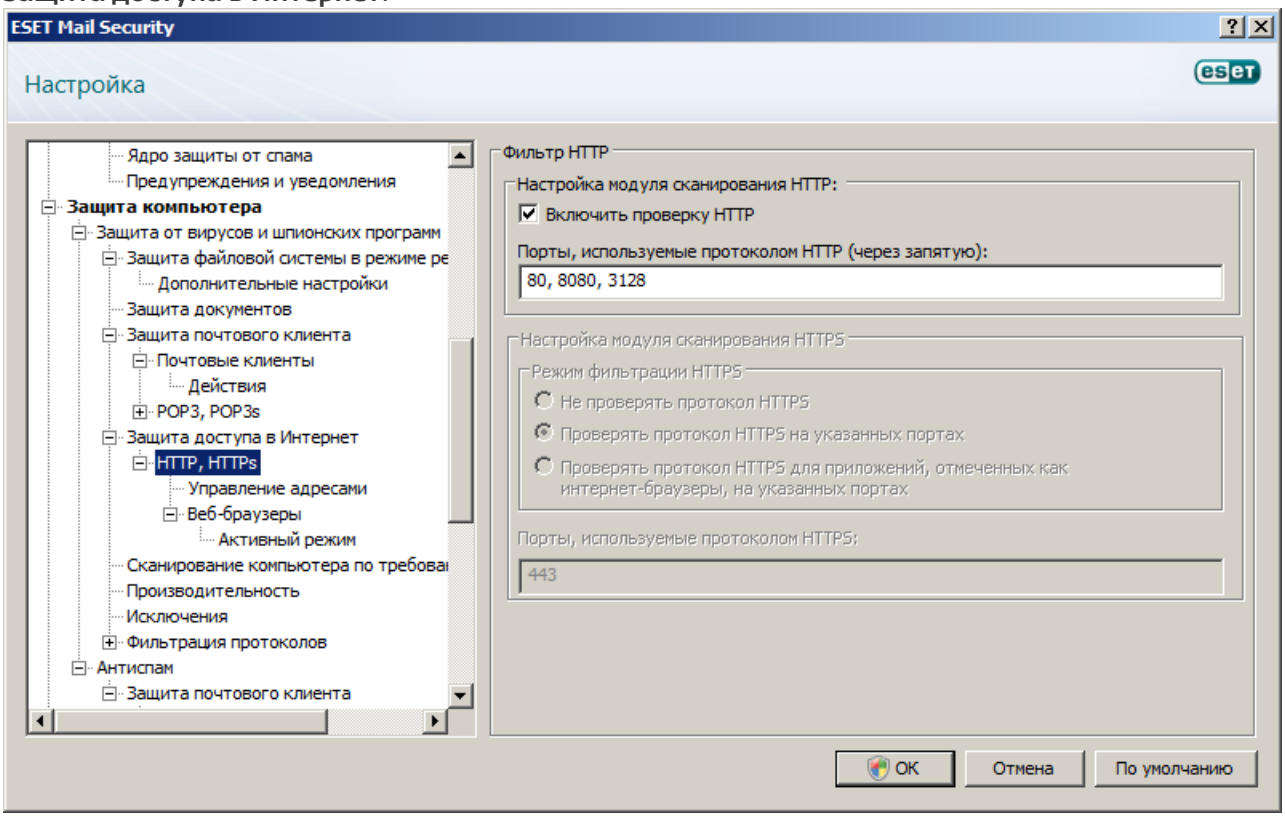
Каждое сообщение электронной почты, просканированное ESET Mail Security, может быть помечено путем добавления уведомления в тему или тело сообщения. Эта функция повышает уровень доверия для получателя, а в случае обнаружения заражения предоставляет важную информацию об уровне угрозы для конкретного сообщения или отправителя.
Параметры для этой функции настраиваются в разделе **Дополнительные настройки** > **Защита от вирусов и шпионских программ** > **Защита почтового клиента**. Можно выбрать вариант **Добавление уведомлений к полученным и прочитанным сообщениям**, а также **Добавление уведомлений к отправленным сообщениям**. Также можно решить, следует ли добавлять уведомления ко всем просканированным сообщениям электронной почты, только к зараженным сообщениям или же не добавлять их вовсе.
ESET Mail Security также позволяет добавлять сообщения к исходной теме зараженного сообщения. Для активации добавления к теме установите и флажок **Добавление примечаний в поле темы полученных и прочитанных зараженных сообщений**, и флажок **Добавление примечаний в поле темы отправленных зараженных сообщений**.
Содержимое уведомлений можно изменять в поле **Шаблон добавления к теме зараженных писем**.
Описанные выше изменения могут помочь автоматизировать процесс фильтрации зараженных сообщений, а также позволяют помещать сообщения с определенной темой (если эта функция поддерживается используемым почтовым клиентом) в отдельную папку.

4.1.2.3 Удаление заражений

При получении зараженного сообщения электронной почты на экран выводится окно предупреждения. В этом окне содержатся имя отправителя, адрес его электронной почты и название заражения. В нижней части окна доступны варианты действий для обнаруженного объекта: **Очистить**, **Удалить** или **Пропустить**. Почти во всех случаях рекомендуется выбирать **Очистить** или **Удалить**. В некоторых ситуациях, если нужно получить зараженный файл, можно выбрать **Пропустить**.
Если включена **тщательная очистка**, на экран будет выведено информационное окно, в котором нельзя выбрать какое-либо действие.

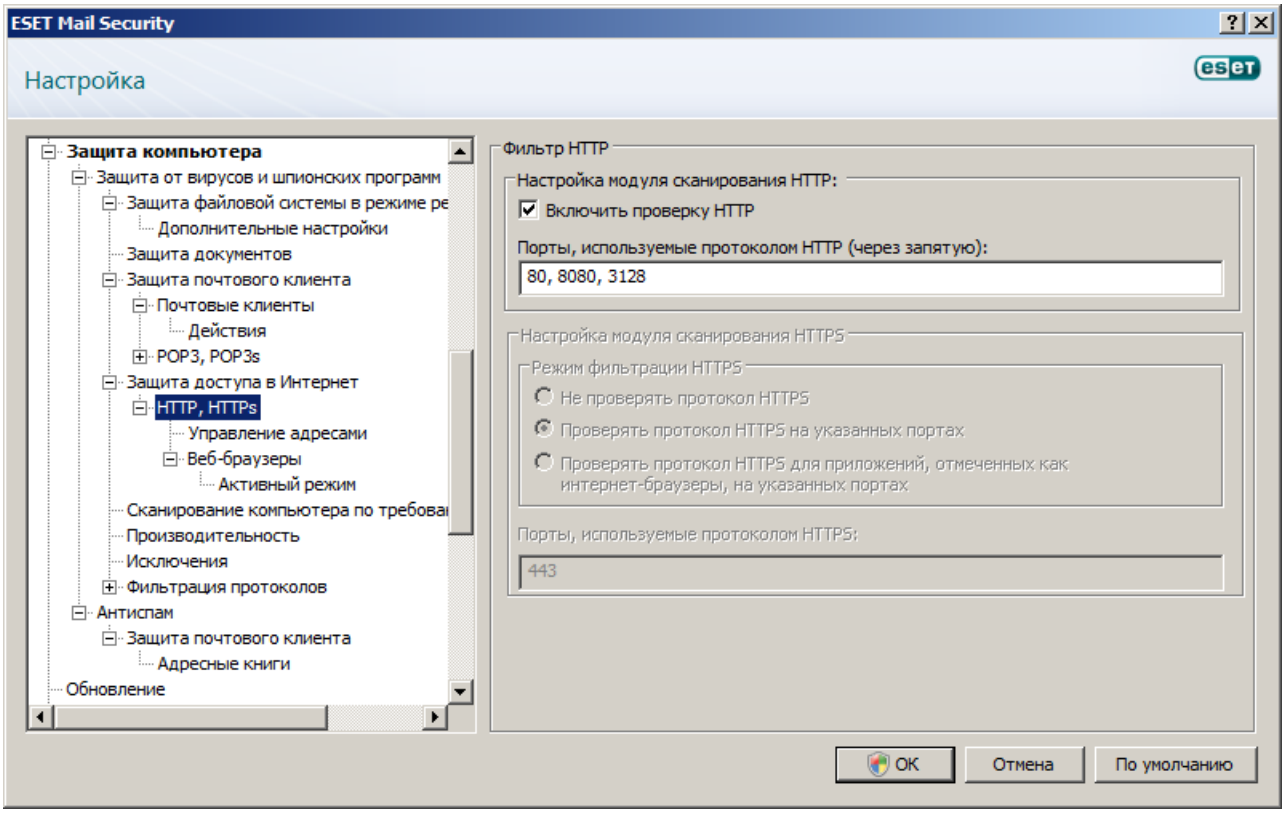
4.1.3 Защита доступа в Интернет

Подключение к Интернету стало стандартной функцией персонального компьютера. К сожалению, Интернет также стал и основной средой распространения злонамеренного кода. Поэтому принципиально важно уделить особое внимание защите доступа в Интернет. Настоятельно рекомендуется установить флажок **Включить защиту интернет-соединения от вирусов и шпионских программ**. Этот параметр находится в разделе **Дополнительные настройки** (F5) > **Защита от вирусов и шпионских программ** > **Защита доступа в Интернет**.



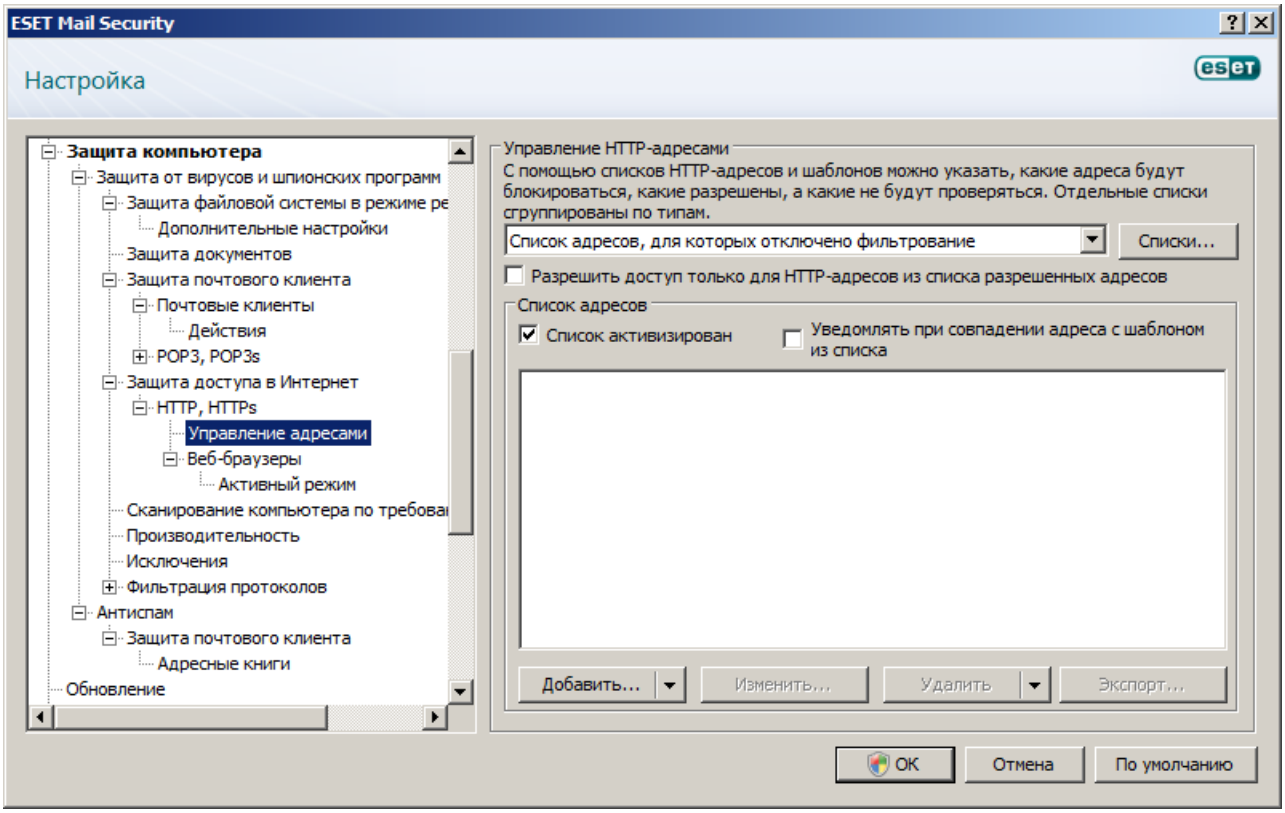
4.1.3.1 HTTP, HTTPs

Защита доступа в Интернет работает путем отслеживания соединений между веб-браузерами и удаленными серверами в соответствии с правилами протоколов HTTP и HTTPS. По умолчанию программа ESET Mail Security сконфигурирована на использование стандартов большинства веб-браузеров. Однако параметры модуля сканирования HTTP можно изменить в разделе **Дополнительные настройки** (F5) > **Защита от вирусов и шпионских программ** > **Защита доступа в Интернет** > **HTTP, HTTPS**. В главном окне фильтрации HTTP можно установить или снять флажок **Включить проверку HTTP**. Также можно указать номера портов, используемых для передачи данных по протоколу HTTP. По умолчанию предварительно заданы номера портов 80, 8080 и 3128. Проверка HTTPs может выполняться в следующих режимах.
Не проверять протокол HTTPS: зашифрованные соединения не будут проверяться.
Проверять протокол HTTPs для выбранных портов: проверка протокола HTTPs выполняется только для портов, указанных в параметре **Порты, используемые протоколом HTTPS**.



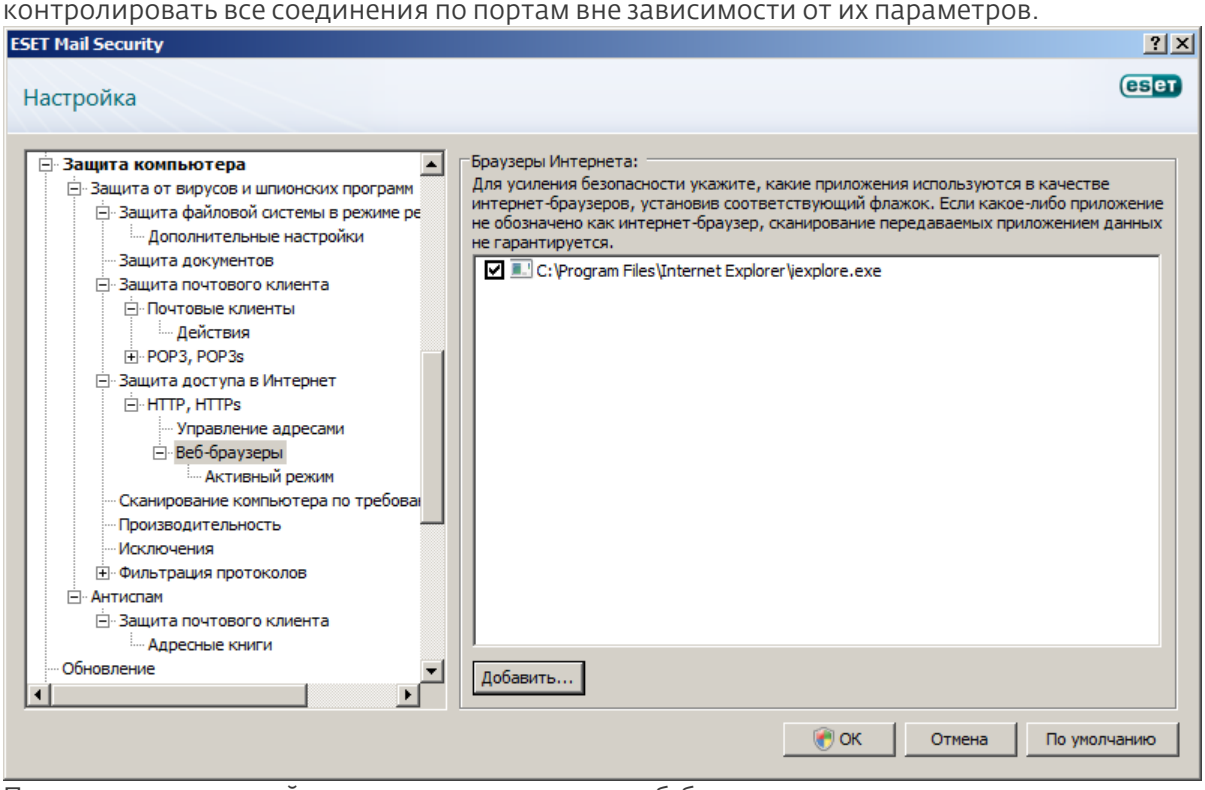
4.1.3.1.1 Управление адресами

В этом разделе можно задавать HTTP-адреса, которые будут блокироваться, разрешаться или исключаться из проверки. Кнопки **Добавить...**, **Изменить...**, **Удалить** и **Экспорт...** позволяют управлять списками адресов. Веб-сайты из списка заблокированных адресов будут недоступны. Веб-сайты из списка исключенных адресов загружаются без сканирования на наличие вредоносного кода. Если выбрать вариант **Разрешить доступ только для HTTP-адресов из списка разрешенных адресов**, будут доступны только адреса из списка разрешенных, а остальные HTTP-адреса будут заблокированы.
Во всех списках можно использовать символы шаблона «*» (звездочка) и «?» (вопросительный знак). Символ звездочки обозначает любую последовательность символов, а вопросительный знак — любой символ. Работать с содержимым списка исключенных адресов следует особенно аккуратно, так как он должен содержать только доверенные и безопасные адреса. Точно так же нужно убедиться в том, что символы шаблона в этом списке используются правильно. Чтобы активировать список, установите флажок **Список активизирован**. Для получения уведомлений при загрузке адреса из текущего списка установите флажок **Уведомлять при применении адреса из списка**.



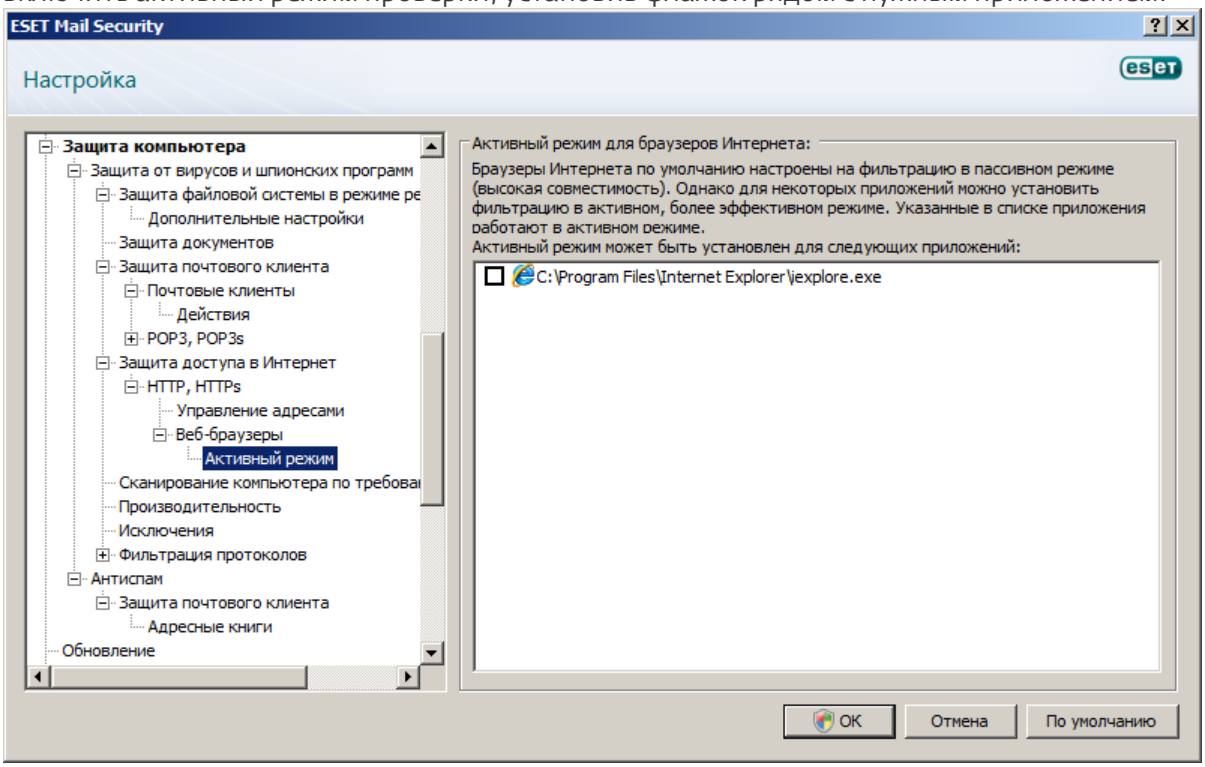
4.1.3.1.2 Активный режим

В программе ESET Mail Security также есть функция, которая дает пользователю возможность указать, является ли конкретное приложение браузером. Если приложение помечено как браузер, все соединения, осуществляемые этим приложением, отслеживаются вне зависимости от используемых портов. Функция веб-браузеров дополняет функцию проверки протокола HTTP, так как проверка HTTP выполняется только для предварительно определенных портов. Однако многие веб-службы используют изменяющиеся или неизвестные номера портов. Именно из этих соображений функция веб-браузеров позволяет контролировать все соединения по портам вне зависимости от их параметров.



Перечень приложений, помеченных в качестве веб-браузеров, можно просмотреть непосредственно в подменю **Веб-браузеры** ветви **HTTP, HTTPs**. В этом разделе также есть подменю **Активный режим**, которое определяет режим проверки для веб-браузеров.
Функция **Активный режим** удобна, так как позволяет проверять все передаваемые данные в целом. Если она отключена, соединения приложений отслеживаются частями в пакетном режиме. Это снижает эффективность процесса проверки данных, но при этом обеспечивает лучшую совместимость для

перечисленных приложений. Если при использовании функции не возникает проблем, рекомендуется включить активный режим проверки, установив флажок рядом с нужным приложением.

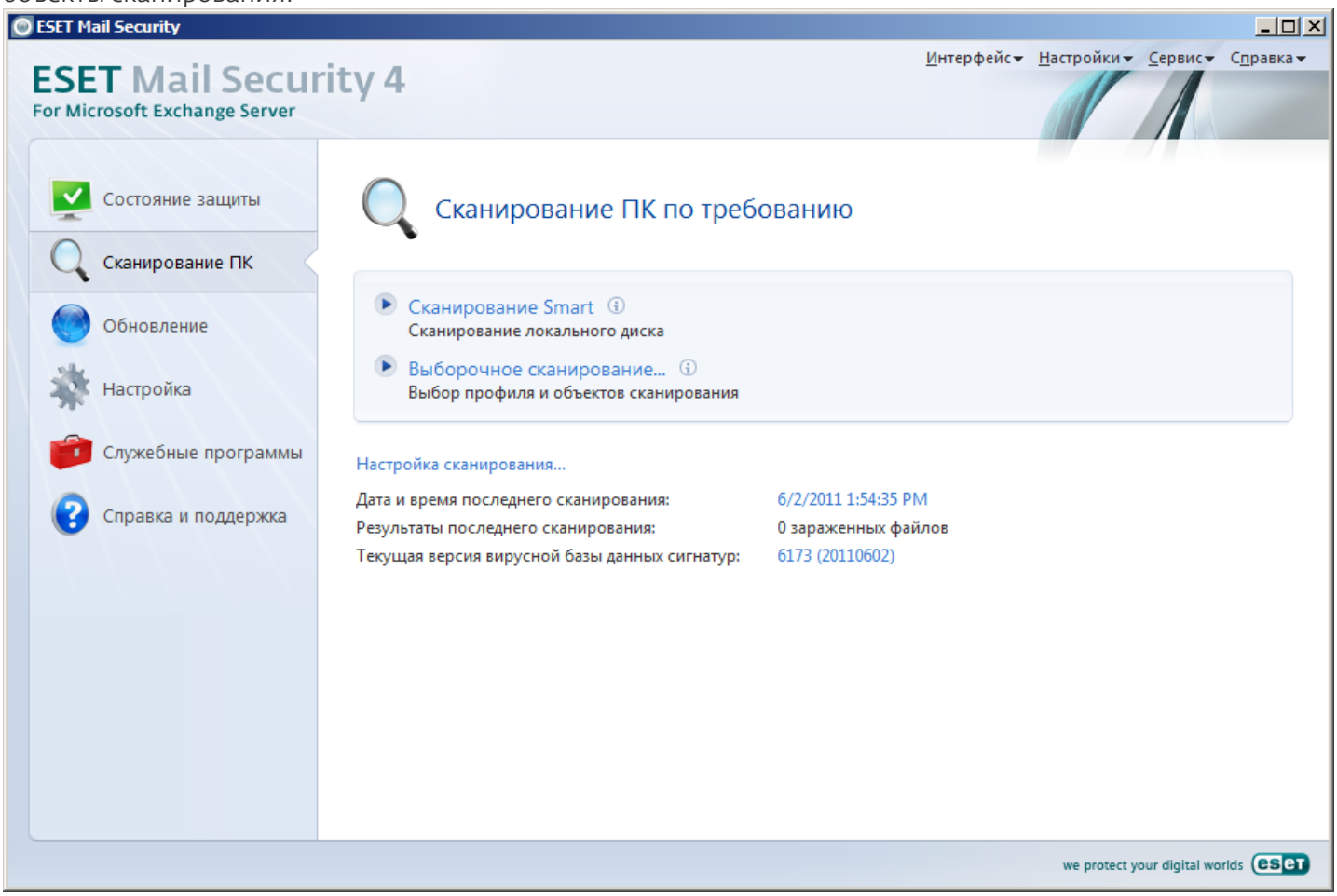


4.1.4 Сканирование ПК по требованию

При наличии подозрения, что компьютер заражен (необычное поведение и т. п.), следует выполнить сканирование компьютера по требованию для проверки наличия заражений. С точки зрения обеспечения безопасности принципиально важно выполнять сканирование компьютера регулярно, а не только при возникновении подозрений. Регулярное сканирование позволяет обнаружить заражения, пропущенные модулем сканирования в режиме реального времени при их записи на диск. Это может произойти, если модуль сканирования в режиме реального времени был отключен или использовалась устаревшая база данных сигнатур вирусов.
Рекомендуется запускать сканирование компьютера по требованию хотя бы раз в месяц. Можно сконфигурировать сканирование в качестве запланированной задачи в разделе **Служебные программы** > **Планировщик**.

4.1.4.1 Тип сканирования

Существует два типа сканирования компьютера по требованию. **Сканирование Smart** позволяет быстро просканировать систему без настройки каких-либо параметров. **Выборочное сканирование...** дает возможность выбрать любой предопределенный профиль сканирования, а также указать конкретные объекты сканирования.



4.1.4.1.1 Сканирование Smart

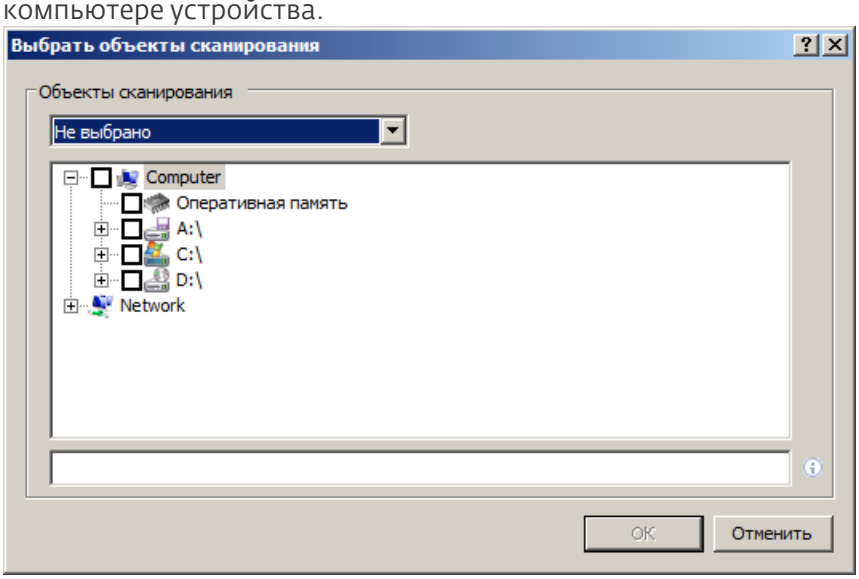
Сканирование Smart позволяет быстро запустить сканирование компьютера и очистить зараженные файлы без вмешательства пользователя. Главным преимуществом этого метода является простота использования без подробной настройки сканирования. При сканировании Smart проверяются все файлы на локальных дисках и автоматически очищаются или удаляются обнаруженные заражения. В качестве уровня очистки автоматически выбран уровень по умолчанию. Дополнительную информацию о типах очистки см. в разделе Очистка 67.

4.1.4.1.2 Выборочное сканирование

Выборочное сканирование является оптимальным решением в том случае, когда нужно указать параметры сканирования, такие как объекты и методы сканирования. Преимуществом выборочного сканирования является возможность подробного конфигурирования параметров. Конфигурации можно сохранять в виде пользовательских профилей сканирования, которые удобно использовать, если регулярно выполняется сканирование с одними и теми же параметрами.
Для выбора объектов сканирования перейдите в раздел **Сканирование компьютера** > **Выборочное сканирование** и выберите один из вариантов из раскрывающегося меню **Объекты сканирования** или конкретные объекты сканирования в древовидной структуре. Объекты сканирования также можно задать более точно, указав пути к папкам и файлам, которые нужно сканировать. Если нужно только выполнить сканирование системы без дополнительных действий по очистке, установите флажок **Сканировать без очистки**. Кроме того, можно выбрать один из трех уровней очистки в разделе **Настройка...** > **Очистка**.

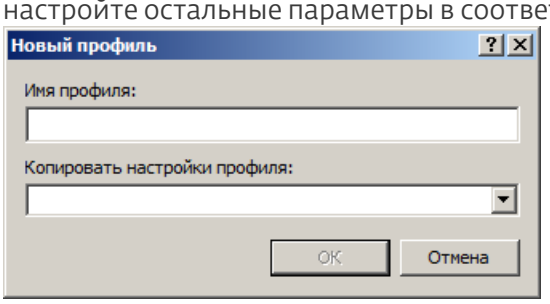
4.1.4.2 Объекты сканирования

В раскрывающемся меню объектов сканирования можно выбрать файлы, папки и устройства (диски), которые нужно сканировать на наличие вирусов.
По параметрам профиля : выбираются объекты, заданные в данном профиле сканирования.
Съемные носители : выбираются дискеты, USB-устройства хранения, компакт- и DVD-диски.
Жесткие диски : выбираются все жесткие диски, существующие в системе.
Сетевые диски : выбираются все подключенные сетевые диски.
Ничего не выбирать: отменяется выбор объектов.
Объекты сканирования можно задать более точно, введя путь к папкам или файлам, подлежащим сканированию. Выберите объекты сканирования в древовидной структуре, содержащей все доступные на компьютере устройства.



4.1.4.3 Профили сканирования

Предпочтительные параметры сканирования можно сохранить для использования в дальнейшем. Рекомендуется создать отдельный профиль для каждого регулярно используемого сканирования (с различными объектами, методами сканирования и прочими параметрами).
Для создания нового профиля откройте окно «Дополнительные настройки» (F5) и нажмите **Сканирование ПК по требованию** > **Профили...** В окне **Профили конфигурации** есть раскрывающееся меню, в котором перечисляются существующие профили сканирования, а также есть возможность создать новый. Для создания профиля сканирования в соответствии с конкретными потребностями см. раздел Настройка параметров модуля ThreatSense 65, где описывается каждый параметр, используемый для настройки сканирования.
ПРИМЕР. Предположим, пользователю требуется создать собственный профиль сканирования, причем конфигурация сканирования Smart частично устраивает его, но не нужно сканировать упаковщики или потенциально опасные приложения, но при этом нужно применить **тщательную очистку**. В окне **Профили конфигурации** нажмите кнопку **Добавить...**. Введите имя создаваемого профиля в поле **Имя профиля**, а затем выберите **Сканирование Smart** в раскрывающемся меню **Копировать настройки профиля**. Затем настройте остальные параметры в соответствии со своими потребностями.



4.1.5 Производительность

В этом разделе можно задать количество модулей сканирования ThreatSense, которые следует использовать для сканирования на наличие вирусов. Большее количество модулей сканирования ThreatSense на многопроцессорных компьютерах может увеличить скорость сканирования. Приемлемы значения в диапазоне от 1 до 20.

ПРИМЕЧАНИЕ. Внесенные в этом разделе изменения будут применены только после перезапуска.

4.1.6 Фильтрация протоколов

Защита от вирусов протоколов приложений POP3 и HTTP обеспечивается модулем сканирования ThreatSense, в котором объединены все современные методы сканирования для выявления вредоносных программ. Контроль осуществляется автоматически вне зависимости от используемого веб-браузера и почтового клиента. Для фильтрации протоколов доступны перечисленные далее варианты (если установлен флажок **Включить фильтрацию содержимого протоколов приложений**).
Порты HTTP и POP3: сканирование ограничивается соединениями по известным портам, используемым протоколами HTTP и POP3.
Приложения, классифицированные как браузеры Интернета и почтовые клиенты: установите этот флажок, чтобы фильтровать только соединения для приложений, помеченных в качестве браузеров (**Защита доступа в Интернет** > **HTTP, HTTPS** > **Веб-браузеры**) или почтовых клиентов (**Защита почтового клиента** > **POP3, POP3s** > **Почтовые клиенты**).
Порты и приложения, классифицированные как браузеры Интернета или почтовые клиенты: и порты, и браузеры проверяются на наличие вредоносных программ.
ПРИМЕЧАНИЕ. Начиная с ОС Windows Vista с пакетом обновления 1 и Windows Server 2008, используется новый метод фильтрации соединений. Из-за этого раздел «Фильтрация протоколов» недоступен.

4.1.6.1 SSL

ESET Mail Security позволяет проверять инкапсулированные в SSL протоколы. Можно использовать различные режимы сканирования для защищенных SSL соединения, при которых используются доверенные сертификаты, неизвестные сертификаты или сертификаты, исключенные из проверки защищенных SSL соединений.
Всегда сканировать протокол SSL: выберите этот вариант, чтобы сканировать все защищенные SSL соединения за исключением защищенных сертификатами, исключенными из проверки. Если устанавливается новое соединение, использующее неизвестный заверенный сертификат, пользователь получит об этом соответствующее уведомление, а само соединение автоматически будет фильтроваться. При доступе к серверу с ненадежным сертификатом, который помечен пользователем в качестве доверенного (добавлен в список доверенных сертификатов), соединение с этим сервером разрешается, а содержимое канала связи фильтруется.
Запрашивать о новых сайтах (возможна настройка исключений): при выполнении входа на новый защищенный SSL сайт (с неизвестным сертификатом) на экран выводится диалоговое окно выбора. Этот режим позволяет создавать список сертификатов SSL, которые будут исключены из сканирования.
Не сканировать протокол SSL: если выбран этот параметр, программа не будет сканировать соединения по протоколу SSL.
Если сертификат невозможно проверить, используя хранилище доверенных корневых сертификатов сертифицирующих органов (**Фильтрация протоколов** > **SSL** > **Сертификаты**), выполняется одно из следующих действий.
Запрашивать действительность сертификата: пользователю предлагается выбрать действие.
Блокировать соединения, использующие сертификат: соединение с сайтом, использующим данный сертификат, разрывается.
Если сертификат недействителен или поврежден (**Фильтрация протоколов** > **SSL** > **Сертификаты**), выполняется одно из следующих действий.
Запрашивать действительность сертификата: пользователю предлагается выбрать действие.
Блокировать соединения, использующие сертификат: соединение с сайтом, использующим данный сертификат, разрывается.

4.1.6.1.1 Доверенные сертификаты

В дополнение к встроенному хранилищу доверенных корневых сертификатов сертифицирующих органов , где программой ESET Mail Security хранятся доверенные сертификаты, можно также создать собственный список доверенных сертификатов, доступный в разделе **Дополнительные настройки** (F5) > **Фильтрация протоколов** > **SSL** > **Сертификаты** > **Доверенные сертификаты**.

4.1.6.1.2 Исключенные сертификаты

В разделе «Исключенные сертификаты» перечислены сертификаты, которые считаются безопасными. Содержимое зашифрованных соединений, использующих сертификаты из данного списка, не будет проверяться на наличие угроз. Рекомендуется исключать только те веб-сертификаты, которые гарантированно являются безопасными, а соединение с их использованием не нуждается в проверке.

4.1.7 Настройка параметров модуля ThreatSense

ThreatSense — это технология, объединяющая ряд сложных методов обнаружения угроз. Эта технология является упреждающей, т. е. она защищает от новой угрозы уже в первые часы ее распространения. При этом используется сочетание нескольких методов (анализ кода, моделирование кода, обобщенные сигнатуры, сигнатуры вирусов), которые совместно значительно повышают уровень безопасности компьютера. Модуль сканирования может контролировать несколько потоков данных одновременно, что делает эффективность и количество обнаруживаемых угроз максимальными. Технология ThreatSense также успешно уничтожает руткиты.
Для технологии ThreatSense можно настроить несколько параметров сканирования:

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

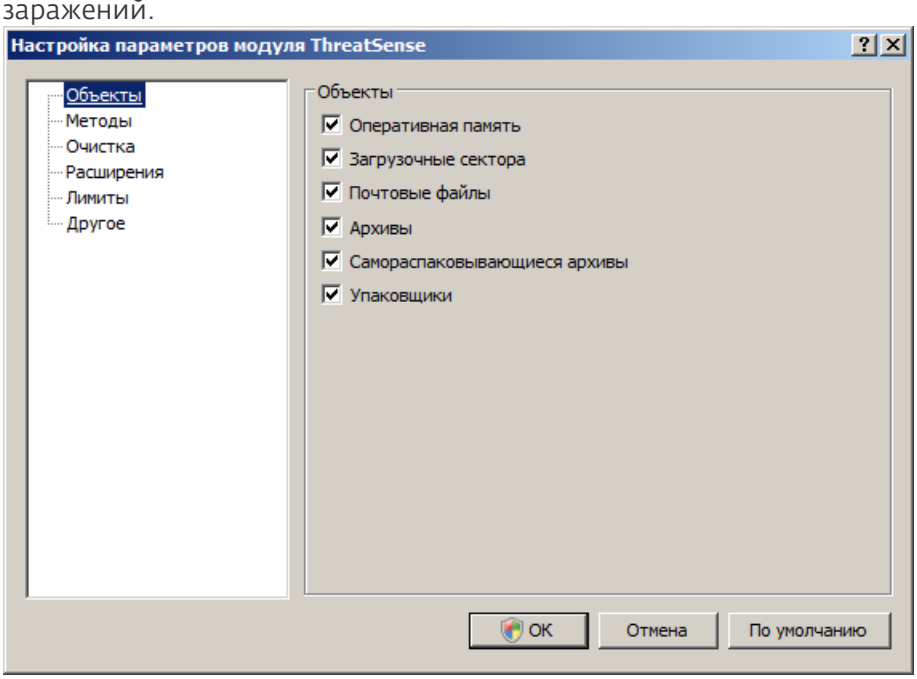
Для того чтобы открыть окно параметров, нажмите кнопку **Настройка...** в окне параметров любого модуля, использующего технологию ThreatSense (см. ниже). Разные сценарии обеспечения безопасности требуют различных настроек, поэтому технологию ThreatSense можно настроить отдельно для каждого из перечисленных далее модулей защиты.

- Защита файловой системы в режиме реального времени 51
- Проверка файлов, исполняемых при запуске системы
- Защита электронной почты 54
- Защита доступа в Интернет 58
- Сканирование ПК по требованию 61

Параметры ThreatSense хорошо оптимизированы для каждого из модулей, а их изменение ведет к существенным изменениям в поведении системы. Например, изменение параметров так, чтобы всегда сканировались упаковщики, или включение расширенной эвристики в модуле защиты файловой системы в режиме реального времени, может замедлить работу системы (обычно только новые файлы сканируются с применением этих методов). В связи с этим рекомендуется не изменять параметры ThreatSense по умолчанию ни для каких модулей, кроме модуля «Сканирование ПК по требованию».

4.1.7.1 Настройка объектов

В разделе **Объекты** можно указать компоненты и файлы, которые должны сканироваться на наличие заражений.

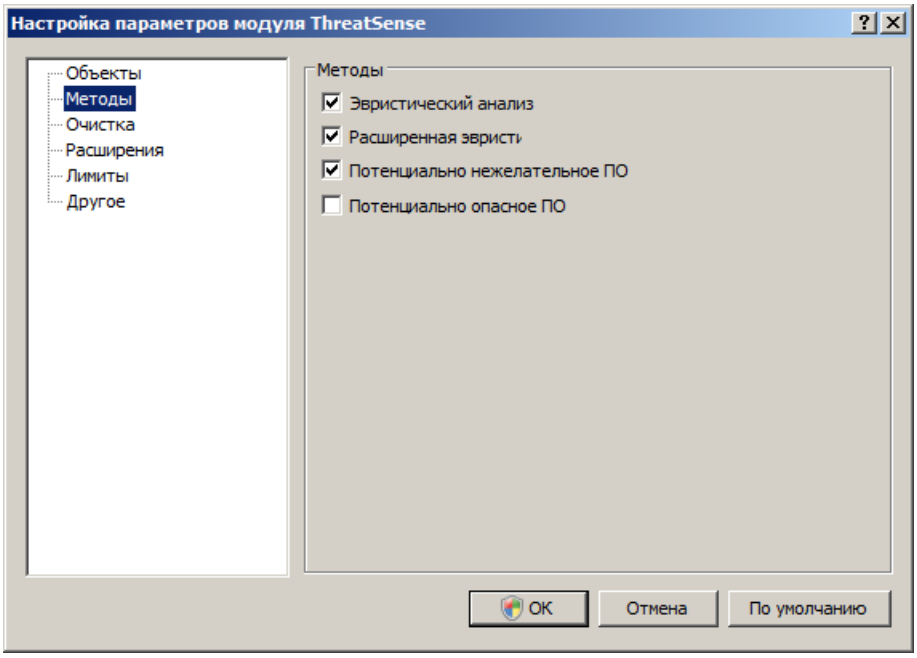


Оперативная память: выполняется сканирование на наличие угроз, которые атакуют оперативную память системы.
Загрузочные секторы: загрузочные секторы сканируются на наличие вирусов в основной загрузочной записи.
Файлы: сканируются файлы всех часто используемых типов (программы, изображения, звуковые и видеофайлы, файлы баз данных и т. д.).
Почтовые файлы: сканируются особые файлы, в которых хранятся сообщения электронной почты.
Архивы: сканируются сжатые файлы в архивах .rar, .zip, .arj, .tar и т. д.
Самораспаковывающиеся архивы: сканируются файлы, запакованные в самораспаковывающихся архивах, которые обычно имеют расширение .exe.
Упаковщики: сканируются упаковщики, которые в отличие от стандартных архивов распаковывают файлы динамически в системную память, и стандартные статические упаковщики (UPX, yoda, ASPack, FGS и т. д.).

4.1.7.2 Параметры

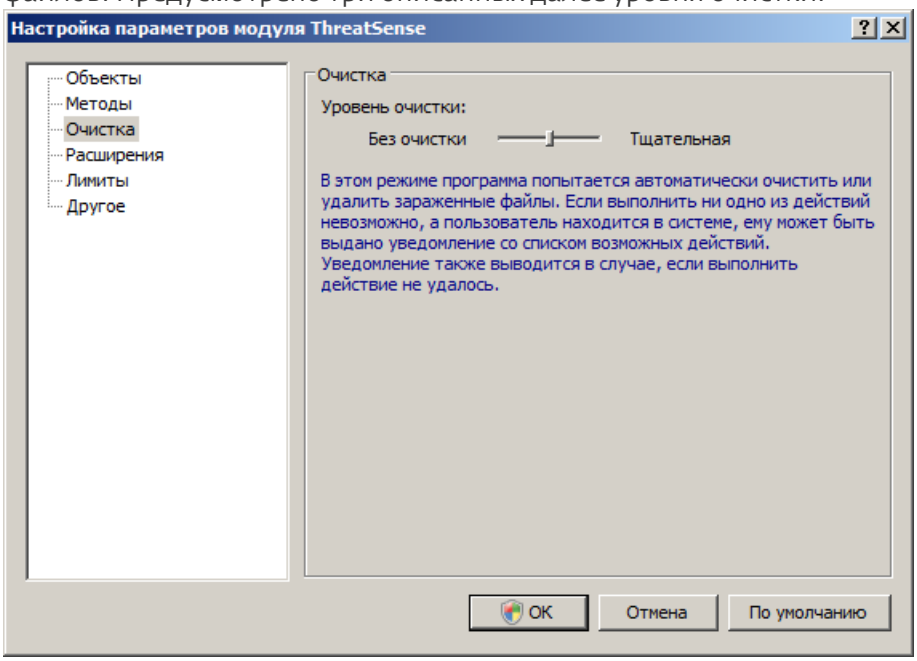
В разделе **Параметры** можно выбрать методы, которые будут использоваться при сканировании системы на наличие заражений. Доступны следующие варианты:
Сигнатуры: сигнатуры представляют собой надежный и точный метод обнаружения и выявления заражений по имени с применением базы данных сигнатур вирусов.
Эвристика: при эвристическом анализе используются алгоритмы, которые анализируют вредоносную активность программ. Основным преимуществом обнаружения путем эвристического анализа является возможность обнаруживать новые вредоносные программы, сведения о которых еще не попали в список известных вирусов (базу данных сигнатур вирусов).
Расширенная эвристика: расширенная эвристика представляет собой уникальный эвристический алгоритм, разработанный компанией ESET и оптимизированный для обнаружения компьютерных червей и троянских программ, написанных на языках программирования высокого уровня. Расширенная эвристика значительно увеличивает возможности программы по обнаружению.
Рекламное/шпионское/опасное ПО: к этой категории относится программное обеспечение, которое собирает различную конфиденциальную информацию о пользователях без их согласия. Также к ней относится программное обеспечение, выводящее на экран рекламные материалы.
Потенциально нежелательное ПО: потенциально нежелательные приложения не обязательно являются вредоносными, но могут негативно влиять на производительность системы. Обычно для установки таких приложений запрашивается согласие пользователя. После их установки поведение системы изменяется (по сравнению с тем, как она вела себя до установки этих приложений). Наиболее существенные изменения связаны с возникновением нежелательных всплывающих окон, запуском и работой скрытых процессов, увеличением уровня использования системных ресурсов, изменениями результатов поиска и обменом данными с удаленными серверами.
Потенциально опасное ПО: к потенциально опасным приложениям относится нормальное коммерческое программное обеспечение. Это в том числе средства удаленного доступа. По умолчанию этот параметр

отключен.



4.1.7.3 Очистка

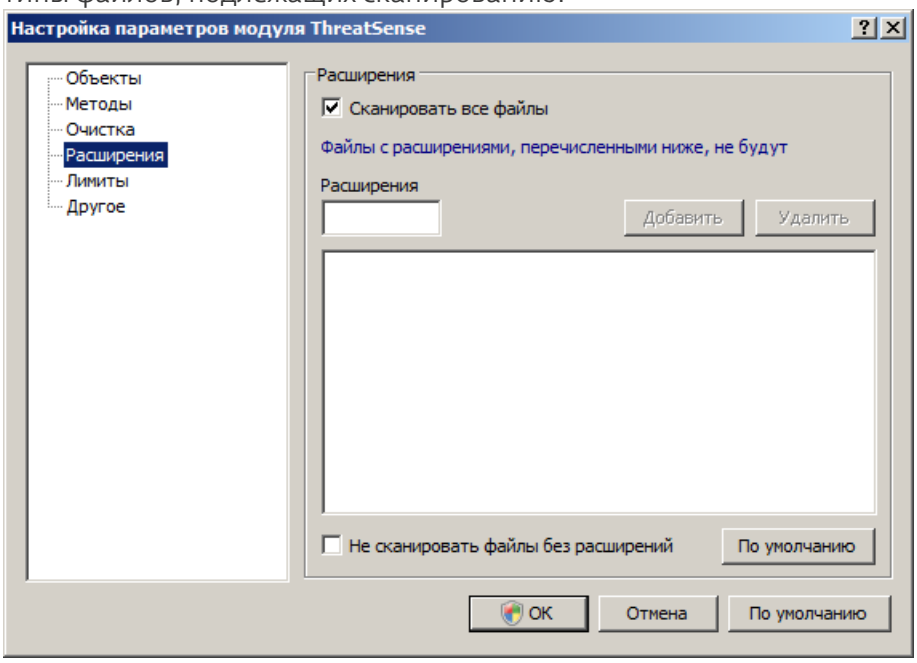
Параметры процесса очистки определяют поведение модуля сканирования при очистке зараженных файлов. Предусмотрено три описанных далее уровня очистки.



Без очистки: зараженные файлы не очищаются автоматически. Программа выводит на экран предупреждение и предлагает пользователю выбрать нужное действие.
Стандартная очистка: программа пытается автоматически очистить или удалить зараженный файл. При невозможности выбрать необходимое действие автоматически программа предлагает сделать выбор пользователю. Выбор пользователю предоставляется и в том случае, если предварительно заданное действие не может быть выполнено.
Тщательная очистка: программа очищает или удаляет все зараженные файлы (в том числе архивы). Единственное исключение составляют системные файлы. Если файлы невозможно очистить, на экран выводится предупреждение с предложением выбрать действие.
Внимание: В используемом по умолчанию режиме архив удаляется целиком только в том случае, если все файлы в нем заражены. Если в архиве есть нормальные файлы, он не удаляется. Если зараженный архив обнаруживается в режиме тщательной очистки, он удаляется целиком, даже если в нем есть незараженные файлы.

4.1.7.4 Расширения

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



По умолчанию сканируются все файлы независимо от их расширения. Любое расширение можно добавить в список файлов, исключенных из сканирования. Если снят флажок **Сканировать все файлы**, список меняется для отображения всех расширений файлов, которые сейчас подвергаются сканированию. С помощью кнопок **Добавить** и **Удалить** можно включать или запрещать сканирование для тех или иных расширений.

Для того чтобы включить сканирование файлов без расширений, установите флажок **Сканировать файлы без расширений**.

Иногда может быть необходимо исключить файлы из сканирования, если сканирование определенных типов файлов препятствует нормальной работе программы, которая использует эти расширения. Например, может быть полезно исключить расширения .edb, .eml и .tmp при использовании серверов Microsoft Exchange.

4.1.7.5 Ограничения

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

Максимальный размер объекта: определяет максимальный размер объектов, подлежащих сканированию. Данный модуль защиты от вирусов будет сканировать только объекты меньше указанного размера. Не рекомендуется изменять значение по умолчанию, так как обычно это не нужно. Этот параметр предназначен для опытных пользователей, которым необходимо исключить большие объекты из сканирования.

Максимальное время сканирования, в секундах: определяет максимальное время для сканирования объекта. Если пользователь укажет здесь собственное значение, модуль защиты от вирусов прекратит сканирование объекта по истечении указанного времени вне зависимости от того, было ли сканирование завершено.

Уровень вложенности архива: определяет максимальную глубину сканирования архивов. Не рекомендуется изменять значение по умолчанию, равное 10; в обычных условиях для этого нет особой причины. Если сканирование преждевременно прерывается из-за превышения уровня вложенности, архив остается непроверенным.

Максимальный размер файла в архиве: этот параметр позволяет указать максимальный размер файлов в архиве (после извлечения), подлежащих сканированию. Если этот параметр прерывает сканирование архива до завершения, то архив останется непроверенным.

4.1.7.6 Другое

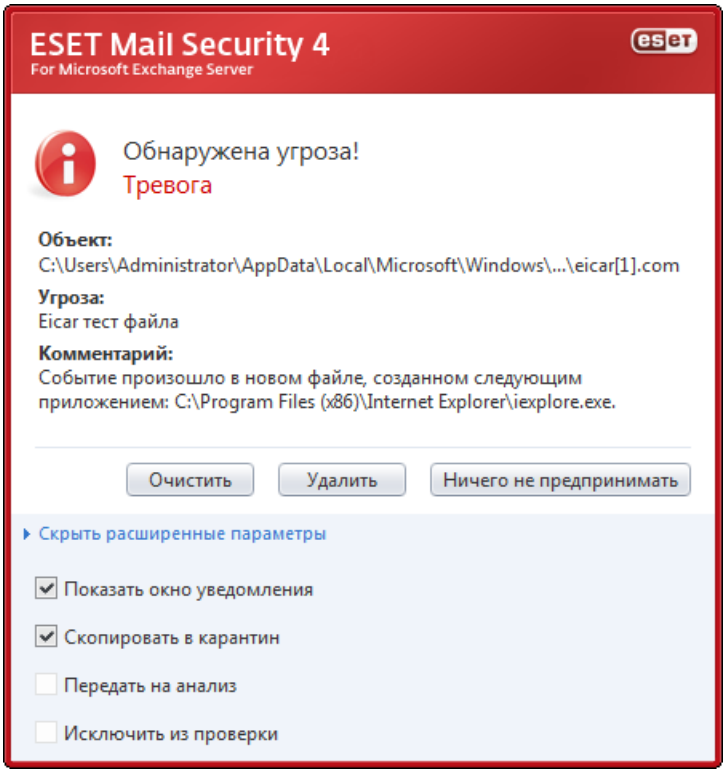
Сканировать альтернативные потоки данных (ADS): альтернативные потоки данных используются файловой системой NTFS для связей файлов и папок, которые не видны для обычных методов сканирования. Многие заражения маскируются под альтернативные потоки данных, пытаясь избежать обнаружения.
Запустить фоновое сканирование с низким приоритетом: каждый процесс сканирования потребляет некоторое количество системных ресурсов. Если пользователь работает с ресурсоемкими программами, можно активировать фоновое сканирование с низким приоритетом и высвободить тем самым ресурсы для других приложений.
Регистрировать все объекты: если этот флажок установлен, в файле журнала будет содержаться информация обо всех просканированных файлах, в том числе незараженных.
Включить оптимизацию Smart: установите этот флажок, чтобы уже просканированные файлы не сканировались повторно, пока не будут изменены. Файлы сканируются повторно сразу после каждого обновления базы данных сигнатур вирусов.
Сохранить отметку о времени последнего доступа: установите этот флажок, чтобы сохранять исходную отметку о времени доступа к сканируемым файлам, не обновляя ее (например, для использования с системами резервного копирования данных).
Прокрутить журнал: этот параметр позволяет включать и отключать прокрутку журнала. Если флажок установлен, в окне можно прокручивать отображаемую информацию вверх.
Показывать уведомление о завершении сканирования в отдельном окне: открывает отдельное окно с информацией о результатах сканирования.

4.1.8 Обнаружение заражения

Заражения могут попасть на компьютер из различных источников: веб-сайты, общие папки, электронная почта или съемные носители (USB-устройства, внешние диски, компакт-диски, DVD-диски и т. д.).
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 нажмите «Сканирование компьютера».
- Нажмите **Сканирование Smart** (Дополнительные сведения см. в разделе Сканирование Smart 62)
- После окончания сканирования проверьте количество просканированных, зараженных и очищенных файлов в журнале.

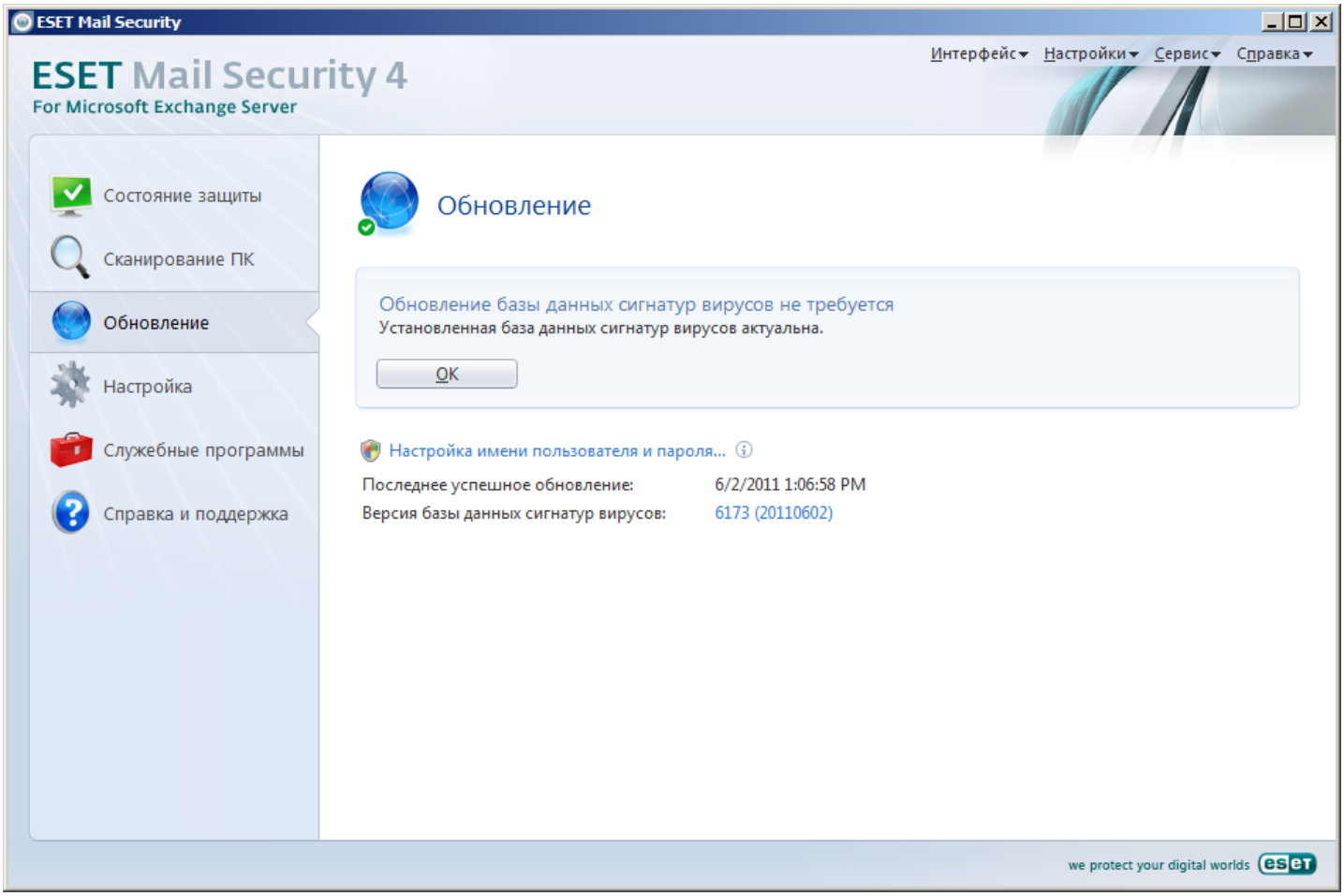
Если следует сканировать только определенную часть диска, выберите вариант **Выборочное сканирование** и укажите объекты, которые нужно сканировать на предмет наличия вирусов.
Ниже описан общий случай работы ESET Mail Security с заражениями. Предположим, что заражение обнаружено модулем защиты файловой системы в режиме реального времени при уровне очистки по умолчанию. Модуль попытается очистить или удалить файл. Если действие по умолчанию для модуля защиты в режиме реального времени не определено, его предлагается выбрать пользователю в специальном окне предупреждения. Обычно доступны действия **Очистить**, **Удалить** и **Пропустить**. Не рекомендуется выбирать вариант **Пропустить**, так как в этом случае зараженные файлы останутся на компьютере. Исключением может быть ситуация, когда имеется полная уверенность в том, что файл безвреден и был обнаружен по ошибке.
Очистка и удаление: примените очистку, если полезный файл был атакован вирусом, который добавил вредоносный код к полезному. В этом случае сначала программа пытается очистить зараженный файл, чтобы восстановить его первоначальное состояние. Если файл содержит только вредоносный код, его следует удалить.



Если зараженный файл заблокирован или используется каким-либо системным процессом, обычно он удаляется только после освобождения. Как правило, это происходит после перезапуска системы.
Удаление файлов из архивов: в режиме очистки по умолчанию архив удаляется целиком только в том случае, если он содержит только зараженные файлы. Иначе говоря, архивы, в которых есть незараженные файлы, не удаляются. Однако следует проявлять осторожность при сканировании в режиме тщательной очистки, так как в этом режиме архив удаляется, если содержит хотя бы один зараженный файл, независимо от состояния других файлов в архиве.

4.2 Обновление программы

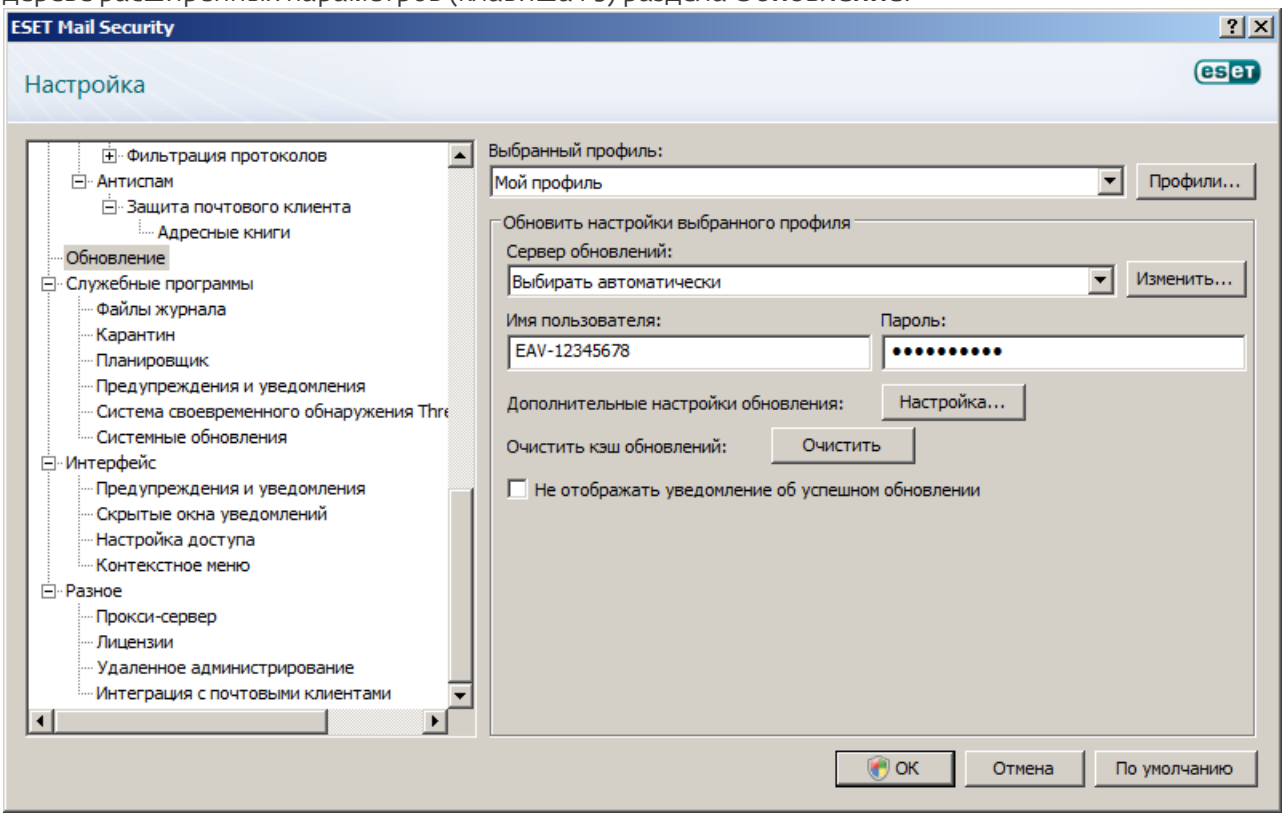
Регулярное обновление ESET Mail Security — основное условие обеспечения максимально высокого уровня безопасности. Модуль обновления поддерживает актуальность программы двумя способами: путем обновления базы данных сигнатур вирусов и путем обновления компонентов системы.
Выбрав пункт **Обновление** в главном меню, можно получить информацию о текущем состоянии обновления, в том числе дату и время последнего успешно выполненного обновления, а также сведения о необходимости обновления. Также в основном окне указывается версия базы данных сигнатур вирусов. Этот числовой индикатор представляет собой активную ссылку на страницу веб-сайта ESET, где перечисляются все сигнатуры, добавленные при данном обновлении.
Кроме того, есть функция для запуска процесса обновления принудительно (**Обновить базу данных сигнатур вирусов**), а также основные параметры обновления, такие как имя пользователя и пароль для доступа к серверам обновлений ESET.
Нажмите ссылку **Активация программы**, чтобы открыть форму регистрации, в которой вы сможете активировать свой программный продукт обеспечения безопасности ESET, после чего получите по электронной почте сообщение с данными аутентификации (имя пользователя и пароль).



ПРИМЕЧАНИЕ: Имя пользователя и пароль предоставляются компанией ESET после приобретения программы ESET Mail Security.

4.2.1 Настройка обновлений

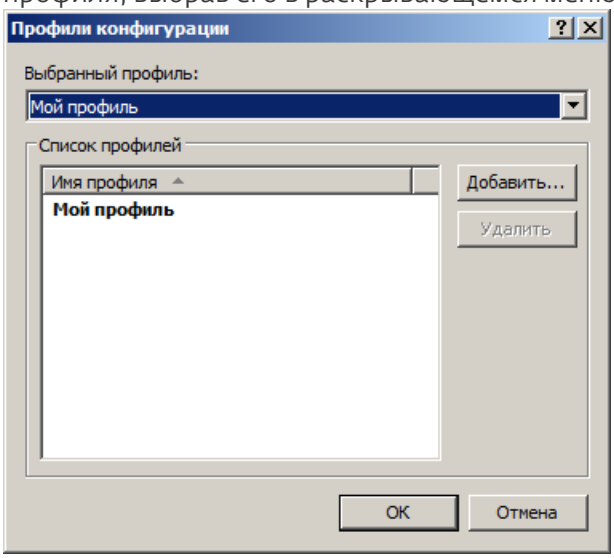
В разделе параметров обновления указывается информация об источниках обновлений, такая как серверы обновлений и данные аутентификации для них. По умолчанию в раскрывающемся меню **Сервер обновлений** выбран параметр **Выбирать автоматически**, обеспечивающий автоматическую загрузку файлов обновлений с сервера ESET с минимальным расходом трафика. Параметры обновлений доступны в дереве расширенных параметров (клавиша F5) раздела **Обновление**.



Список доступных серверов обновлений можно просмотреть с помощью раскрывающегося меню **Сервер обновлений**. Для добавления нового сервера обновлений нажмите кнопку **Изменить...** в разделе **Обновить настройки выбранного профиля**, а затем кнопку **Добавить**. Для аутентификации на серверах обновлений используются **имя пользователя** и **пароль**, созданные и отправленные вам после покупки.

4.2.1.1 Профили обновления

Профили обновления можно создавать для различных конфигураций и задач обновления. Создание профилей обновления особенно полезно для пользователей мобильных устройств, которые могут создать вспомогательный профиль в случае, когда свойства подключения к Интернету регулярно меняются.
В раскрывающемся меню **Выбранный профиль** отображается текущий профиль. По умолчанию это **Мой профиль**. Для создания нового профиля нажмите кнопку **Профили...**, затем **Добавить...** и введите нужное **Имя профиля**. При создании нового профиля можно скопировать параметры из уже существующего профиля, выбрав его в раскрывающемся меню **Копировать настройки профиля**.



В окне настройки профиля можно выбрать сервер обновлений из списка доступных серверов или добавить новый. Список существующих серверов обновлений можно просмотреть с помощью раскрывающегося меню **Сервер обновлений**. Для добавления нового сервера обновлений нажмите кнопку **Изменить...** в разделе **Обновить настройки выбранного профиля**, а затем кнопку **Добавить**.

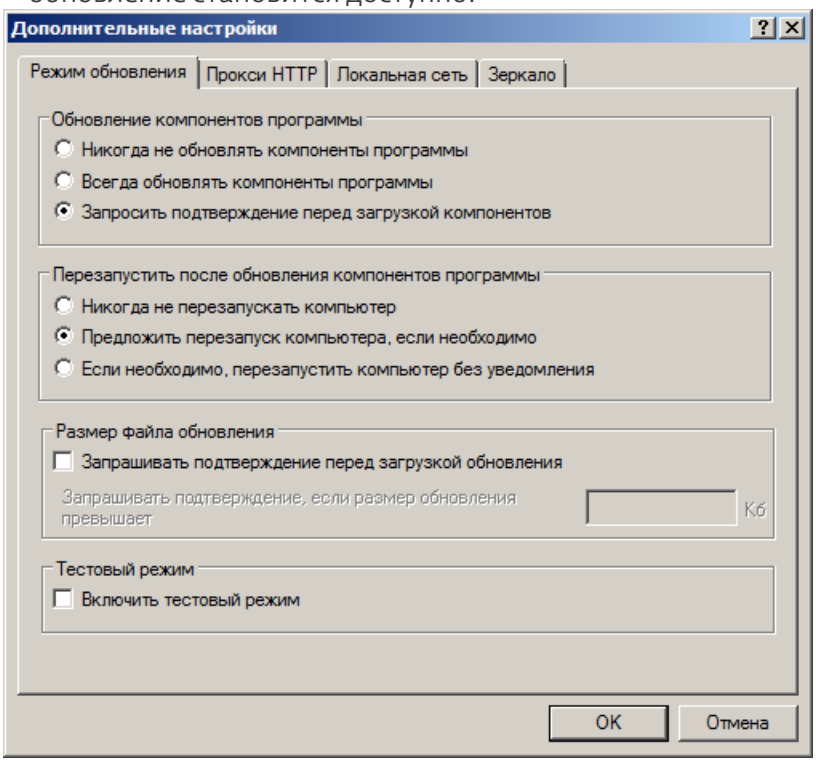
4.2.1.2 Дополнительные настройки обновления

Для просмотра расширенных параметров обновления нажмите кнопку **Настройка...**. Расширенные параметры обновления позволяют настроить **режим обновления**, **прокси HTTP**, **локальную сеть** и **зеркало** .

4.2.1.2.1 Режим обновления

Вкладка **«Режим обновления»** содержит параметры обновления программы.
В разделе **Обновление компонентов программы** доступно три описанных далее варианта.

- **Никогда не обновлять компоненты программы**: появляющиеся обновления компонентов программы не будут загружаться.
- **Выполнять обновление компонентов программы, если доступно**: появляющиеся обновления компонентов программы будут устанавливаться автоматически.
- **Запросить подтверждение перед загрузкой компонентов**: Вариант по умолчанию. Пользователю будет предлагаться подтвердить обновление компонентов программы или отказаться от него, когда такое обновление становится доступно.



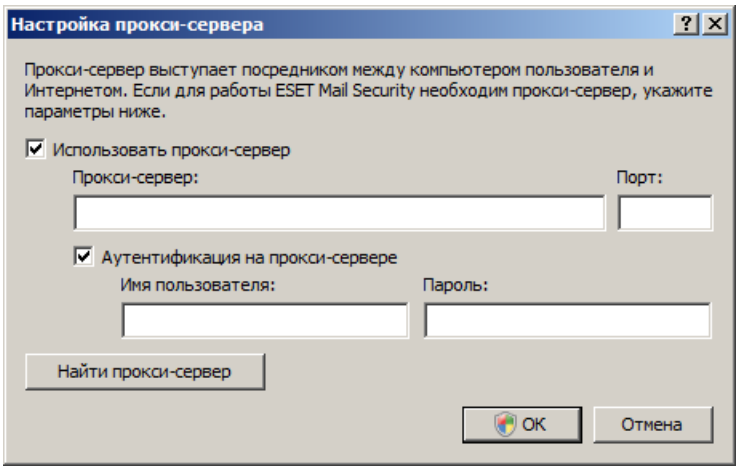
После обновления компонентов программы может быть необходимо перезапустить компьютер, чтобы все модули работали полностью корректно. В разделе **Перезапустить после обновления компонентов программы** можно выбрать один из следующих вариантов.

- **Никогда не перезапускать компьютер**
- **Предложить перезапуск компьютера, если необходимо**
- **Если необходимо, перезапустить компьютер без уведомления**

По умолчанию выбран вариант **Предложить перезапуск компьютера, если необходимо**. 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. Например, автоматический перезапуск сервера после обновления программы может привести к серьезным проблемам.

4.2.1.2.2 Прокси-сервер

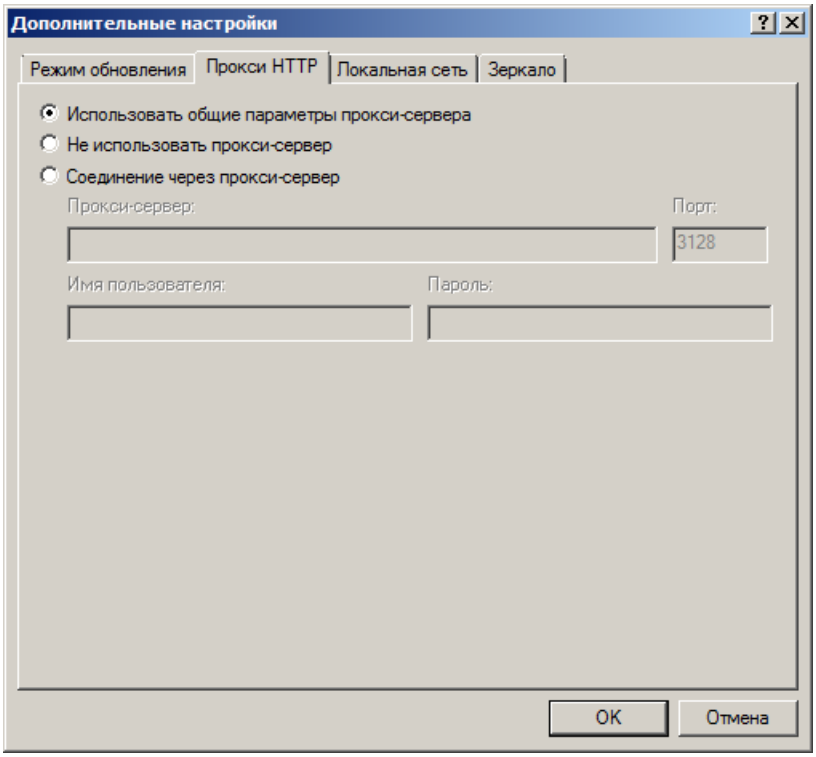
В ESET Mail Security настройку прокси-сервера можно выполнить в двух разных разделах дерева расширенных параметров.
Во-первых, параметры прокси-сервера можно сконфигурировать в разделе **Разное** > **Прокси-сервер**. Настройка прокси-сервера на этом уровне позволяет задать его параметры для программы ESET Mail Security в целом. Они используются всеми модулями программы, которым требуется подключение к Интернету.
Для настройки параметров прокси-сервера на этом уровне установите флажок **Использовать прокси-сервер**, а затем введите адрес прокси-сервера в поле **Прокси-сервер** и номер **порта** в соответствующее поле.



Если требуется аутентификация на прокси-сервере, установите флажок **«Прокси-сервер требует аутентификации»**, а затем укажите **имя пользователя** и **пароль** в соответствующих полях. Нажмите кнопку **Найти прокси-сервер**, чтобы автоматически определить параметры прокси-сервера и вставить их. Будут скопированы параметры, указанные в Internet Explorer.
ПРИМЕЧАНИЕ: Эта функция не позволяет получить данные аутентификации (имя пользователя и пароль), их пользователь должен указать самостоятельно.
Также параметры прокси-сервера можно настроить в разделе «Дополнительные настройки обновления». В этом случае параметры применяются к конкретному профилю обновления. Параметры прокси-сервера для конкретного профиля обновления можно открыть, перейдя на вкладку **Прокси HTTP** в разделе **Дополнительные настройки обновления**. Здесь можно выбрать один из трех вариантов.

- **Использовать общие параметры прокси-сервера**
- **Не использовать прокси-сервер**
- **«Соединение через прокси-сервер»** (указываются параметры подключения).

Если выбрать вариант **Использовать общие параметры прокси-сервера**, будут использоваться параметры прокси-сервера, уже заданные в разделе **Разное** > **Прокси-сервер** дерева расширенных параметров (как описано в начале данной статьи).



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

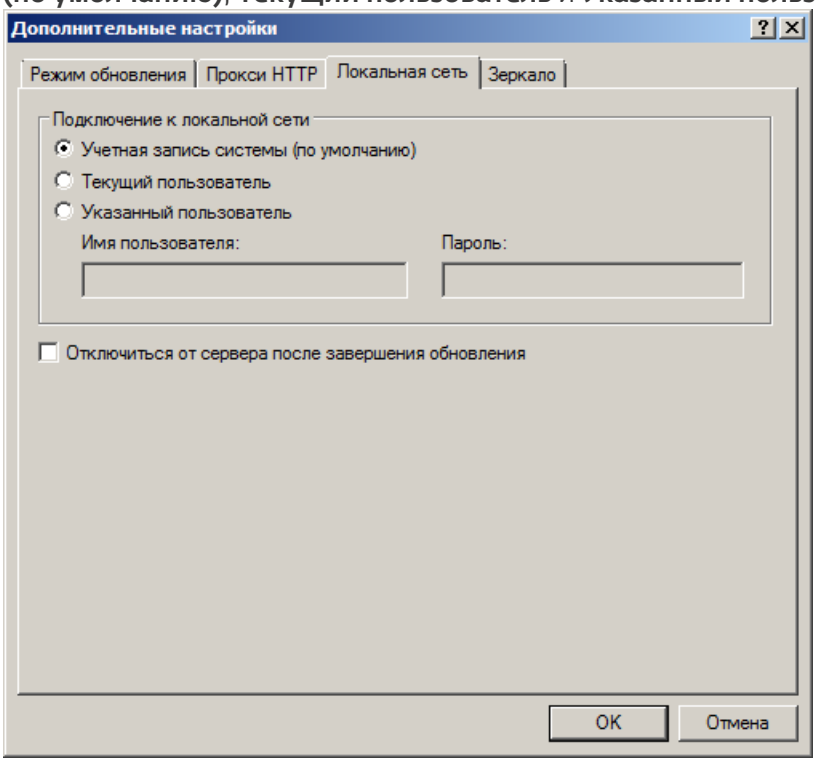
Вариант **Соединение через прокси-сервер** следует выбрать, если для обновления ESET Mail Security нужно использовать прокси-сервер, причем он отличается от указанного в общие параметрах (**Разное** > **Прокси-сервер**). В этом случае нужно указать параметры: адрес (поле **Прокси-сервер**), **порт** для соединения, а также при необходимости **имя пользователя** и **пароль**.

Также этот вариант следует выбрать, если общие параметры прокси-сервера заданы не были, но при этом ESET Mail Security будет подключаться к прокси-серверу для получения обновлений.

По умолчанию выбран вариант **Использовать общие параметры прокси-сервера**.

4.2.1.2.3 Подключение к локальной сети

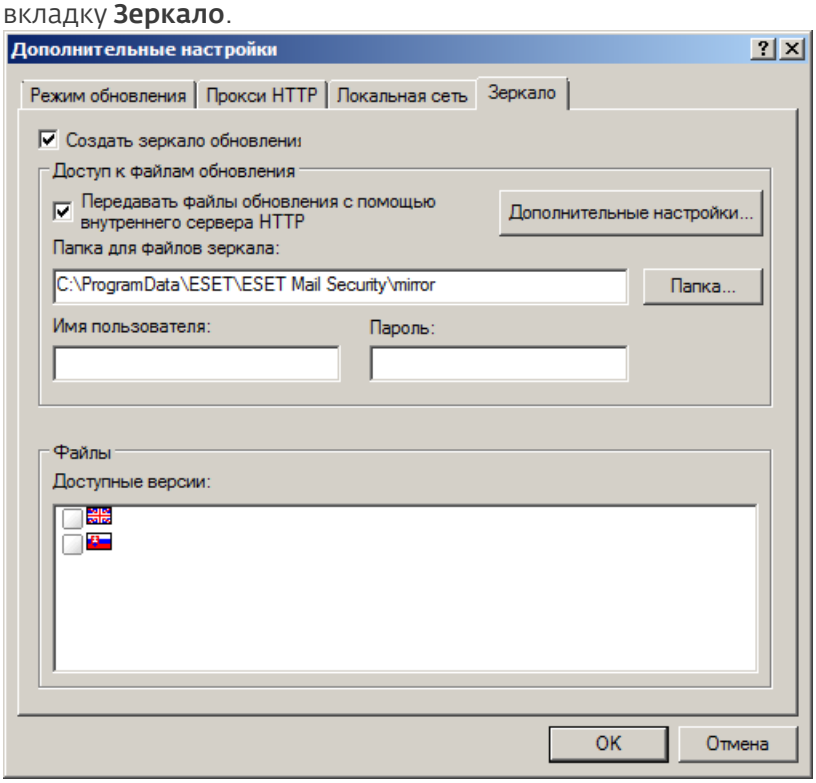
При обновлении с локального сервера под управлением операционной системы на базе NT по умолчанию требуется аутентификация всех сетевых подключений. Чаще всего у локальной учетной записи системы недостаточно прав для доступа к папке зеркала (папке, в которой хранятся копии файлов обновления). В этом случае введите имя пользователя и пароль в разделе параметров обновления или укажите существующую учетную запись, под которой программа сможет получить доступ к серверу обновлений (зеркалу).
Для конфигурирования такой учетной записи перейдите на вкладку **Локальная сеть**. В разделе **Подключение к локальной сети** можно выбрать один из следующих вариантов: **Учетная запись системы (по умолчанию)**, **Текущий пользователь** и **Указанный пользователь**.



Выберите **Учетная запись системы (по умолчанию)**, чтобы использовать для аутентификации учетную запись системы. Если данные аутентификации в главном разделе параметров обновлений не указаны, как правило, процесса аутентификации не происходит.
Для того чтобы программа использовала для аутентификации учетную запись, под которой в данный момент выполнен вход в систему, выберите вариант **Текущий пользователь**. Недостаток этого варианта заключается в том, что программа не может подключиться к серверу обновлений, если в данный момент ни один пользователь не выполнил вход в систему.
Выберите **«Указанный пользователь»**, если нужно указать учетную запись пользователя для аутентификации.
Внимание: Если выбран вариант **Текущий пользователь** или **Указанный пользователь**, может произойти ошибка при изменении учетной записи программы. В главном разделе параметров обновления рекомендуется указывать данные аутентификации в локальной сети. В этом разделе параметров обновлений данные аутентификации нужно указать в следующем формате: имя_домена\пользователь (а для рабочей группы рабочая_группа\имя) и пароль. При обновлении по протоколу HTTP с локального сервера аутентификация не требуется.

4.2.1.2.4 Создание копий обновлений, зеркало

ESET Mail Security позволяет создавать копии файлов обновлений, которые могут использоваться для обновления других рабочих станций в сети. Обновление клиентских рабочих станций с зеркала оптимизирует трафик в сети и сокращает объем потребляемого интернет-трафика.
Параметры конфигурации локального сервера зеркала можно найти (после добавления действительного лицензионного ключа в менеджере лицензий, который расположен в разделе «Дополнительные настройки» ESET Mail Security), воспользовавшись разделом **Дополнительные настройки обновления**. Для доступа к этому разделу нажмите клавишу F5 и выберите **Обновление** в дереве расширенных параметров, после чего нажмите кнопку **Настройка...** рядом с пунктом **Дополнительные настройки обновления** и перейдите на вкладку **Зеркало**.



На первом этапе настройки зеркала нужно выбрать вариант «Создать зеркало обновления». После этого становятся доступны другие параметры настройки зеркала, такие как способ доступа к файлам обновлений и путь к файлам зеркала.
Методы активации зеркала подробно описываются в разделе Обновление с зеркала 78. Пока что достаточно заметить, что существует два основных метода доступа к зеркалу: папка с файлами обновлений может существовать как общая сетевая папка или как HTTP-сервер.
Папка, предназначенная для хранения файлов обновлений, указывается в разделе **Папка для дублируемых файлов**. Нажмите **Папка...**, чтобы найти нужную папку на локальном компьютере или в общей сетевой папке. Если для указанной папки нужна авторизация, данные аутентификации должны быть указаны в полях **Имя пользователя** и **Пароль**. Имя пользователя и пароль следует вводить в формате *Домен/ Пользователь* или *Рабочая_группа/Пользователь*. Не забудьте ввести соответствующие пароли.
При настройке зеркала пользователь также может указать языковые версии, для которых нужно загружать копии обновлений. Настройка языковых версий доступна в разделе **Файлы** — **Доступные версии**.
ПРИМЕЧАНИЕ: Базу данных модуля защиты от спама невозможно обновлять с зеркала. Для получения дополнительных сведений о том, как обеспечить корректное обновление базы данных модуля защиты от спама, воспользуйтесь этой ссылкой 38.

4.2.1.2.4.1 Обновление с зеркала

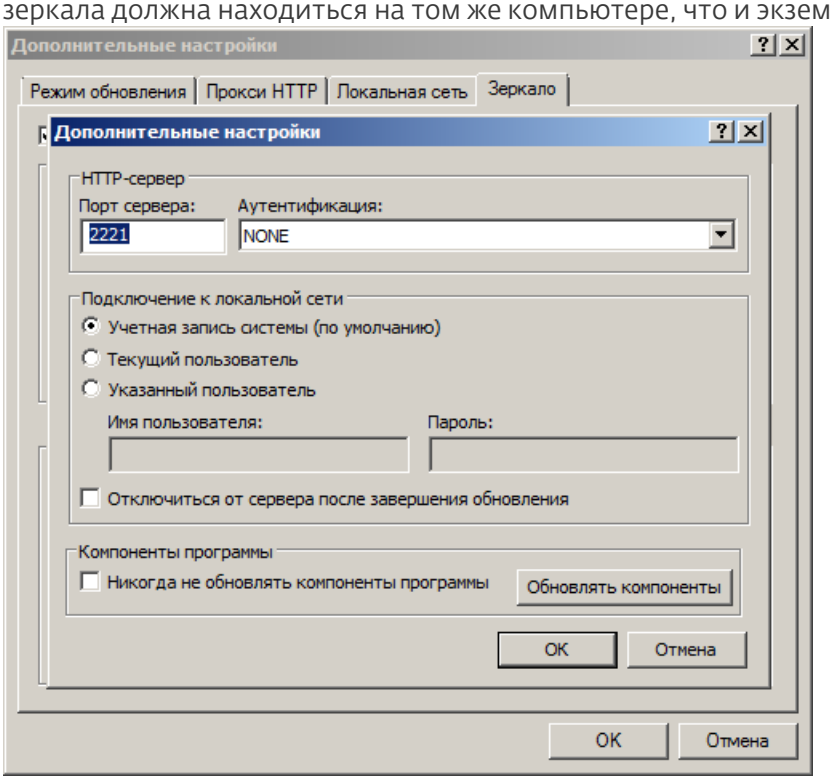
Существует два основных метода настройки зеркала: папка с файлами обновлений может существовать как общая сетевая папка или как HTTP-сервер.

Доступ к файлам зеркала с помощью внутреннего сервера HTTP

Это вариант по умолчанию, выбранный в предварительно заданной конфигурации программы. Для обеспечения доступа к зеркалу с помощью HTTP-сервера перейдите в раздел **Дополнительные настройки обновления** (вкладка **Зеркало**) и выберите вариант **Создать зеркало обновления**.

В разделе **Дополнительные настройки** 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**. В параметре **Аутентификация** определяется метод аутентификации, используемый для доступа к файлам обновлений. Доступны следующие варианты: **Ничего**, **Основное** и **NTLM**. Для того чтобы использовать кодирование base64 и упрощенную аутентификацию по имени пользователя и паролю, выберите **Основное**. Вариант **NTLM** обеспечивает шифрование за счет метода безопасного шифрования. Для аутентификации используется учетная запись пользователя, созданная на рабочей станции, которая предоставляет общий доступ к файлам обновлений. Значение по умолчанию — **Ничего**. Этот вариант дает доступ к файлам обновлений без аутентификации.

Внимание: Если планируется организовать доступ к файлам обновлений с помощью HTTP-сервера, папка зеркала должна находиться на том же компьютере, что и экземпляр ESET Mail Security, который ее создает.



После завершения настройки зеркала следует воспользоваться рабочими станциями и добавить новый сервер обновлений в формате **http://IP-адрес_вашего_сервера:2221**. Для этого выполните следующие действия.

- Откройте раздел ESET Mail Security **Дополнительные настройки** и нажмите **Обновление** .
- Нажмите **Изменить...** справа от раскрывающегося меню **Сервер обновлений** и добавьте новый сервер в формате http://IP_адрес_вашего_сервера:2221.
- Выберите вновь добавленный сервер из списка серверов обновлений.

Доступ к зеркалу через общий системный ресурс

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 ESET Smart Security из папки зеркала.

Далее следует сконфигурировать доступ к зеркалу в разделе **Дополнительные настройки обновления** (вкладка **Зеркало**), сняв флажок **Передавать файлы обновления с помощью внутреннего сервера HTTP**. Этот вариант включен по умолчанию после установки программы.

Если общая папка расположена на другом компьютере в сети, необходимо указать данные аутентификации для доступа к этому компьютеру. Для ввода данных аутентификации откройте раздел «Дополнительные настройки» ESET Mail Security (F5) и выберите ветвь **Обновление**. Нажмите кнопку **Настройка...** и перейдите на вкладку **Локальная сеть**. Этот параметр аналогичен используемому для обновления и описан в разделе Подключение к локальной сети 76.

После окончания настройки зеркала укажите на рабочих станциях адрес нового сервера обновлений в формате \\UNC-ИМЯ_КОМПЬЮТЕРА\ПУТЬ. Это действие можно выполнить следующим образом.

- Откройте раздел «Дополнительные настройки» ESET Mail Security и нажмите **Обновление**.
- Нажмите **Изменить...** рядом с пунктом «Сервер обновлений» и добавьте новый сервер в формате *\\UNC-ИМЯ_КОМПЬЮТЕРА\ПУТЬ*.
- Выберите вновь добавленный сервер из списка серверов обновлений.

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

4.2.1.2.4.2 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** Windows, выберите **Выполнить**, вставьте имя папки и нажмите кнопку **ОК**. На экран должно быть выведено содержимое папки.

ESET Mail Security **запрашивает имя пользователя и пароль**: вероятная причина заключается в том, что введены неверные данные аутентификации (имя пользователя и пароль) в разделе обновлений. Имя пользователя и пароль используются для доступа к серверу обновлений, с которого выполняется обновление программы. Убедитесь, что данные аутентификации указаны верно и в правильном формате. Например, *Домен/Имя_пользователя* или *Рабочая_группа/ имя_пользователя* в сочетании с соответствующим паролем. Если сервер зеркала доступен всем участникам сети, это не означает, что у любого пользователя есть к нему доступ. Параметр «Все участники» означает то, что папка доступна всем пользователям домена, а не то, что предоставляется доступ без авторизации. 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: обмен данными по указанному порту подключения к HTTP-версии зеркала блокируется.

4.2.2 Создание задач обновления

Обновление можно запустить вручную с помощью функции **Обновить базу данных сигнатур вирусов** в основном окне, которое появляется после выбора пункта «Обновление» в главном меню.

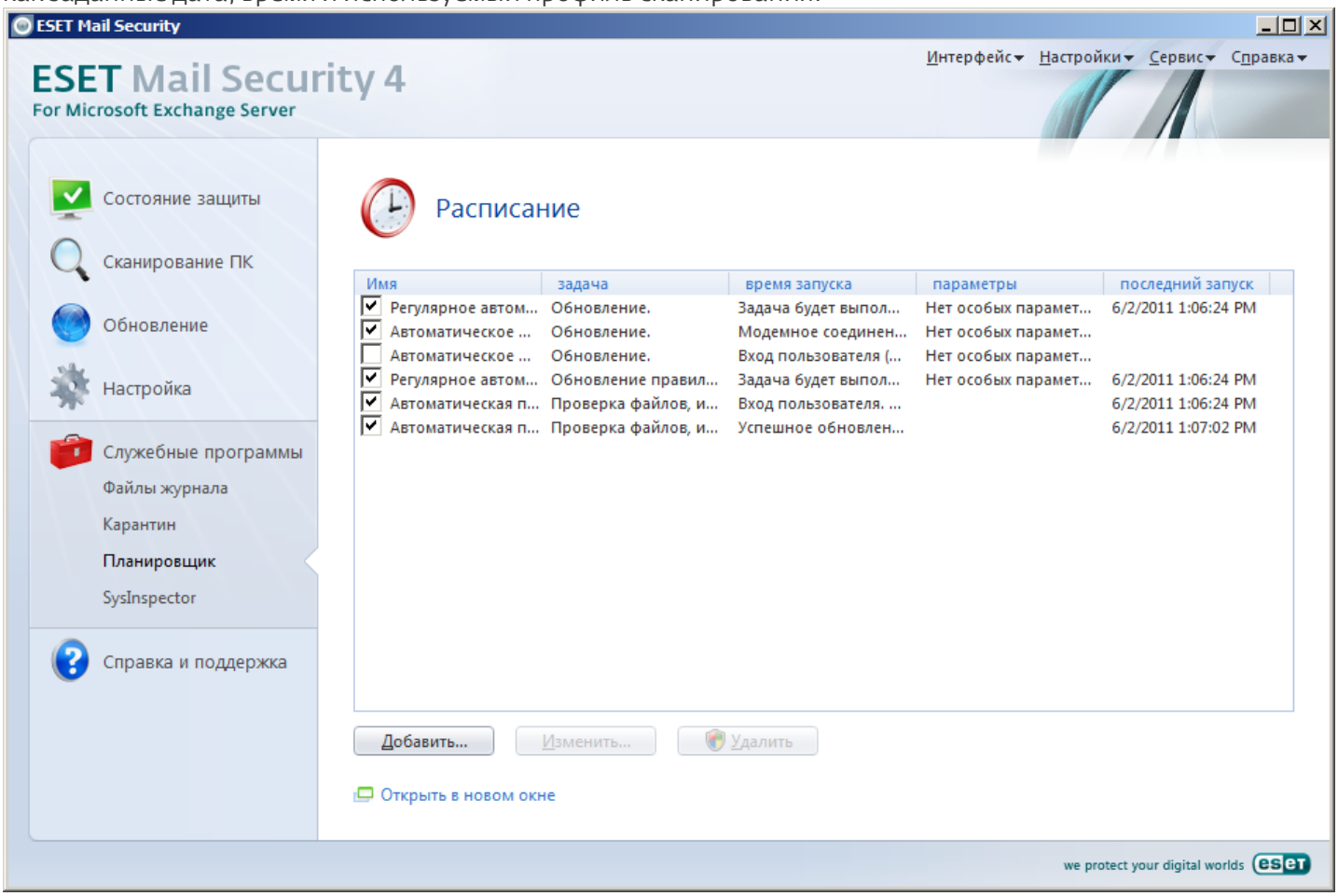
Обновления также можно выполнять как запланированную задачу. Для конфигурирования запланированной задачи перейдите в раздел **Служебные программы** > **Планировщик**. По умолчанию в ESET Mail Security активированы указанные ниже задачи.

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

Каждую задачу обновления можно изменить в соответствии с конкретными требованиями. В дополнение к существующим по умолчанию задачам обновления можно создать другие задачи с пользовательскими настройками. Дополнительную информацию о создании и настройке задач обновления см. в разделе Планировщик 80.

4.3 Планировщик

Планировщик доступен, если в ESET Mail Security активирован расширенный режим. Перейти к **планировщику** можно через главное меню ESET Mail Security, воспользовавшись пунктом **Служебные программы**. 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.

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

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...**.

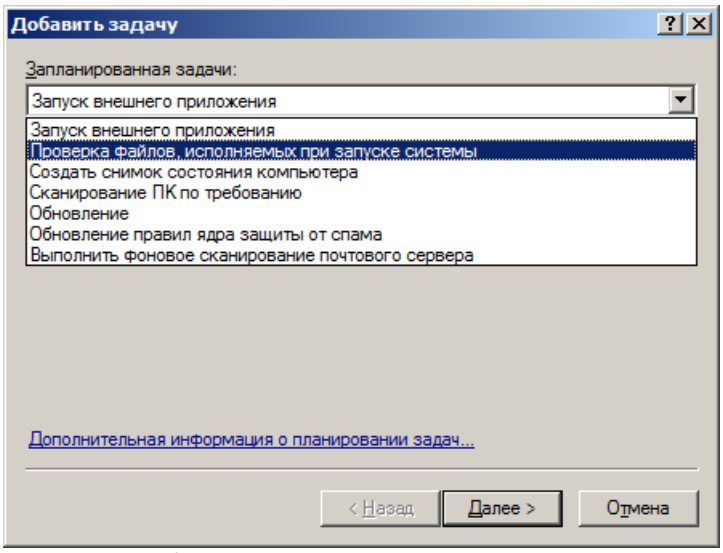
4.3.1 Цель планирования задач

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

4.3.2 Создание новых задач

Для создания задачи в планировщике нажмите кнопку **Добавить...** или щелкните правой кнопкой мыши и выберите в контекстном меню команду **Добавить...**. Доступно пять типов задач.

- **Запуск внешнего приложения**
- **Проверка файлов, исполняемых при запуске системы**
- **Создать снимок состояния компьютера**
- **Сканирование ПК по требованию**
- **Обновление**



Поскольку **обновление** — одна из самых часто используемых запланированных задач, ниже описано добавление задачи обновления.

В раскрывающемся меню **Запланированная задача** выберите пункт **Обновление**. Нажмите кнопку **Далее** и введите название задачи в поле **Название задачи**. Выберите частоту выполнения задачи. Доступны следующие варианты: **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.

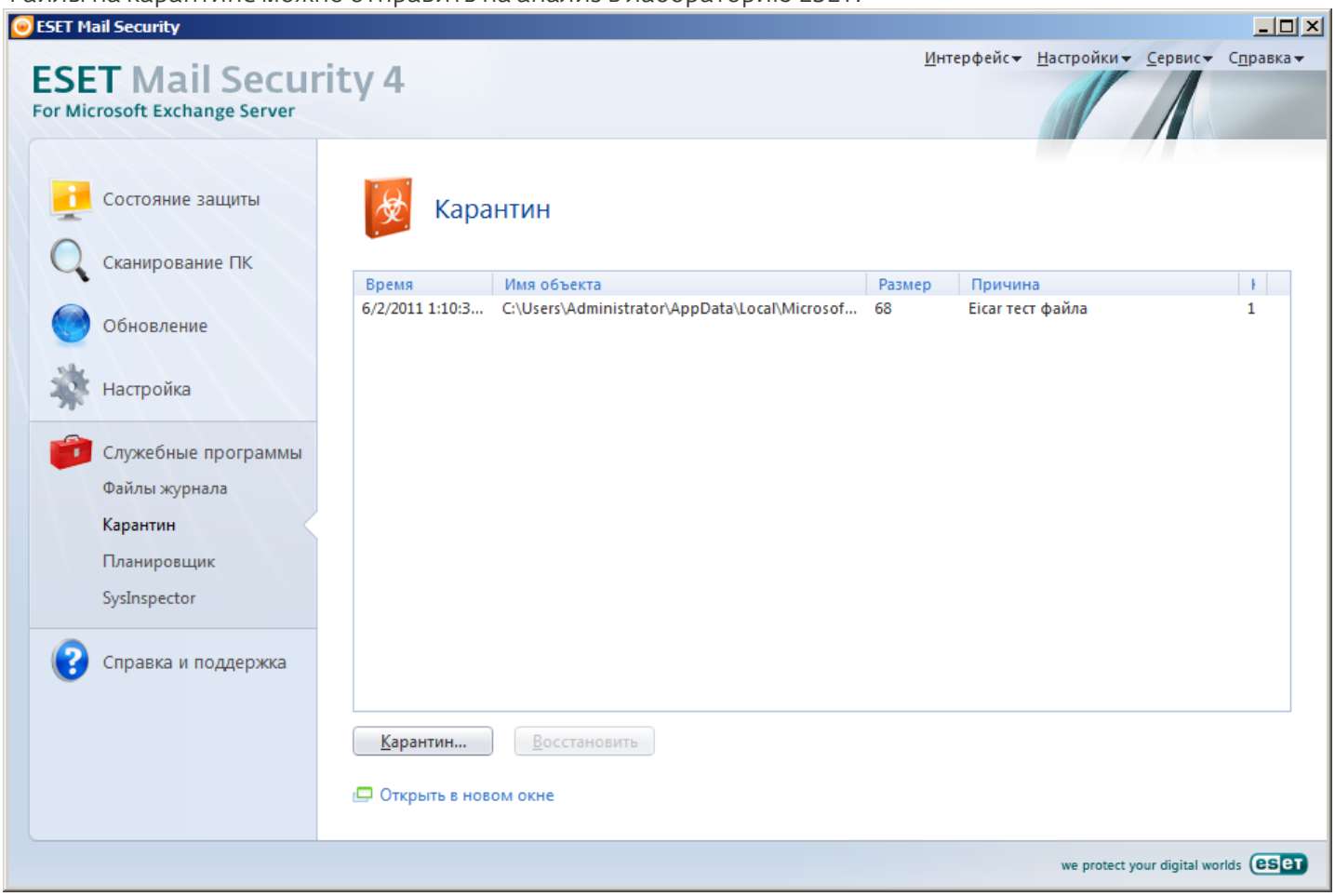
- **Ждать до следующего намеченного момента**
- **Выполнить задачу как можно скорее**
- **Выполнить задачу немедленно, если время, прошедшее с последнего запуска, превысило указанный интервал** (интервал можно указать с помощью параметра «Интервал между задачами»)

На следующем этапе отображается сводная информация о текущей запланированной задаче. Пункт **Запустить задачу с указанными параметрами** автоматически выбран. Нажмите кнопку **Готово**.

На экран будет выведено диалоговое окно, в котором можно выбрать профили, используемые для запланированной задачи. Можно выбрать основной профиль и вспомогательный, который будет использоваться, если задачу невозможно выполнить с применением основного профиля. Подтвердите настройки, нажав кнопку **ОК** в окне **Профили обновления**. Новая задача появится в списке существующих запланированных.

4.4 Карантин

Главная задача карантина заключается в безопасном хранении зараженных файлов. Файлы следует помещать на карантин, если они не могут быть очищены или безопасно удалены, если удалять их не рекомендуется или если они ошибочно отнесены программой ESET Mail Security к зараженным. 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 на анализ в лабораторию ESET.



Информацию о файлах, помещенных на карантин, можно просмотреть в виде таблицы, содержащей дату и время помещения файла на карантин, путь к его исходному расположению, его размер в байтах, причину помещения файла на карантин (например, мнение пользователя об объекте) и количество обнаруженных угроз (например, если архив содержит несколько вирусов).

4.4.1 Помещение файлов на карантин

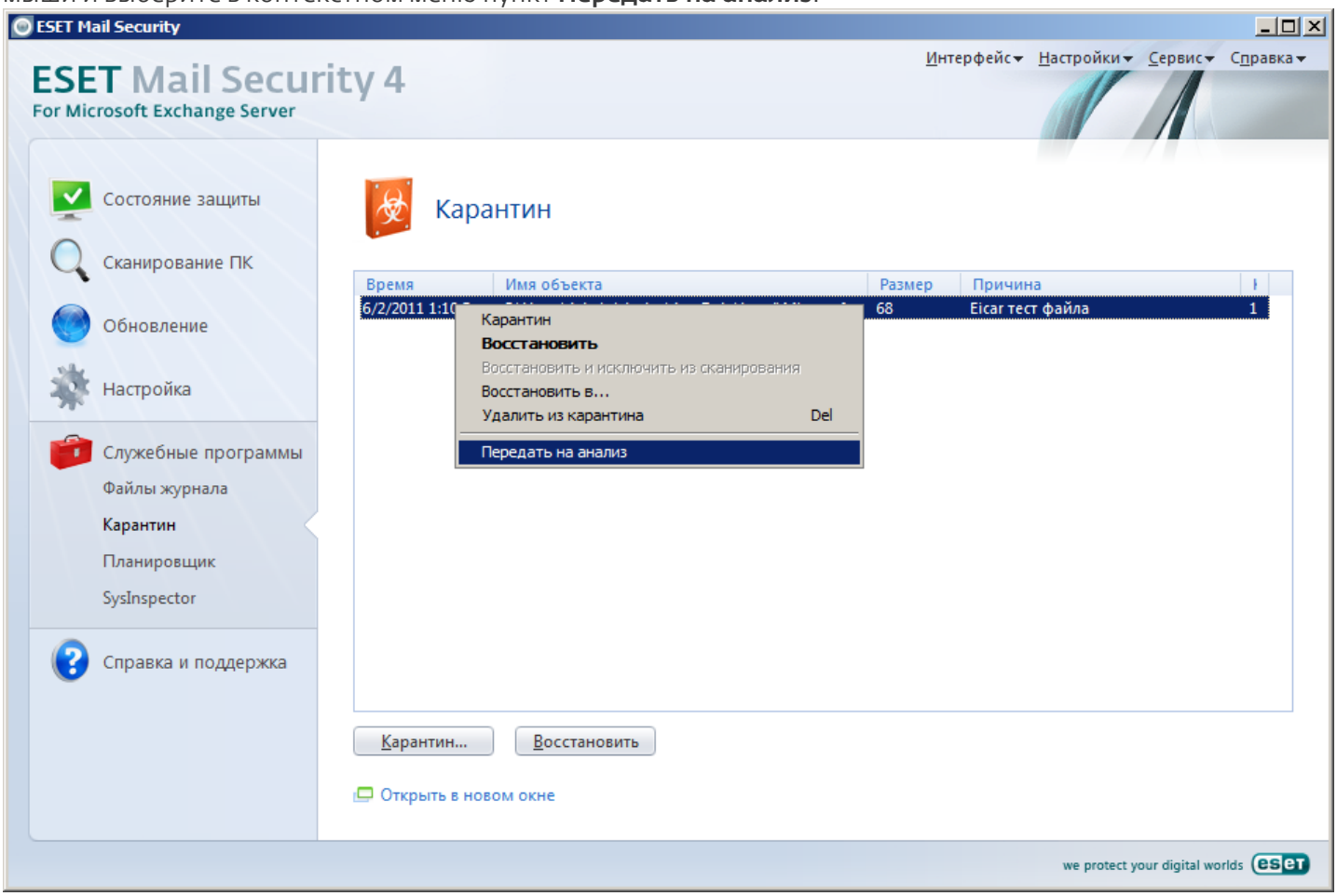
Программа ESET Mail Security автоматически помещает удаленные файлы на карантин (если этот параметр не был отменен пользователем в окне предупреждения). При желании любой подозрительный файл можно поместить на карантин вручную с помощью кнопки **Карантин...**. При этом исходная копия файла не удаляется.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

4.4.2 Восстановление из карантина

Файлы, находящиеся на карантине, можно восстановить в исходном месте. Для этого используется функция **Восстановить**. Команда **Восстановить** доступна в контекстном меню, которое открывается правым щелчком мыши по нужному файлу в окне «Карантин». 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.

4.4.3 Отправка файла из карантина

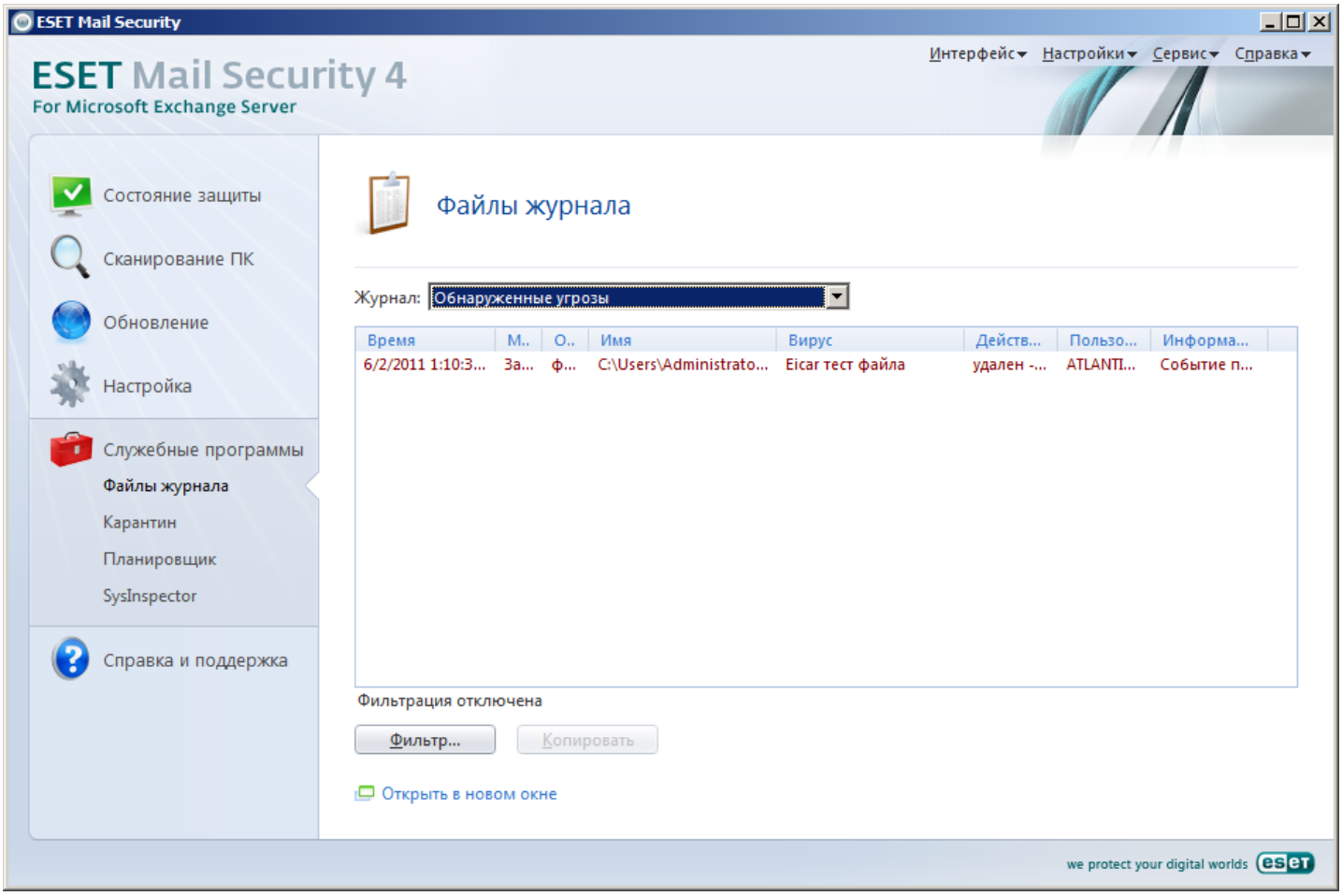
Если на карантин помещен подозрительный файл, не обнаруженный программой, или файл неверно квалифицирован как зараженный (например, путем эвристического анализа кода) и помещен на карантин, отправьте его в лабораторию ESET. Чтобы отправить файл из карантина, щелкните его правой кнопкой мыши и выберите в контекстном меню пункт **Передать на анализ**.



4.5 Файлы журнала

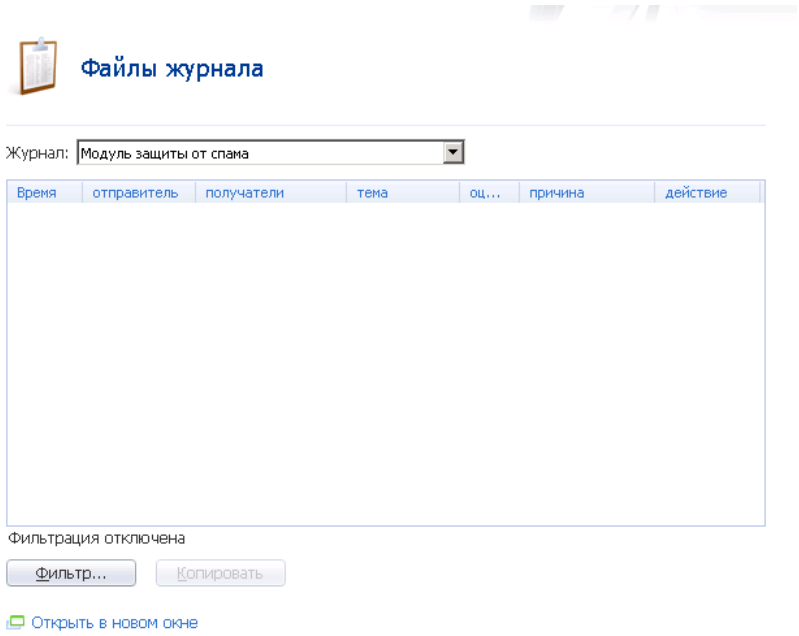
В журналах хранится информация о важных событиях: обнаруженные заражения, журналы сканирование по требованию, журналы резидентных модулей сканирования и системная информация.

В журналах защиты от спама и защиты путем работы с «серыми» списками (находятся среди других журналов в разделе **Служебные программы** > **Файлы журнала**) приводятся подробные сведения о сообщениях, которые были подвергнуты сканированию, и дальнейших действиях, примененных к таким сообщениям. Журналы могут быть очень полезны при поиске недоставленной электронной почты, выяснении того, почему какое-либо сообщение было помечено как спам, и т. п.



Модуль защиты от спама

Все сообщения, классифицированные ESET Mail Security как спам или вероятный спам, регистрируются здесь.



Описание столбцов

Время — время записи в журнал защиты от спама.
Отправитель — адрес отправителя.
Получатель — адрес получателя.
Тема — тема сообщения.
Оценка — оценка нежелательности, присвоенная сообщению (в диапазоне от 0 до 100).
Причина — указание того, что вызвало классификацию сообщения как спама. Приводится наиболее серьезная причина. Если нужно просмотреть другие причины, дважды щелкните запись. На экран будет выведено окно **Причина**, в котором содержатся остальные причины в порядке убывания серьезности.

Репутация URL-адреса как связанного с рассылкой спама	URL-адреса в сообщениях часто являются признаком спама.
Форматирование HTML (шрифты, цвета и т. д.)	Форматирование элементов в той части сообщения, которая составлена в формате HTML, имеет характеристики спама (тип шрифта и размер, его цвет и т. д.)
Уловки спама: умышленное запутывание	Используемые в спаме слова часто маскируются путем использования других символов. Стандартным примером является название «Viagra», которое часто записывается в виде «V1agra», чтобы избежать обнаружения средствами защиты от спама.
Спам типа изображения HTML	Нежелательные сообщения часто оформляются в виде изображений, что является еще одной стратегией маскировки для противодействия обнаружения средствами защиты от спама. В таких изображениях часто содержатся интерактивные ссылки на веб-страницы.
Форматирование URL как у домена, размещающего сервисы	URL-адрес содержит домен, размещающий сервисы.
Ключевое слово спама...	В сообщении есть типичные для спама слова.
Непоследовательность заголовка сообщения электронной почты	Информация в заголовке изменяется таким образом, чтобы выдать источник за того отправителя, которым он не является.
Вирус	В сообщении содержится подозрительное вложение.
Фишинг	В сообщении есть текст, являющийся типичным для фишинга.
Реплика	В сообщении есть текст, являющийся стандартным для категории спама, которая направлена на продажу подделок.

Общий индикатор спама	В сообщении есть слова или символы, являющиеся типичными для спама, такие как «Уважаемый друг», «Здравствуйте, победитель», «!!!» и т. п.
Индикатор разрешенных сообщений	Это индикатор, функции которого противоположны остальным перечисленным индикаторам. Он анализирует элементы, являющиеся характерными для нормальной желательной электронной почты. Данный индикатор уменьшает общую оценку нежелательности.
Неспецифический индикатор спама	В сообщении содержатся другие элементы спама, такие как кодирование base64.
Пользовательские фразы спама	Другие стандартные фразы, используемые в спаме.
URL-адрес занесен в "черный" список	URL-адрес в сообщении присутствует в «черном» списке.
IP %s в "черном" списке реального времени	IP-адрес … присутствует в «черном» списке реального времени.
URL %s в DNSBL	URL-адрес … присутствует в списке DNSBL.
URL %s в "черном" списке реального времени или сервер не имеет права на отправку почты	URL-адрес … присутствует в «черном» списке реального времени или же у сервера нет привилегий, необходимых для отправки сообщений электронной почты. Адреса, которые были частью маршрута электронной почты, проверяются по «черному» списку реального времени. Последний адрес проверяется на предмет прав подключения к общедоступным почтовым серверам. Если невозможно обнаружить действительные права на подключение, этот адрес находится в списке LBL. Сообщения помечаются как спам, потому что у индикатора LBL в поле **Причина** указывается следующий текст: «сервер не имеет права на отправку почты».

Действие — выполненное с сообщением действие. Возможны следующие действия.

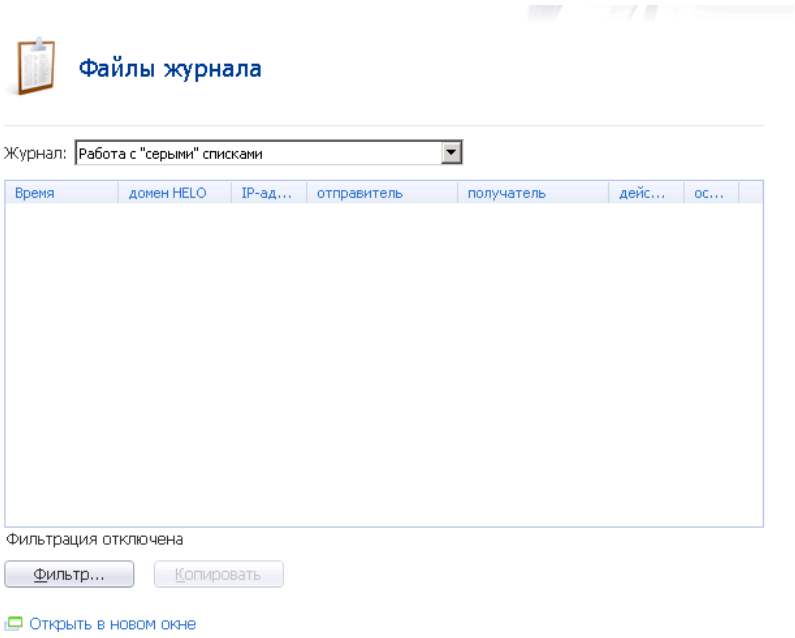
Сохранено	С сообщением не выполнены никакие действия.
Направлено на карантин	Сообщение было перемещено в карантин.
Очищено и направлено на карантин	Из сообщения был удален вирус, а само сообщение направлено на карантин.
Отклонено	Получение сообщения было запрещено, а отправителю направлен ответ отклонения по SMTP 20.
Удалено	Сообщение было удалено с использованием необъявленной потери 20.

Получено — время, когда сообщение было получено сервером.

ПРИМЕЧАНИЕ. Если сообщения получаются через сервер электронной почты, значения времени в полях **Время** и **Получено** практически одинаковы.

Работа с "серыми" списками

Все сообщения, которые оценивались с применением метода работы с «серыми» списками, регистрируются в этом журнале.



Описание столбцов

Время — время записи в журнал защиты от спама.
Домен HELO — имя домена, использованное отправляющим сервером для идентификации перед принимающим сервером.
IP-адрес — IP-адрес отправителя.
Отправитель — адрес отправителя.
Получатель — адрес получателя.
Действие — столбец, который может содержать одно из перечисленных далее состояний.

Отклонено	Было запрещено получение входящего сообщения с применением основного правила работы с «серыми» списками (первая попытка доставки)
Отклонено (не проверено)	Входящее сообщение было доставлено отправляющим сервером, но еще не истекло время, в течение которого соединения отклоняются (**Ограничение времени для первоначального отклонения подключения**)
Проверено	Входящее сообщение было повторно доставлено отправляющим сервером несколько раз, значение времени в параметре **Ограничение времени для первоначального отклонения подключения** истекло, и сообщение было успешно проверено и доставлено. См. также Транспортный агент 39.

Оставшееся время — время, оставшееся до окончания периода **Ограничение времени для первоначального отклонения подключения**

Обнаруженные угрозы

Журнал угроз содержит подробную информацию о заражениях, обнаруженных модулями ESET Mail Security. Регистрируется информация о времени обнаружения, типе модуля сканирования, типе объекта, имени объекта, имени заражения, месте обнаружения, выполненном действии и пользователе, который находился в системе при обнаружении заражения. Для копирования или удаления одной или нескольких строк журнала (или удаления всего журнала) используйте контекстное меню.

События

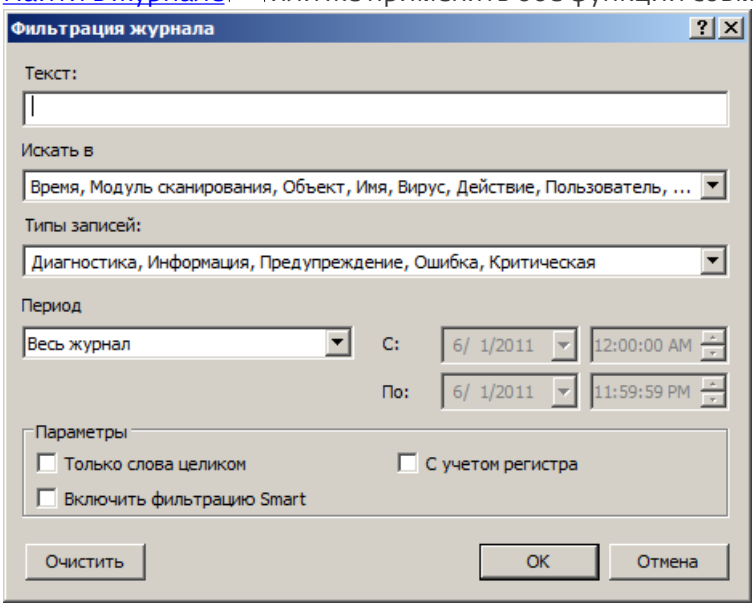
Журнал событий содержит информацию о событиях и ошибках, которые произошли во время работы программы. Зачастую информация, которая содержится в этом журнале, оказывается весьма полезной при решении проблем, возникающих в работе программы.

Сканирование ПК по требованию
Журнал модуля сканирования содержит информацию о результатах запущенного вручную сканирования или запланированного сканирования. Каждая строка соответствует одной проверке компьютера. Она содержит следующие данные: дата и время сканирования, общее количество просканированных, зараженных и очищенных фалов и текущее состояние сканирования.

Дважды щелкните запись в **журнале сканирования ПК по требованию**, чтобы вывести на экран подробное содержимое в новом окне.
Для того чтобы скопировать одну или несколько помеченных записей (из любого типа журнала), используйте контекстное меню (открывается щелчком правой кнопки мыши).

4.5.1 Фильтрация журнала

Фильтрация журнала — удобная функция, помогающая находить записи в файлах журнала, особенно когда записей много и сложно найти нужную информацию.
При использовании фильтрации можно ввести строку **поиска** для фильтра, указать, в каких **столбцах выполнять поиск**, выбрать **типы записей** и задать **период времени**, чтобы сократить количество записей. Если указать определенные параметры фильтрации, только отвечающие таким условиям записи отображаются в окне **Файлы журнала**, что обеспечивает удобный быстрый просмотр.
Для того чтобы открыть окно **Фильтрация журнала**, один раз нажмите кнопку **Фильтр...** в разделе **Служебные программы** > **Файлы журнала** или воспользуйтесь сочетанием клавиш Ctrl + Shift + F.
ПРИМЕЧАНИЕ: Для поиска конкретной записи можно использовать вместо фильтрации журнала функцию Найти в журнале 89 или же применять обе функции совместно.



Если указать определенные параметры фильтрации, только отвечающие таким условиям записи отображаются в окне «Файлы журнала». Это позволяет отфильтровать записи (сократить их количество), благодаря чему найти нужное будет проще. Чем более конкретные параметры фильтра используются, тем меньше результатов вы получите.
Что:: введите строку (слово целиком или частично). Будут показаны только записи, в которых содержится эта строка. Остальные записи не будут видимы, что позволяет удобнее работать с журналом.
Искать в столбцах:: выберите, какие столбцы будут учитываться при фильтрации. Для использования в фильтрации можно отметить один столбец или сразу несколько. По умолчанию отмечаются все столбцы:
- **Время**
- **Модуль**
- **Событие**
- **Пользователь**

Типы записей:: позволяет выбрать, записи какого типа следует показывать. Можно выбрать один конкретный тип записей, несколько типов одновременно или же показывать все типы записей (по умолчанию):
- **Диагностика**
- **Информация**
- **Внимание**
- **Ошибка**
- **Критические**

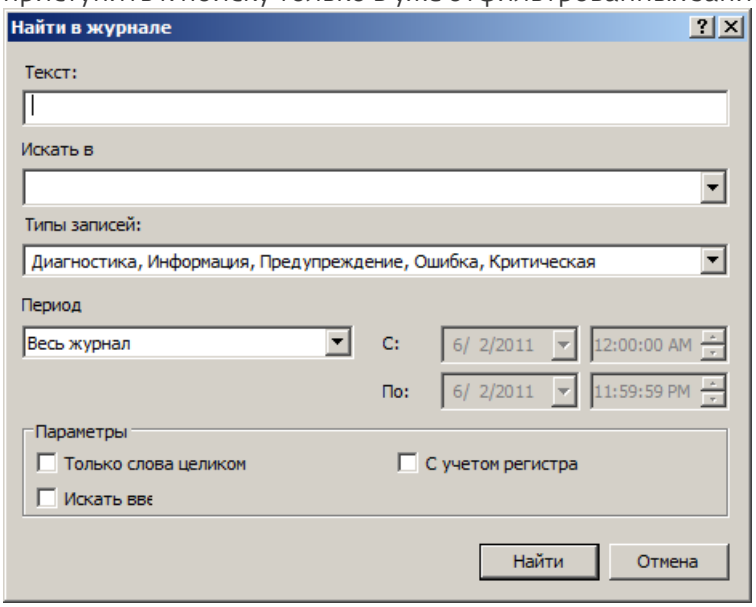
Период времени:: этот параметр позволяет фильтровать записи по времени. Можно выбрать одно из следующих значений.

- **Весь журнал** (по умолчанию): фильтрация по периоду времени не выполняется, отображается журнал целиком.
- **Последний день**
- **Последняя неделя**
- **Последний месяц**
- **Период**: если выбрать это значение, то можно указать конкретный период времени (дата и время), чтобы на экран выводились только те записи, регистрация которых относится к указанному периоду.

В дополнение к указанным выше параметрам фильтрации можно также использовать ряд **параметров**.
Только слова целиком: будут показаны только записи, соответствующие строке, введенной в текстовом поле **Что**, как целому слову.
С учетом регистра: будут показаны только записи, соответствующие строке, введенной в текстовом поле **Что**, с учетом регистра.
Включить фильтрацию Smart: этот параметр позволяет ESET Mail Security выполнять фильтрацию с применением своих собственных методов.
По окончании настройки параметров фильтрации нажмите кнопку **OK**, чтобы применить созданный фильтр. В окне **Файлы журнала** будут показаны только записи, соответствующие критериям фильтра.

4.5.2 Найти в журнале

В дополнение к фильтрации журнала 88 можно использовать в файлах журнала 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.
При использовании функции поиска в журнале можно ввести строку **поиска**, указать, в каких **столбцах выполнять поиск**, выбрать **типы записей** и задать **период времени**, чтобы искать только записи, относящиеся к этому периоду. Если указать определенные параметры поиска, только отвечающие таким условиям записи отображаются в окне «Файлы журнала».
Для выполнения поиска в журналах откройте окно **Найти в журнале**, нажав клавиши Ctrl + f.
ПРИМЕЧАНИЕ: Функцию «Найти в журнале» можно использовать в сочетании с фильтрацией журнала 88. Сначала можно сократить количество записей, воспользовавшись фильтрацией журнала, а затем приступить к поиску только в уже отфильтрованных записях.



Что:: 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**
- **Модуль**
- **Событие**
- **Пользователь**

Типы записей:: позволяет выбрать, записи какого типа следует искать. Можно выбрать один конкретный тип записей, несколько типов одновременно или же искать все типы записей (по умолчанию):

- **Диагностика**

- **Информация**
- **Внимание**
- **Ошибка**
- **Критические**

Период времени:: этот параметр позволяет находить только записи, относящиеся к определенному периоду времени. Можно выбрать одно из следующих значений.

- **Весь журнал** (по умолчанию): поиск по периоду времени не выполняется, поиск ведется в журнале целиком.
- **Последний день**
- **Последняя неделя**
- **Последний месяц**
- **Период**: если выбрать это значение, то можно указать конкретный период времени (дата и время), чтобы выполнялся поиск только тех записей, регистрация которых относится к указанному периоду.

В дополнение к указанным выше параметрам поиска можно также использовать ряд **параметров**.

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.

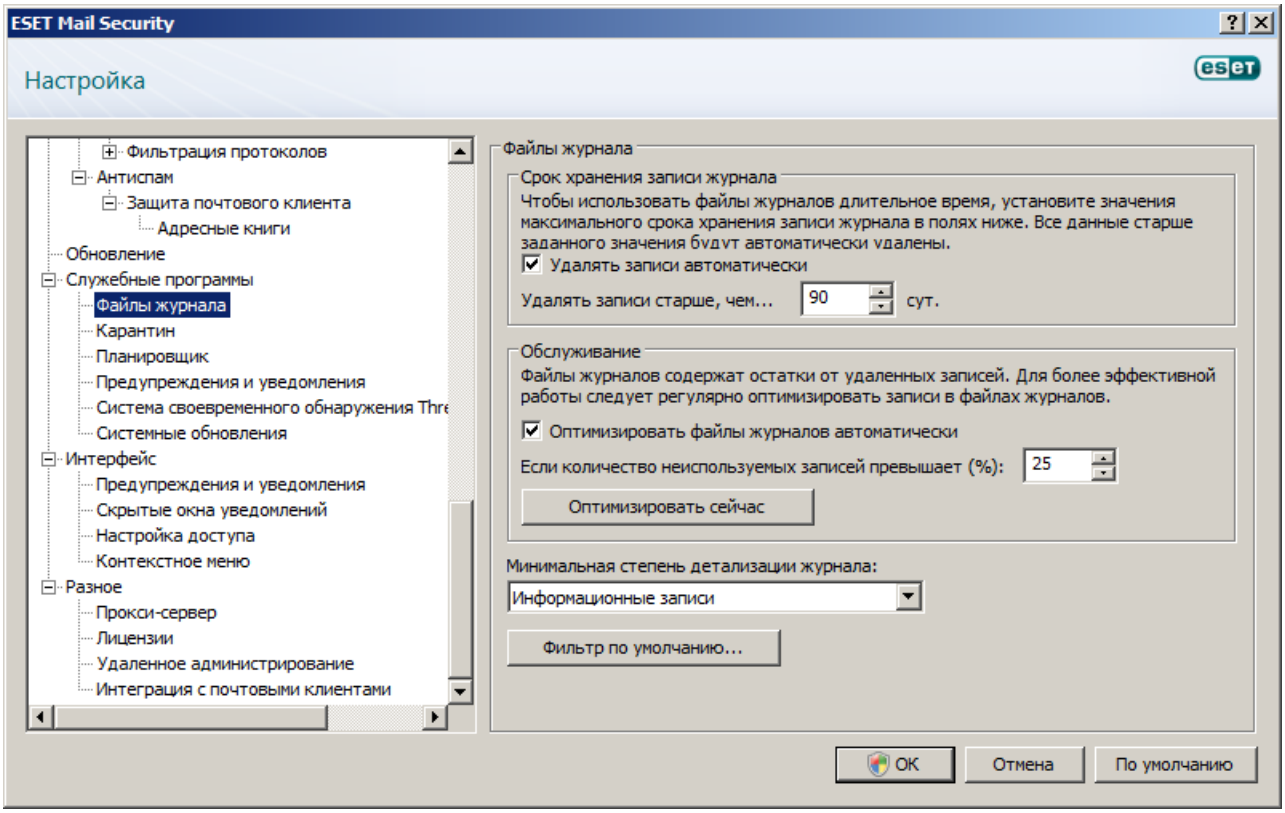
После конфигурирования параметров поиска нажмите кнопку **Найти**, чтобы приступить к поиску. Поиск прекращается, когда находится первая соответствующая его критериям запись. Снова нажмите кнопку **Найти**, чтобы продолжить поиск. Поиск в файлах журнала ведется сверху вниз, начиная с текущего положения (выделенной записи).

4.5.3 Обслуживание журнала

Настройку ведения журнала ESET Mail Security можно открыть из главного окна программы. Нажмите **Настройка** > **Ввод всего дерева расширенных параметров...** > **Служебные программы** > **Файлы журнала**. Для файлов журнала можно задать параметры, указанные ниже.

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

- **Диагностические записи**: записывается информация, необходимая для тонкой настройки программы, а также все перечисленные выше записи.
- **Информационные записи**: записываются информационные сообщения, в том числе сообщения об успешном выполнении обновления, а также все перечисленные выше записи.
- **Предупреждения**: записывается информация обо всех критических ошибках и предупреждениях.
- **Ошибки**: записываются только сообщения типа «Ошибка загрузки файла», а также критические ошибки.
- **Критические предупреждения**: регистрируются только критические ошибки (ошибки запуска защиты от вирусов и т. п.).



4.6 ESET SysInspector

4.6.1 Введение в ESET SysInspector

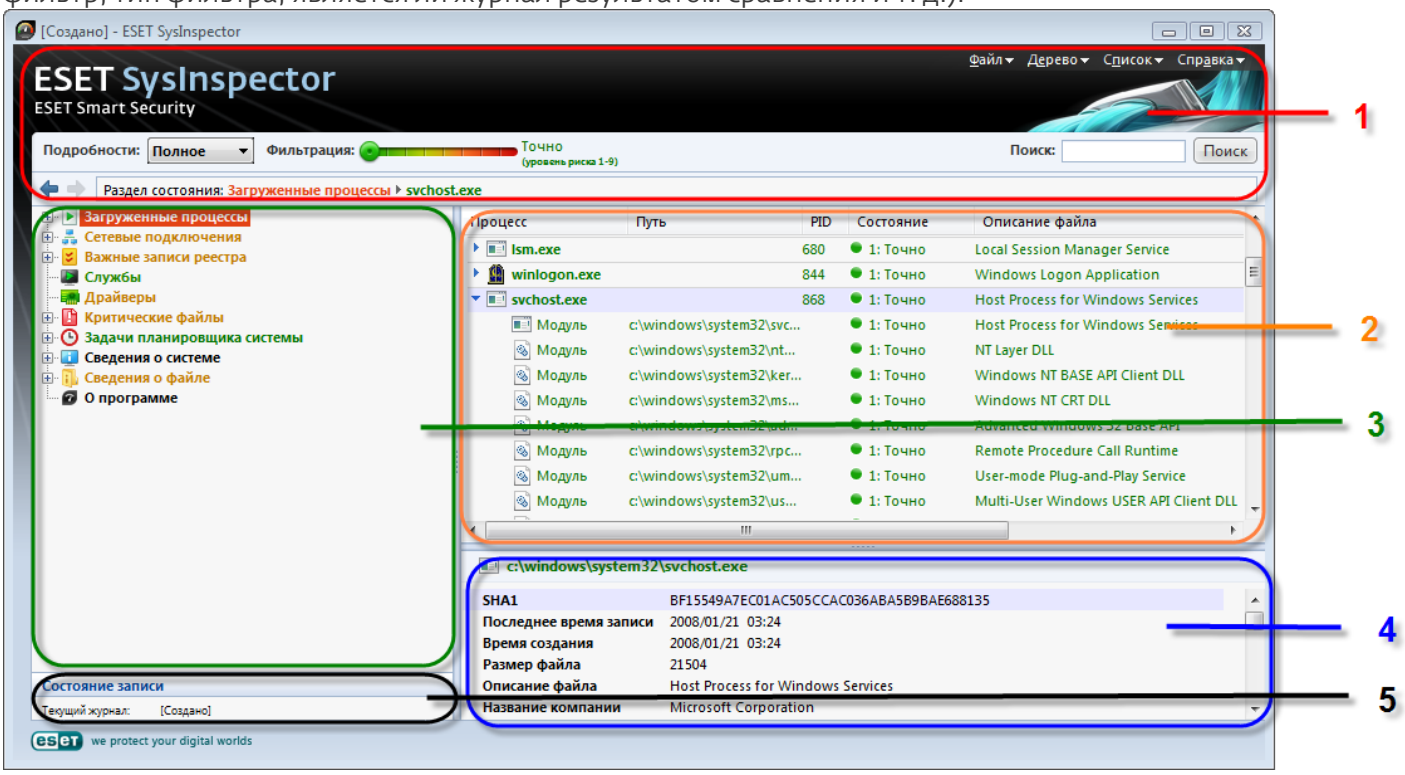
ESET SysInspector — это приложение, которое тщательно проверяет компьютер и отображает собранные данные в понятном виде. Представляемые данные, такие как информация об установленных драйверах и приложениях, сетевых подключениях и важных записях реестра, позволяют определить причину подозрительного поведения системы, которое может быть вызвано несовместимостью программного или аппаратного обеспечения или заражением вредоносными программами.
Существует два способа воспользоваться приложением SysInspector. Во-первых, можно открыть интегрированную в ESET Mail Security версию, а, во-вторых, загрузить самостоятельную версию (SysInspector.exe) бесплатно с веб-сайта ESET. Для того чтобы открыть SysInspector, активируйте расширенный режим, воспользовавшись сочетанием клавиш CTRL + M, и перейдите в раздел **Служебные программы** > **SysInspector**. Обе версии аналогичны по своим функциям и имеют одинаковые элементы управления программой. Единственное отличие заключается в том, как осуществляется управление результатами. И загружаемая, и интегрированная версии позволяют экспортировать снимки системы в файл в формате XML и сохранять его на диске. Однако интегрированная версия также дает возможность сохранять снимки системы непосредственно в разделе **Служебные программы** > **SysInspector** (для получения дополнительных сведений см. раздел SysInspector как часть ESET Mail Security 100).
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.

4.6.1.1 Запуск ESET SysInspector

Для запуска ESET SysInspector достаточно выполнить файл *SysInspector.exe*, загруженный с веб-сайта ESET. Если у вас уже установлен один из программных продуктов ESET для обеспечения безопасности, ESET SysInspector можно запустить непосредственно из меню «Пуск» («**Программы** > **ESET** > **ESET Mail Security**). Дождитесь окончания проверки системы приложением. Это может занять до нескольких минут в зависимости от оборудования и данных, которые нужно собрать.

4.6.2 Интерфейс пользователя и работа в приложении

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



4.6.2.1 Элементы управления программой

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

Файл

Элемент **Файл** позволяет 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 него исключается конфиденциальная информация (например, имя текущего пользователя, имена компьютера и домена, права текущего пользователя, переменные окружения и т. п.).

ПРИМЕЧАНИЕ. Чтобы просмотреть сохраненные ранее отчеты ESET SysInspector, достаточно просто перетащить их в главное окно приложения.

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 отображаемую в главном окне информацию, делая более удобной работу с ней. В режиме «Основное» пользователю доступна информация, необходимая для поиска решений распространенных проблем в системе. В режиме «Среднее» программа отображает реже используемые сведения. Режим «Полное» ESET SysInspector предназначен для вывода на экран всей информации, необходимой для решения самых нестандартных проблем.

Фильтрация элементов

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 отобразит только те элементы, уровень подозрительности которых выше отображаемого уровня. Если ползунок находится в крайнем правом положении, программа отображает

только определенно вредоносные элементы.
Все элементы с уровнем риска от 6 до 9 могут представлять угрозу для безопасности. Если вы не используете решения компании ESET для обеспечения безопасности, после нахождения приложением ESET SysInspector любого такого элемента рекомендуется проверить систему с помощью ESET Online Scanner. ESET Online Scanner является бесплатной службой.
ПРИМЕЧАНИЕ. Уровень риска элемента легко определяется путем сравнения цвета элемента с цветом на ползунке уровней рисков.
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 переходить в окне описания к ранее отображенной информации. Вместо кнопок перехода назад и вперед можно использовать клавишу 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.

4.6.2.2 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 из разделов, разверните вложенные узлы соответствующего узла. Для того чтобы открыть или свернуть узел, дважды щелкните название узла или нажмите значок ⊞ или ⊟ рядом с его названием. При перемещении по древовидной структуре узлов и вложенных узлов в окне навигации различные сведения о каждом узле отображаются в окне описания. При переходе к конкретному элементу в окне подробной информации отображаются дополнительные сведения о нем.
Ниже описаны основные узлы, отображаемые в окне навигации, и относящаяся к ним информация, доступная в окнах описания и подробных сведений.
Запущенные процессы
Этот узел содержит сведения о приложениях и процессах, выполняемых в момент создания журнала. В окне описания могут находиться дополнительные сведения о каждом из процессов, например названия динамических библиотек, используемых процессом, и их местонахождение в системе, название поставщика приложения и уровень риска файла.
Окно подробных сведений содержит дополнительную информацию об элементах, выделенных в окне описания, такую как размер файла или его хэш.
ПРИМЕЧАНИЕ. Любая операционная система состоит из нескольких компонентов ядра, которые постоянно выполняются и обеспечивают работу базовых принципиально важных функций 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.
Окно подробных сведений содержит дополнительную информацию об элементах, выделенных в окне описания, такую 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 может отображаться, какие файлы связаны с конкретными записями реестра. 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 критических файлов, относящихся к операционной системе

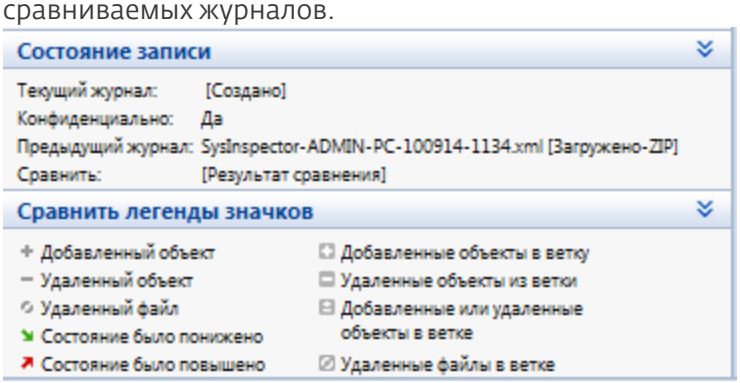
Microsoft Windows.
Информация о системе
Содержит подробные сведения об оборудовании и программном обеспечении, а также информацию о заданных переменных среды и правах пользователя.
Сведения о файле
Список важных системных файлов и файлов в папке Program Files. В окнах описания и подробных сведений может отображаться дополнительная информация о файлах.
О программе
Информация о приложении ESET SysInspector.

4.6.2.3 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 активности злонамеренного кода.
После запуска приложение создает новый журнал, который выводится на экран в новом окне. Для того 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 настоящий момент журнал и сохраненный в файле 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. Сравнительный журнал отображает только различия между этими двумя журналами.
ПРИМЕЧАНИЕ. При сравнении двух файлов журналов в меню **Файл** выберите пункт **Сохранить журнал** и сохраните журнал как файл в формате ZIP. В результате будут сохранены оба файла. Если позже открыть такой файл, содержащиеся в нем журналы будут автоматически сравниваться.
Напротив отображенных элементов SysInspector выводит символы, обозначающие различия между сравниваемыми журналами.
Элементы, помеченные символом «–», присутствуют только в активном журнале, но отсутствуют в открытом журнале, с которым он сравнивается. Элементы, отмеченные знаком +, присутствуют только в открытом журнале и отсутствуют в активном.
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 SysInspector и разрешите приложению 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

4.6.3 Параметры командной строки

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

/gen	создание журнала непосредственно из командной строки без запуска графического интерфейса пользователя
/privacy	создание журнала без включения в него конфиденциальной информации
/zip	сохранение журнала непосредственно на диск в сжатом файле
/silent	скрытие индикатора выполнения при создании журнала
/help, /?	отображение сведений о параметрах командной строки

Примеры
Чтобы открыть определенный журнал непосредственно в браузере, воспользуйтесь следующей командой: *SysInspector.exe "c:\клиентский_журнал.xml"*
Чтобы создать журнал в текущей папке, воспользуйтесь следующей командой: *SysInspector.exe /gen*
Чтобы создать журнал в определенной папке, воспользуйтесь следующей командой: *SysInspector.exe /gen="c:\папка\"*
Чтобы создать журнал в определенной папке и в определенном файле, воспользуйтесь следующей командой: *SysInspector.exe /gen="c:\папка\новый_журнал.xml"*
Чтобы создать журнал, из которого исключена конфиденциальная информация, непосредственно в сжатом файле, воспользуйтесь следующей командой: *SysInspector.exe /gen="c:\новый_журнал.zip" /privacy /zip*
Чтобы сравнить два журнала, воспользуйтесь следующей командой: *SysInspector.exe "текущий.xml" "исходный.xml"*
ПРИМЕЧАНИЕ. Если название файла или папки содержит пробел, это название необходимо заключить в кавычки.

4.6.4 Сценарий службы

Сценарий службы — это специальное средство, помогающее пользователям ESET SysInspector с легкостью удалять нежелательные объекты с компьютера.
Сценарий службы дает пользователям возможность целиком или частично экспортировать журнал SysInspector. После экспорта пользователь может пометить нежелательные объекты для удаления. Затем можно запустить сценарий с отредактированным журналом для удаления помеченных объектов.
Сценарий службы предназначен для пользователей, имеющих опыт в диагностике компьютерных систем. Неквалифицированные действия могут привести к повреждению операционной системы.
Пример
При наличии подозрения о заражении компьютера вирусом, который не обнаруживается программой защиты от вирусов, можно выполнить описанные далее указания.

- Запустите ESET SysInspector и создайте новый снимок системы.
- Выделите первый элемент в разделе слева (в древовидной структуре), нажмите клавишу CTRL, а затем выберите последний элемент, чтобы пометить все элементы.
- Щелкните правой кнопкой мыши выделенные объекты и выберите пункт контекстного меню **Экспортировать выбранные разделы в сценарий службы** .
- Выделенные объекты будут экспортированы в новый журнал.
- Далее следует наиболее важный этап всей процедуры. Откройте созданный журнал и измените атрибут «-» на «+» для всех объектов, которые нужно удалить. Следите за тем, что не помечаются никакие важные файлы или объекты операционной системы.
- Откройте ESET SysInspector, воспользуйтесь пунктом меню **Файл** > **Запустить сценарий службы** и введите путь к сценарию.
- Нажмите кнопку **OK**, чтобы запустить сценарий.

4.6.4.1 Создание сценариев службы

Для того чтобы создать сценарий, щелкните правой кнопкой мыши любой объект в древовидном меню (в левой панели) главного окна 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.

4.6.4.2 Структура сценария службы

Первая строка заголовка сценария содержит данные о версии ядра (ev), версии интерфейса (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 элементов 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 регистрация выбранных драйверов отменяется, а драйверы удаляются.

09) Critical files (Критические файлы)

Этот раздел содержит информацию о файлах, являющихся критическими для 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.

4.6.4.3 Выполнение сценариев службы

Пометьте все нужные объекты, сохраните и закройте сценарий. Запустите измененный сценарий непосредственно из главного окна SysInspector с помощью пункта **Запустить сценарий службы** из 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 появится подтверждение выполнения 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 следующее сообщение: **«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.

4.6.5 Сочетания клавиш

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	стандартная проверка состояния системы
Ctrl + H	выполнение проверки системы, при которой также может регистрироваться 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 + O	выбор режима фильтрации, только равный уровень

Просмотр

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

4.6.6 Системные требования

Для правильной работы ESET SysInspector система должна отвечать перечисленным ниже аппаратным и программным требованиям.

ОС Windows 2000, XP, 2003
Процессор 400 МГц, 32-разрядный (x86) или 64-разрядный (x64)
128 МБ оперативной памяти
10 МБ свободного места на диске
Монитор Super VGA (800 × 600)

ОС Windows 7, Vista, 2008
Процессор 1 ГГц, 32-разрядный (x86) или 64-разрядный (x64)
512 МБ оперативной памяти
10 МБ свободного места на диске
Монитор Super VGA (800 × 600)

4.6.7 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 выберите в главном меню команду **Файл** > **Сохранить журнал**. Журналы сохраняются в формате XML. По умолчанию файлы сохраняются в папке *%ПРОФИЛЬ_ПОЛЬЗОВАТЕЛЯ%\Мои документы* в файл с именем SysInpsector-%ИМЯ_КОМПЬЮТЕРА%-ГГММДД-ЧЧММ.XML. Перед сохранением файла журнала можно изменить его местоположение и название.

Как просмотреть файл журнала ESET SysInspector?
Чтобы просмотреть журнал, созданный в ESET SysInspector, запустите программу и выберите в главном меню команду **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 запрещено 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. По результатам этого эвристического анализа объектам присваивается уровень риска от **1 — ХОРОШО (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 на наличие необычного поведения.

Зачем ESET SysInspector в ходе работы подключается к Интернету?

Как и многие приложения, приложение ESET SysInspector подписано цифровой подписью («сертификатом»), которая гарантирует, что издателем данного программного обеспечения является компания ESET и что само программное обеспечение 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 подвергается атаке злонамеренного кода, который ведет себя как руткит, пользователь подвергается риску повреждения или воровства 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?

В ходе идентификации цифровой подписи исполняемого файла SysInspector сначала проверяет наличие в файле встроенной цифровой подписи. В этом случае найденная в файле цифровая подпись будет использоваться для проверки. Если же в файле отсутствует цифровая подпись, 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.

Пример.

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

4.6.8 SysInspector как часть ESET Mail Security

Для того чтобы в ESET Mail Security открыть раздел SysInspector, в меню **Служебные программы** выберите пункт **SysInspector**. В окне 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 SysInspector содержит основные сведения о созданных снимках состояния, такие как время, краткий комментарий, имя создавшего снимок пользователя, а также состояние снимка.

Для **сравнения**, **добавления** и **удаления** снимков используются соответствующие кнопки, расположенные в окне SysInspector под списком снимков. Эти функции также можно вызвать из контекстного меню. Для просмотра выбранного снимка системы используется команда контекстного меню **Просмотреть**. Чтобы экспортировать выделенный снимок в файл, щелкните его правой кнопкой и выберите в контекстном меню пункт **Экспорт...**.

Ниже приведено подробное описание доступных функций.

- **Сравнение** : сравнение двух существующих журналов. Эта функция удобна, если нужно найти различия между текущим и более старым журналом. Для использования этой функции нужно выбрать два снимка, которые следует сравнить.
- **Добавить** : создание новой 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** .
- **Удаление** : удаление записей из списка.
- **Экспорт...**: сохранение выбранной записи в XML-файле с возможностью упаковки в архив.

4.7 ESET SysRescue

ESET SysRescue — это утилита для создания загрузочного диска, содержащего ESET Mail Security. Главным преимуществом ESET SysRescue является то, что программа ESET Mail Security работает независимо от операционной системы компьютера, имея при этом доступ к жесткому диску и всей файловой системе. Это позволяет удалять такие заражения, которые в обычной ситуации (например, при запущенной операционной системе и т. п.) удалить невозможно.

4.7.1 Минимальные требования

ESET SysRescue работает в среде предустановки Microsoft Windows версии 2.x, созданной на основе Windows Vista. Среда предустановки Windows является частью бесплатного пакета автоматической установки Windows (Windows AIK), поэтому перед созданием компакт-диска ESET SysRescue необходимо установить Windows AIK (http://go.eset.eu/AIK). Поскольку поддержка среды предустановки Windows ограничивается ее 32-разрядной версией, необходимо использовать 32-разрядный установочный пакет ESET Mail Security при создании ESET SysRescue в 64-разрядных операционных системах. Средство ESET SysRescue поддерживает пакет Windows AIK версии 1.1 и более поздних. Средство ESET SysRescue доступно в составе ESET Mail Security версии 4.0 и более поздних.

Поддерживаемые операционные системы

- Windows 7
- Windows Vista
- Windows Vista с пакетом обновления 1
- Windows Vista с пакетом обновления 2
- Windows Server 2008
- Windows Server 2003 с пакетом обновления 1 с KB926044
- Windows Server 2003 с пакетом обновления 2
- Windows XP с пакетом обновления 2 с KB926044
- Windows XP с пакетом обновления 3

4.7.2 Создание компакт-диска аварийного восстановления

Чтобы запустить мастер ESET SysRescue, выберите в меню **Пуск** > **Программы** > **ESET** > **ESET Mail Security** > **ESET SysRescue**.

На первом этапе мастер определяет наличие в системе установленного пакета Windows AIK и подходящего для создания загрузочного носителя устройства записи. Если пакет *Windows AIK* не установлен на компьютере, установлен некорректно или поврежден, мастер предложит установить этот пакет или ввести путь к папке с Windows AIK (http://go.eset.eu/AIK).

На следующем этапе 101 предлагается выбрать носитель для размещения на нем файлов ESET SysRescue.

4.7.3 Выбор объекта

Помимо компакт-диска, DVD-диска и USB-устройства, ESET SysRescue также можно сохранить в файл образа диска ISO. Впоследствии этот файл с образом ISO можно записать на компакт- или DVD-диск или использовать его другим способом (например, в виртуальной среде VMware или VirtualBox).

Если в качестве целевого носителя было выбрано USB-устройство, загрузка с него может не работать на некоторых компьютерах. Некоторые версии BIOS могут сообщать о наличии проблем при обмене данными между BIOS и диспетчером загрузки (например, в Windows Vista), в результате чего загрузка завершается следующим сообщением об ошибке:

```
file : \boot\bcd
status : 0xc000000e
info : an error occurred while attemping to read the boot configuration data (ошибка при попытке чтения конфигурационн
```

При появлении этого сообщения рекомендуется выбрать в качестве носителя компакт-диск вместо USB-устройства.

4.7.4 Параметры

Прежде чем приступать к созданию ESET SysRescue, мастер установки выводит на экран параметры компиляции на последнем этапе работы ESET SysRescue. Их можно изменить, нажав кнопку **Изменить...**. Доступны следующие параметры.

- Папки 102
- Антивирус ESET 102
- Дополнительно 102
- Интернет-протокол 103
- Загружаемое устройство USB 103 (если в качестве объекта выбрано USB-устройство)
- Запись 103 (если в качестве объекта выбран дисковод компакт-/DVD-дисков)

Если не указан установочный пакет MSI или на компьютере не установлено никакое решение обеспечения безопасности ESET, кнопка **Создать** будет неактивна. Чтобы выбрать установочный пакет, нажмите кнопку **Изменить** и перейдите на вкладку **Антивирус ESET**. Если не ввести имя пользователя и пароль (**Изменить** > **Антивирус ESET**), кнопка **Создать** также будет неактивна.

4.7.4.1 Папки

Папка временного хранения — это рабочий каталог для файлов, необходимый для компиляции ESET SysRescue.
Папка ISO — это папка, в которую сохраняется полученный файл ISO после завершения компиляции.
В списке на этой вкладке перечислены все локальные и сопоставленные сетевые диски с указанием доступного на них места. Если какие-то из показанных папок располагаются на диске, где свободного места недостаточно, рекомендуется выбрать другой диск, на котором места больше. В противном случае недостаток свободного места приведет к досрочному завершению компиляции.
Внешние приложения: позволяет указать дополнительные программы, которые будут выполняться или устанавливаться после загрузки с носителя ESET SysRescue.
Включить внешние приложения: позволяет добавить внешние программы в компиляцию ESET SysRescue.
Выбранная папка: папка, где расположены программы, которые следует добавить на диск ESET SysRescue.

4.7.4.2 Антивирус ESET

При создании компакт-диска ESET SysRescue можно выбрать один из двух источников файлов ESET для компилятора.
Папка ESS/EAV — файлы, уже содержащиеся в папке, в которую установлен программный продукт ESET.
MSI-файл — файлы, которые содержатся в установщике MSI.
Затем можно принять решение, следует ли обновлять расположение файлов с расширением .nup. Обычно следует выбрать параметр по умолчанию **Папка ESS/EAV/MSI-файл**. В некоторых случаях можно выбрать собственную папку **Папка обновлений**, например для использования более старой или новой версии базы данных сигнатур вирусов.
В качестве источника имени пользователя и пароля может послужить один из следующих двух вариантов.
Установленная программа ESS/EAV: имя пользователя и пароль копируются из установленной программы ESET Mail Security.
От пользователя: имя пользователя и пароль вводятся в соответствующие текстовые поля, расположенные ниже.
ПРИМЕЧАНИЕ. Программа ESET Mail Security на компакт-диске ESET SysRescue обновляется либо через Интернет, либо из решения ESET Security, установленного на компьютере, на котором запускается компакт-диск ESET SysRescue.

4.7.4.3 Дополнительные параметры

На вкладке **Дополнительно** можно оптимизировать параметры компакт-диска ESET SysRescue в соответствии с объемом оперативной памяти компьютера. Чтобы записать содержимое компакт-диска в оперативную память (ОЗУ), выберите вариант **576 МБ и больше**. Если выбрать пункт **менее 576 МБ**, при работе среды предустановки Windows будет постоянно происходить обращение к компакт-диску восстановления.
В разделе **Внешние драйверы** можно вставить драйверы для конкретного оборудования (обычно для сетевого адаптера). Хотя среда предустановки Windows основана на ОС Windows Vista с пакетом обновления 1, которая поддерживает самое разнообразное оборудование, иногда оборудование все же не распознается. В этом случае нужно будет добавить драйвер вручную. Добавить драйвер в компиляцию ESET SysRescue можно двумя способами: вручную (кнопка **Добавить**) и автоматически (кнопка **Авто поиск**). При добавлении драйвера вручную необходимо указать путь к соответствующему INF-файлу (в той же папке должен находиться и SYS-файл). В случае автоматического добавления драйвер находится в операционной

системе данного компьютера автоматически. Режим автоматического добавления рекомендуется использовать только в том случае, если средство ESET SysRescue установлено на компьютере с такой же сетевой картой, как и на компьютере, на котором был создан диск ESET SysRescue. При создании диска ESET SysRescue драйвер добавляется в компиляцию, поэтому пользователю впоследствии не приходится его искать.

4.7.4.4 Интернет-протокол

В этом разделе можно конфигурировать базовую информацию о сети и настраивать предопределенные подключения после работы ESET SysRescue.
Выберите вариант **Автоматический частный IP-адрес**, чтобы получить IP-адрес автоматически с DHCP-сервера.
Либо же этим сетевым подключением может использоваться введенный вручную IP-адрес (также называется статическим IP-адресом). Выберите вариант **Выборочная**, чтобы сконфигурировать соответствующие параметры IP. Если выбрать этот вариант, нужно заполнить поле **IP-адрес**, а для локальных сетей и высокоскоростных подключений к Интернету также поле **Маска подсети**. В поля **Предпочтительный сервер DNS** и **Дополнительный сервер DNS** следует ввести адреса основного и дополнительного DNS-серверов.

4.7.4.5 Загружаемое устройство USB

Если в качестве целевого носителя было выбрано USB-устройство, на вкладке **Загрузочное USB-устройство** можно указать одно из доступных USB-устройств (если их несколько).
Выберите нужное **Устройство**, на котором будет установлено приложение ESET SysRescue.
Внимание: Выбранное USB-устройство будет отформатировано при создании ESET SysRescue. Все данные на этом устройстве будут удалены.
Если выбрать вариант **Быстрое форматирование**, при форматировании будут удалены все файлы из раздела, но диск не будет сканироваться на наличие поврежденных секторов. Используйте эту возможность, если USB-устройство уже было отформатировано ранее и вы уверены, что оно не повреждено.

4.7.4.6 Запись

Если в качестве целевого носителя выбран компакт- или DVD-диск, на вкладке **Запись** можно задать дополнительные параметры записи.
Удалить файл ISO: установите этот флажок, чтобы удалить временный ISO-файл после создания компакт-диска ESET SysRescue.
Удаление разрешено: этот параметр позволяет сделать выбор между быстрой и полной очисткой диска.
Записывающее устройство: выберите дисковод, который будет использоваться для записи.
Предупреждение. Этот параметр установлен по умолчанию. При использовании перезаписываемого компакт- или DVD-диска все данные на нем будут стерты.
В разделе «Носитель» указаны сведения о диске в дисководе.
Скорость записи: выберите нужную скорость из раскрывающегося меню. При выборе скорости необходимо учитывать возможности записывающего устройства и тип компакт- или DVD-диска.

4.7.5 Работа с ESET SysRescue

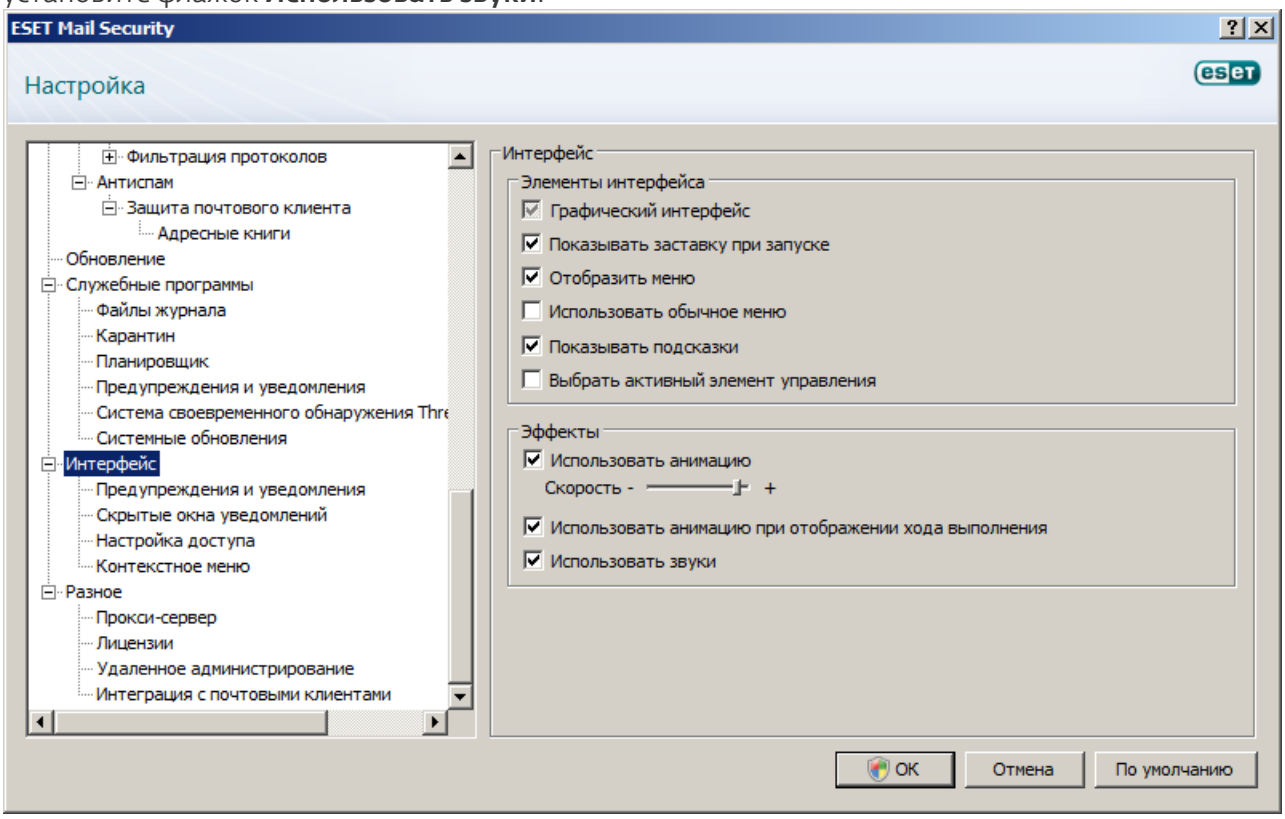
Для эффективного использования аварийного восстановления с компакт- и DVD-дисков или USB-устройств необходимо загрузить компьютер с загрузочного носителя, на котором установлено средство ESET SysRescue. Порядок загрузки настраивается в BIOS. Также на этапе загрузки компьютера можно использовать меню загрузки; обычно оно вызывается с помощью клавиш F9–F12 в зависимости от версии материнской платы и BIOS.
После загрузки с загрузочного носителя будет запущено приложение ESET Mail Security. Поскольку средство ESET SysRescue используется лишь в особых случаях, некоторые модули защиты и функции программы, имеющиеся в стандартной версии ESET Mail Security, не нужны, а потому их список сужен до функций **сканирования компьютера**, **обновления** и некоторых разделов **настройки**. Возможность обновлять базу данных сигнатур вирусов является самой важной функцией ESET SysRescue, рекомендуется обновить программу, прежде чем приступать к сканированию компьютера.

4.7.5.1 Использование ESET SysRescue

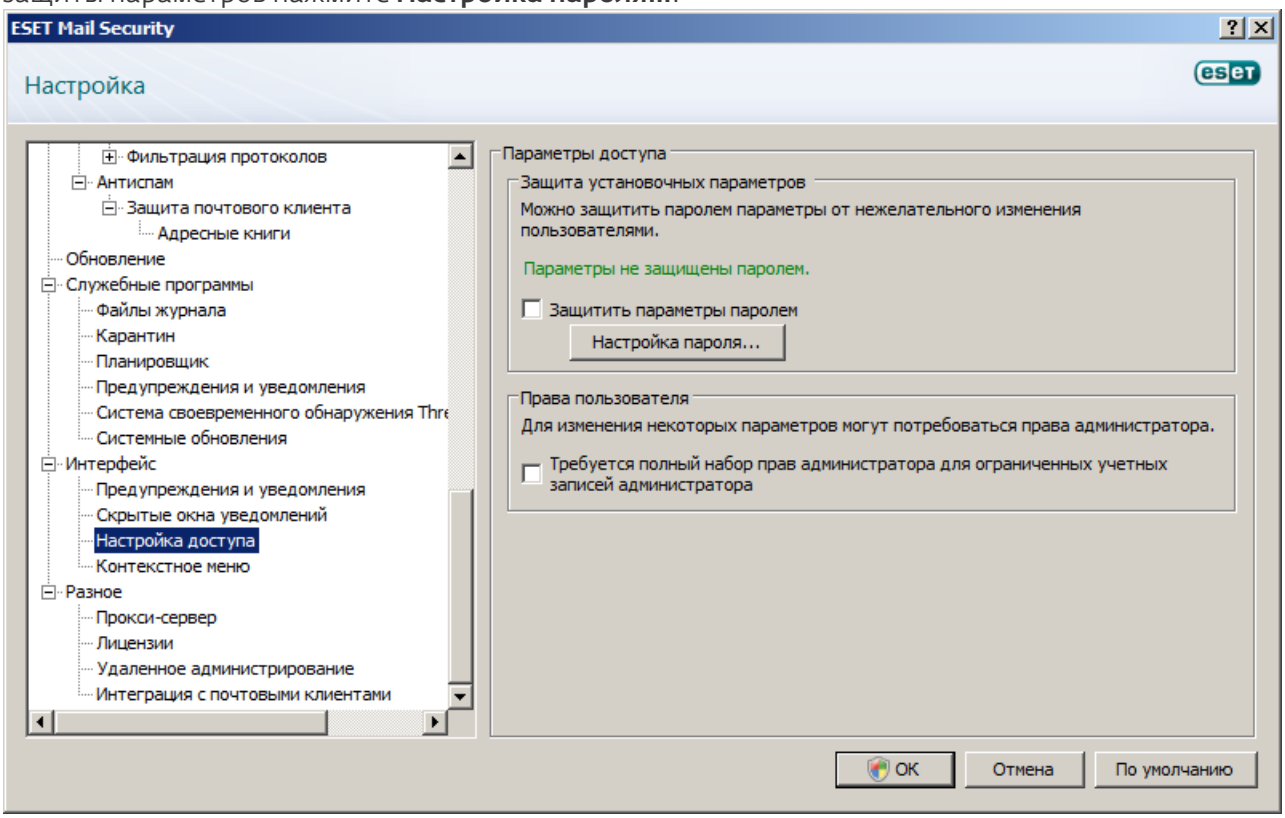
Предположим, что компьютеры в сети были заражены вирусом, который вносит изменения в исполняемые файлы (.exe). ESET Mail Security может очистить все зараженные файлы кроме *explorer.exe*, который невозможно очистить даже в безопасном режиме.
Это связано с тем, что *explorer.exe*, будучи одним из важнейших процессов Windows, запускается также и в безопасном режиме. ESET Mail Security не сможет выполнить никаких действий с файлом, из-за чего он останется зараженным.
В такой ситуации можно использовать ESET SysRescue для решения этой проблемы. Средству ESET SysRescue не нужны никакие компоненты операционной системы компьютера, а потому оно может обработать (очистить, удалить) любой файл на диске.

4.8 Параметры интерфейса пользователя

Параметры интерфейса пользователя в ESET Mail Security позволяют настроить рабочую среду в соответствии с конкретными требованиями. Эти параметры доступны в ветви **Интерфейс** дерева расширенных параметров ESET Mail Security.
В разделе **Элементы интерфейса** параметр **Расширенный режим** дает пользователям возможность включать и отключать расширенный режим. В расширенном режиме отображаются более подробные параметры и дополнительные элементы управления для ESET Mail Security.
Флажок **Графический интерфейс** следует снять, если отображение графических элементов снижает производительность компьютера или вызывает другие проблемы. Графический интерфейс также может быть необходимо отключить пользователям с ослабленным зрением, поскольку он может конфликтовать со специальными приложениями, используемыми для работы с отображаемым на экране текстом.
Если нужно отключить заставку ESET Mail Security, снимите флажок **Показывать заставку при запуске**.
В верхней части главного окна программы ESET Mail Security находится обычное меню, которое можно активировать или отключить с помощью флажка **Использовать обычное меню**.
Если установлен флажок **Показывать подсказки**, при наведении курсора на какой-либо элемент на экран будет выводиться его краткое описание. При установленном флажке **Выбрать активный элемент управления** система будет выделять любой элемент, в данный момент находящийся в активной области курсора мыши. Выделенный элемент активируется нажатием кнопки мыши.
Для уменьшения или увеличения скорости анимированных эффектов установите флажок **Использовать анимацию** и переместите ползунок **Скорость** влево или вправо.
Для того чтобы использовать анимированные значки для отображения хода выполнения различных операций, установите флажок **Использовать анимацию при отображении хода выполнения**. Если программа должна воспроизводить звуковое предупреждение при возникновении важного события, установите флажок **Использовать звуки**.



Функции **интерфейса пользователя** также позволяют защищать параметры ESET Mail Security паролем. Этот параметр расположен в подменю **Защита настроек** раздела **Интерфейс**. Для обеспечения максимальной безопасности компьютера принципиально важно правильно сконфигурировать программу. Несанкционированное изменение может привести к потере важных данных. Для установки пароля для защиты параметров нажмите **Настройка пароля...**.



4.8.1 Предупреждения и уведомления

Раздел **Настройка предупреждений и уведомлений** (является подчиненным по отношению к разделу **Интерфейс**) позволяет сконфигурировать обработку системных уведомлений и предупреждений об угрозах в ESET Mail Security.

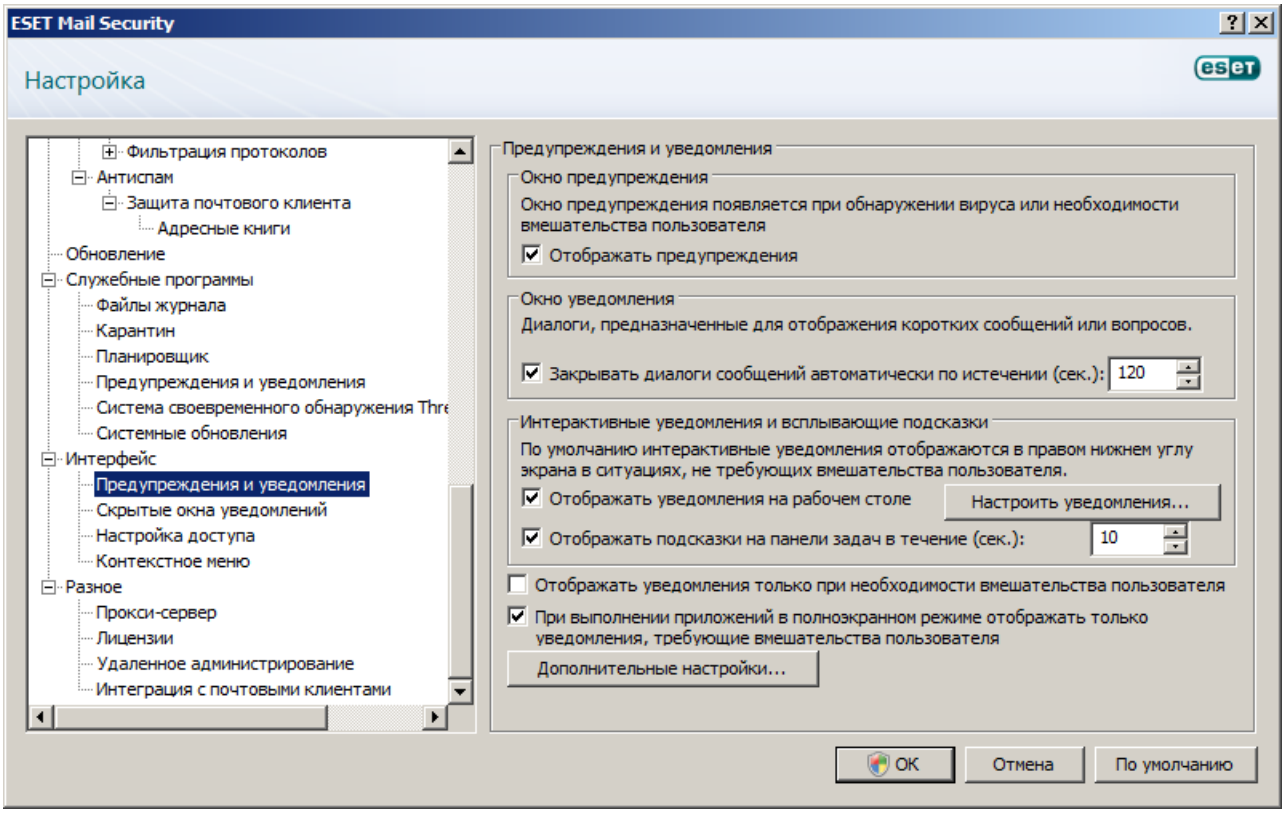
Первый пункт — **«Окно предупреждения»**. Если этот флажок снят, окна предупреждения не будут выводиться на экран. Такой подход следует использовать только в небольшом количестве особых ситуаций. В большинстве случаев рекомендуется оставить для этого параметра значение по умолчанию (включен).

Для того чтобы всплывающие окна закрывались автоматически по истечении определенного периода времени, установите флажок **Закрывать диалоги сообщений автоматически по истечении (сек.)**. Если окно предупреждения не будет закрыто пользователем, оно закрывается автоматически через указанный промежуток времени.

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.

Для того чтобы активировать отображение уведомлений на рабочем столе, установите флажок **Отображать уведомления на рабочем столе**. Более подробные параметры — время отображения и прозрачность окна — доступны с помощью кнопки **Настроить уведомления...**.

Для предварительного просмотра уведомлений нажмите кнопку **Просмотр**. Параметр **«Отображать подсказки на панели задач в течение (сек.)»** предназначен для настройки времени отображения всплывающих подсказок.



Нажмите **Дополнительные настройки...**, чтобы ввести расширенные параметры **предупреждений и уведомлений**, среди которых есть также и вариант **Отображать уведомления только при необходимости вмешательства пользователя**. Этот параметр позволяет включать и выключать отображение предупреждений и уведомлений, которые не требуют вмешательства со стороны пользователя. Установите флажок **При выполнении приложений в полноэкранном режиме отображать только уведомления, требующие вмешательства пользователя**, чтобы запретить все неинтерактивные уведомления. В раскрывающемся меню **Минимальная детализация отображаемых событий** можно выбрать начальный уровень серьезности предупреждений и уведомлений, которые следует отображать.
Последний параметр этого раздела позволяет сконфигурировать, кто именно должен получать уведомления в многопользовательской среде. Поле **В многопользовательских системах отображать уведомления для пользователя** позволяет решить, кто именно будет получать важные уведомления от ESET Mail Security. Обычно это системный или сетевой администратор. Этот параметр особенно полезен для серверов терминалов при условии, что все системные уведомления отправляются администратору.

4.8.2 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 для сеансов терминала, выполните следующие действия.

1. Запустите *regedit.exe*
2. Найдите запись *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*
3. Щелкните правой кнопкой мыши значение *egui* и выберите пункт контекстного меню *Изменить...*
4. Добавьте параметр `/terminal` в конец существующей строки

Ниже приведен пример данных значения *egui* :

```
"C:\Program Files\ESET\ESET Mail Security\egui.exe" /hide /waitservice /terminal
```

Если нужно отменить этот параметр и включить автоматический запуск графического интерфейса пользователя ESET Mail Security, удалите параметр `/terminal` . Для перехода к значению реестра *egui* повторите действия 1–3

4.9 Командная строка

Модуль защиты от вирусов программного обеспечения ESET Mail Security может быть запущен из командной строки вручную (с помощью команды «ecls») или в пакетном режиме (с помощью файла «bat»).
Следующие параметры и аргументы могут быть использованы при запуске сканирования по требованию из командной строки.

Общие параметры

- help	показать справку и выйти
- version	показать сведения о версии и выйти
- base-dir = ПАПКА	загрузить модули из ПАПКИ
- quar-dir = ПАПКА	ПАПКА карантина
- aind	показывать индикатор работы

Объекты

- files	сканировать файлы (по умолчанию)
- no-files	не сканировать файлы
- boots	сканировать загрузочные секторы (по умолчанию)
- no-boots	не сканировать загрузочные секторы
- arch	сканировать архивы (по умолчанию)
- no-arch	не сканировать архивы
- max-archive-level = УРОВЕНЬ	максимальный УРОВЕНЬ вложенности архивов
- scan-timeout = ИНТЕРВАЛ	сканировать архивы не дольше указанного ИНТЕРВАЛА в секундах. При достижении этого предельного значения сканирование архива останавливается, а сам процесс переходит к следующему файлу.
- max-arch-size=РАЗМЕР	сканировать только первый кусок файла РАЗМЕРОМ в байтах (по умолчанию 0 = не ограничено)
- mail	сканировать файлы электронной почты
- no-mail	не сканировать файлы электронной почты
- sfx	сканировать самораспаковывающиеся архивы
- no-sfx	не сканировать самораспаковывающиеся архивы
- rtp	сканировать упаковщики
- no-rtp	не сканировать упаковщики
- exclude = ПАПКА	исключить ПАПКУ из сканирования
- subdir	сканировать вложенные папки (по умолчанию)
- no-subdir	не сканировать вложенные папки
- max-subdir-level = УРОВЕНЬ	максимальный УРОВЕНЬ вложенности папок (по умолчанию 0 = не ограничено)
- symlink	следовать по символическим ссылкам (по умолчанию)
- no-symlink	пропускать символические ссылки
- ext-remove = РАСШИРЕНИЯ	
- ext-exclude = РАСШИРЕНИЯ	исключить из сканирования РАСШИРЕНИЯ, разделенные двоеточием

Методы

- adware	сканировать на наличие рекламных/шпионских/опасных программ
- no-adware	не сканировать на наличие рекламных/шпионских/опасных программ
- unsafe	сканировать на наличие потенциально опасных приложений
- no-unsafe	не сканировать на наличие потенциально опасных приложений
- unwanted	сканировать на наличие потенциально нежелательных приложений
- no-unwanted	не сканировать на наличие потенциально нежелательных приложений
- pattern	использовать сигнатуры
- no-pattern	не использовать сигнатуры
- heur	включить эвристический анализ
- no-heur	отключить эвристический анализ
- adv-heur	включить расширенную эвристику
- no-adv-heur	отключить расширенную эвристику

Очистка

- action = ДЕЙСТВИЕ	применить ДЕЙСТВИЕ к зараженным объектам. Возможные действия: «none» (ничего), «clean» (очистка), «prompt» (запрос)
- quarantine	копировать зараженные файлы в карантин (дополнительно к ДЕЙСТВИЮ)
- no-quarantine	не копировать зараженные файлы в карантин

Журналы

- log-file=ФАЙЛ	вывод журнала в ФАЙЛ
- log-rewrite	перезаписывать выходной файл (по умолчанию добавлять)
- log-all	регистрировать также незараженные файлы
- no-log-all	не регистрировать незараженные файлы (по умолчанию)

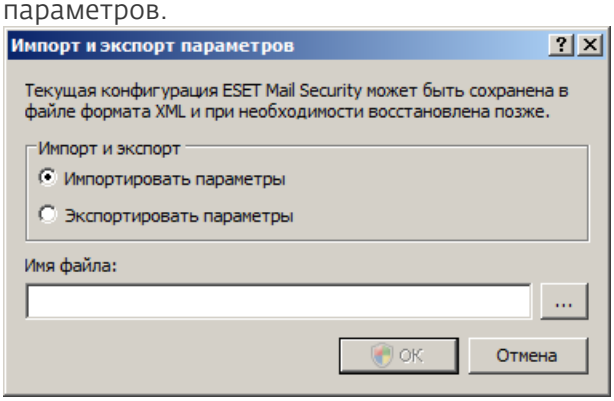
Возможные коды завершения сканирования

0	угроз не обнаружено
1	угроза обнаружена, но не очищена
10	остались зараженные файлы
101	ошибка архива
102	ошибка доступа
103	внутренняя ошибка

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

4.10 Импорт и экспорт параметров

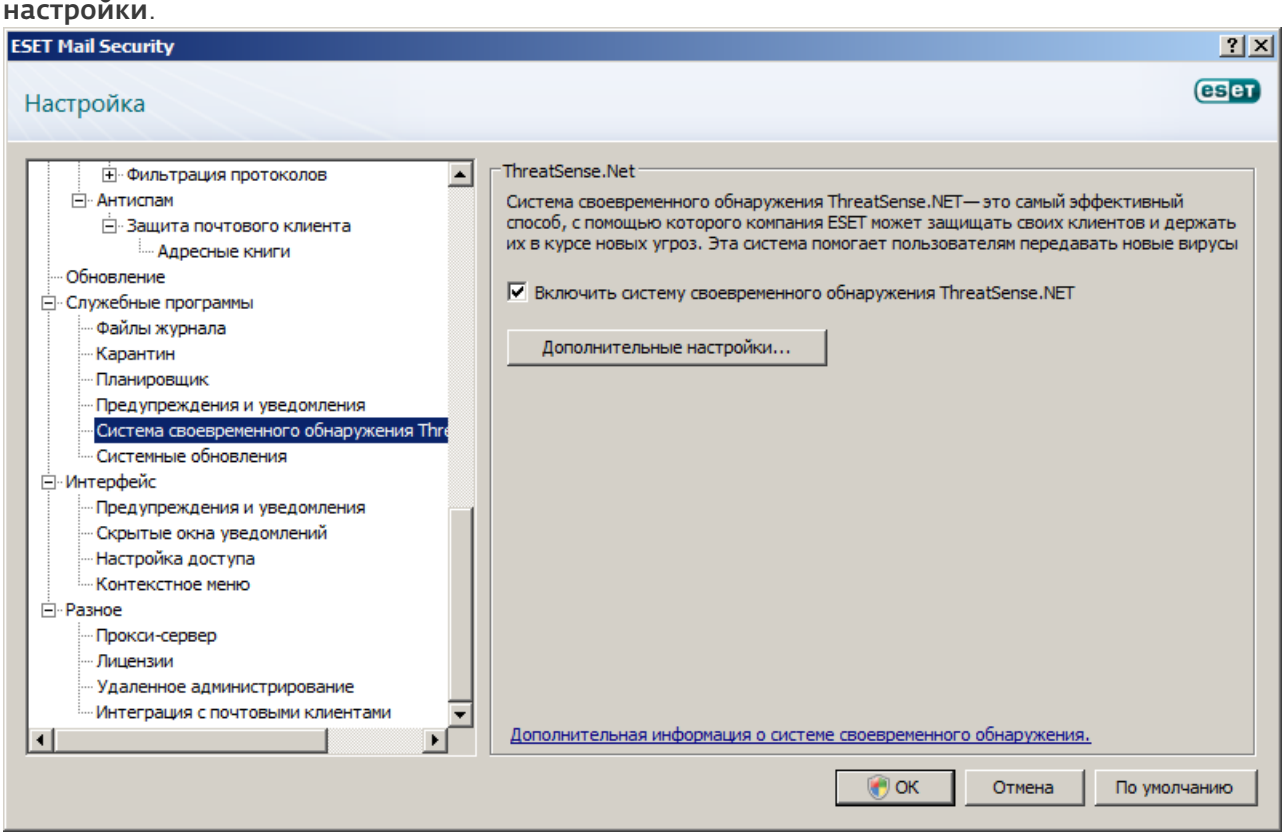
Импорт и экспорт конфигураций ESET Mail Security выполняется в разделе **Настройка**. Для этого используется ссылка **Импорт и экспорт параметров**.
И для импорта, и для экспорта используются файлы в формате XML. Импорт и экспорт удобны, если нужно создать резервную копию текущей конфигурации ESET Mail Security для дальнейшего использования. Экспорт параметров также полезен, если необходимо использовать выбранную конфигурацию ESET Mail Security на нескольких компьютерах. Для этого файл XML можно легко импортировать для переноса нужных параметров.



4.11 ThreatSense.Net

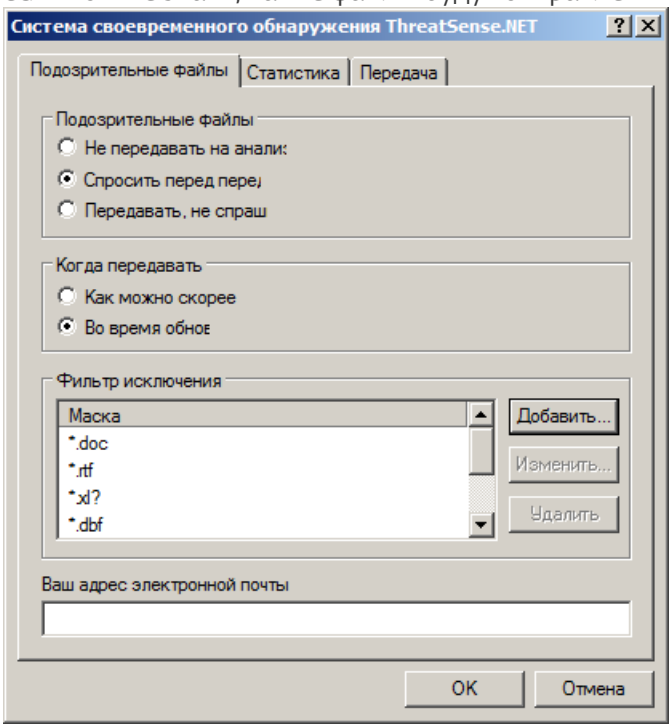
Система своевременного обнаружения ThreatSense.Net оперативно непрерывно уведомляет компанию ESET о новых заражениях. Действующая в обоих направлениях система своевременного обнаружения ThreatSense.Net имеет единственное предназначение — сделать защиту компьютера пользователя еще более надежной. Лучшим способом обеспечить обнаружение новых угроз сразу после их появления является сбор информации от как можно большего числа пользователей. Существует два варианта работы.
1. Пользователь отключает систему своевременного обнаружения ThreatSense.Net. Функциональность программного обеспечения при этом не ограничивается, и пользователь все равно получает наилучшую защиту.
2. Можно разрешить системе своевременного обнаружения ThreatSense.Net отправлять анонимную информацию о новых угрозах и файлах, содержащих неизвестный пока опасный код. Файл может быть отправлен в ESET для тщательного анализа. Изучение этих угроз поможет компании ESET обновить средства обнаружения угроз.
Система своевременного обнаружения ThreatSense.Net 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.
Поскольку в отправляемую в лабораторию ESET информацию могут иногда попадать сведения о пользователе и его компьютере (например, имя пользователя в пути к файлу), компания ESET заверяет, что такая информация будет использоваться исключительно для немедленного реагирования на новые угрозы.
По умолчанию программа ESET Mail Security запрашивает разрешение на отправку подозрительных файлов в лабораторию ESET для тщательного анализа. Всегда исключаются файлы с определенными расширениями, такими как .doc и .xls. Также можно добавить другие расширения, если политика вашей организации предписывает исключение из отправки.

Параметры системы своевременного обнаружения ThreatSense.Net доступны через дерево расширенных параметров в разделе **Служебные программы** > **ThreatSense.Net**. Установите флажок **Включить систему быстрого оповещения ThreatSense**, чтобы активировать ее, и нажмите кнопку **Дополнительные настройки**.



4.11.1 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. Можно настроить автоматическую отправку файлов или же выбрать вариант **Спросить перед передачей**, если хотите знать, какие файлы будут отправлены на анализ, и подтверждать данное действие.



Если вы не хотите отправлять 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 110).
Когда передавать: по умолчанию для отправки подозрительных файлов в лабораторию ESET выбран

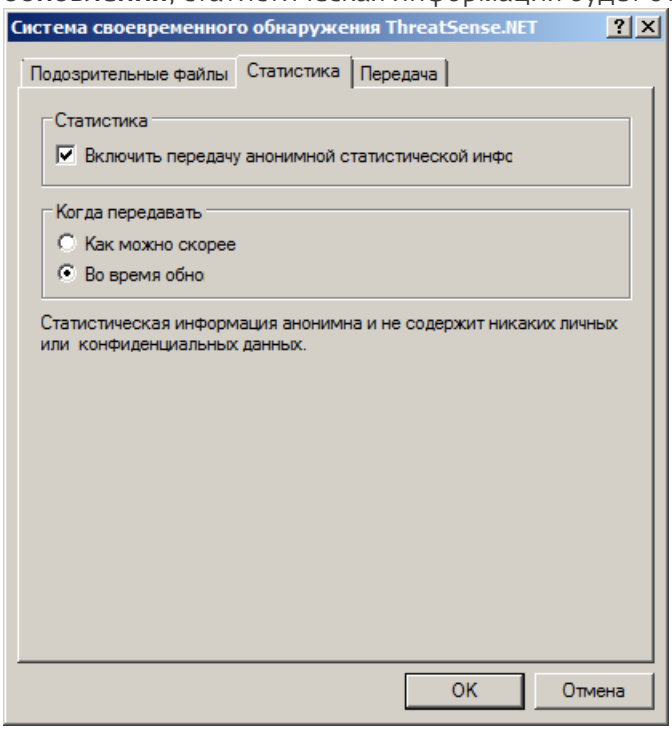
вариант **Как можно скорее**. Этот вариант рекомендуется использовать, если существует постоянное подключение к Интернету, а подозрительные файлы могут доставляться без задержек. Установите флажок **Во время обновления**, чтобы подозрительные файлы загружались в ThreatSense.Net при следующем обновлении.
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 можно дополнять список исключенных файлов.
Адрес электронной почты (необязательно): можно отправить адрес электронной почты вместе с подозрительными файлами, чтобы специалисты ESET могли обратиться к вам, если для анализа потребуется дополнительная информация. Имейте в виду, что компания ESET не отправляет ответы пользователям без необходимости.

4.11.2 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 отправляется на серверы ESET один или два раза в день.
Пример отправляемого пакета со статистикой представлен ниже.

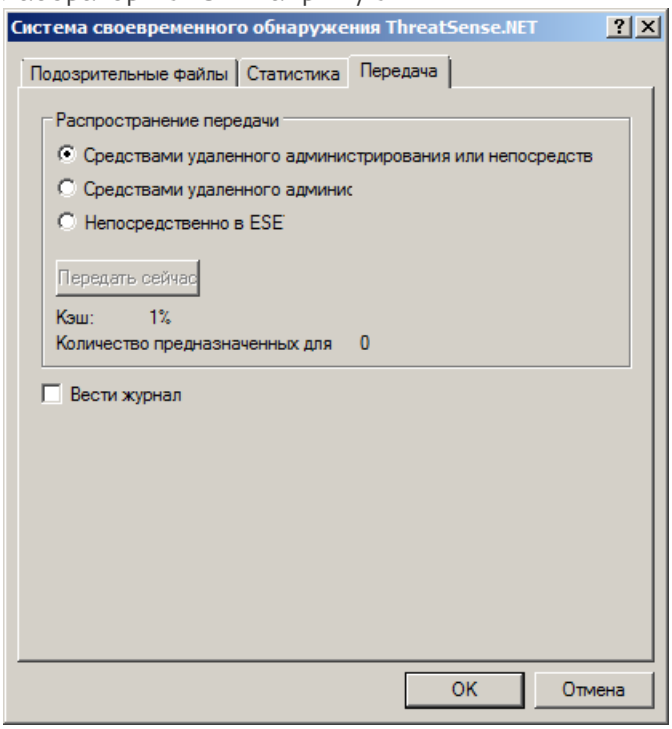
```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C14J8NS7\rdgFR1
```

Когда отправлять: можно указать, когда будет отправляться статистическая информация. Если выбрать вариант **Как можно скорее**, статистическая информация будет отправляться сразу после сбора. Этот вариант уместен при наличии постоянного подключения к Интернету. Если выбран вариант **Во время обновления**, статистическая информация будет отправляться одним пакетом при следующем обновлении.



4.11.3 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 уже обеспечивает их отправку в лабораторию ESET. При выборе варианта **Непосредственно в ESET** подозрительные файлы и статистика отправляются программой в лабораторию ESET напрямую.

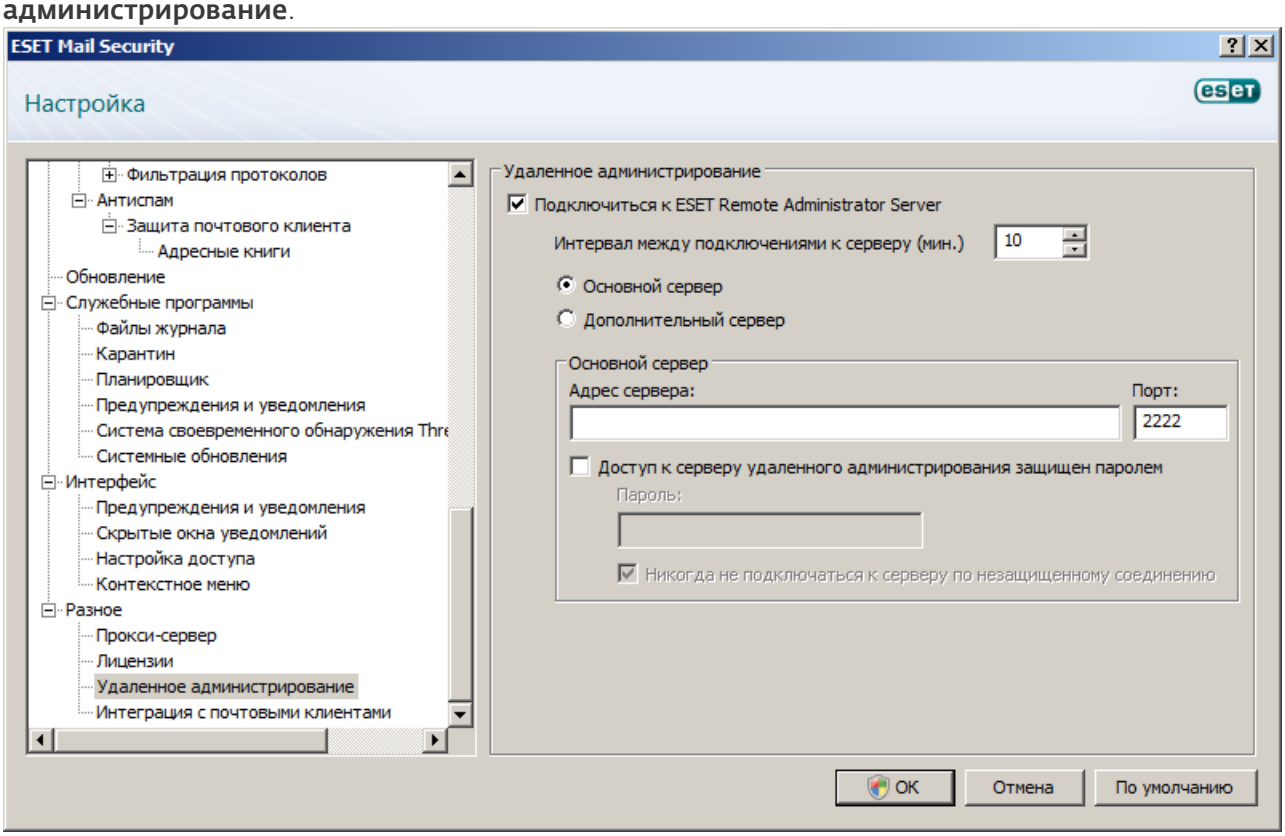


Если есть ожидающие отправки файлы, будет доступна кнопка **Передать сейчас**. Нажмите эту кнопку, чтобы немедленно отправить файлы и статистическую информацию.

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

4.12 Удаленное администрирование

ESET Remote Administrator (ERA) — это полезное средство, используемое для управления политикой безопасности и получения общих сведений о безопасности сети. Это особенно полезно в больших сетях. Средство ERA не только повышает уровень безопасности, но и облегчает администрирование ESET Mail Security на клиентских рабочих станциях.
Параметры удаленного администрирования доступны из главного окна программы ESET Mail Security. Нажмите **Настройка** > **Ввод всего дерева расширенных параметров...** > **Разное** > **Удаленное администрирование**.



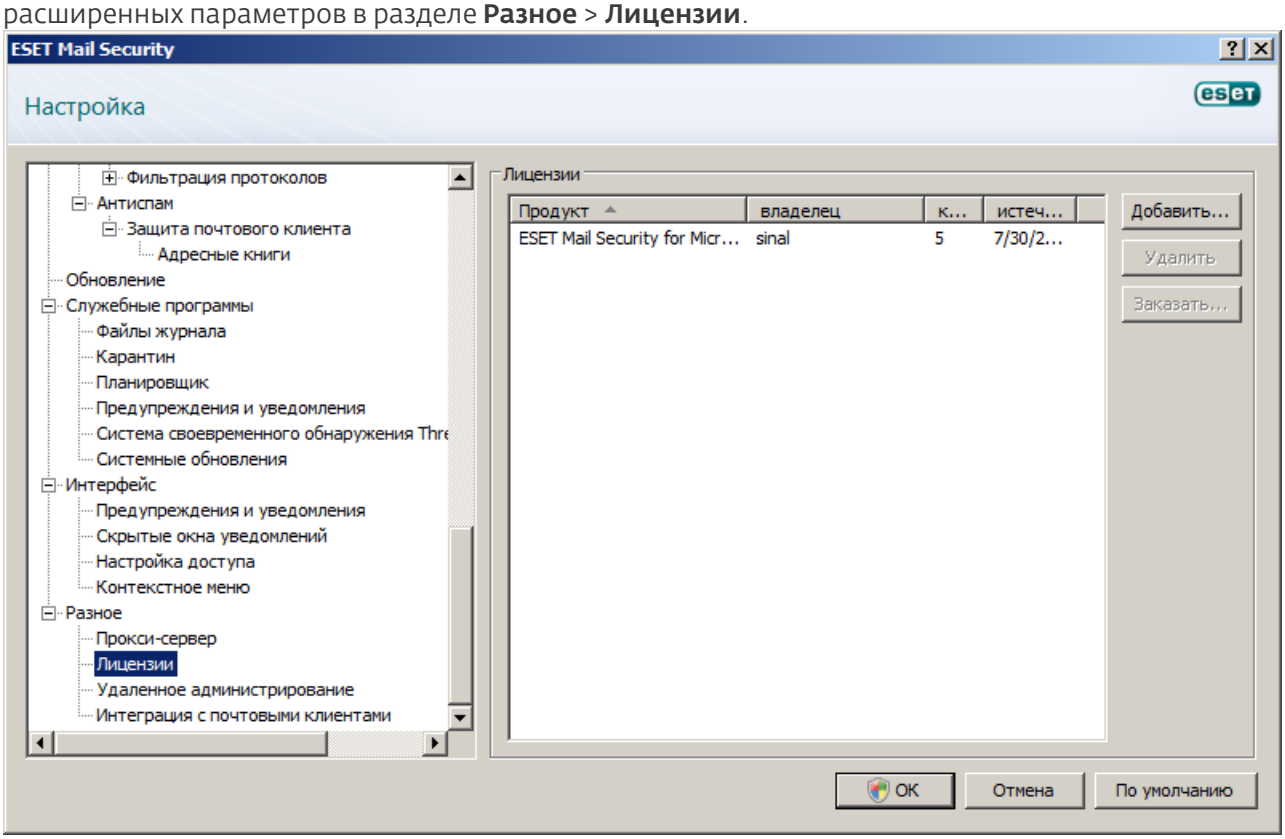
Активируйте удаленное администрирование, установив флажок **«Подключиться к серверу Remote Administrator Server»**. После этого станут доступны остальные описанные далее параметры.

- **Интервал между подключениями к серверу (мин.)** : этим параметром задается частота подключения ESET Mail Security к серверу ERA Server. Если установлено значение 0, данные отправляются каждые 5 секунд.
- **Адрес сервера:**: сетевой адрес сервера, на котором установлен сервер ERA Server.
- **Порт:** в этом поле указан предварительно заданный порт сервера, используемый для соединения. Рекомендуется не изменять порт по умолчанию (2222).
- **Для доступа к серверу Remote Administrator требуется аутентификация**: позволяет ввести пароль для подключения к серверу ERA Server, если он необходим.

Нажмите кнопку **OK**, чтобы подтвердить внесение изменений, и примените параметры. ESET Mail Security будет использовать эти параметры для подключения к серверу ERA Server.

4.13 Лицензии

В ветви **Лицензии** можно управлять лицензионными ключами для ESET Mail Security и других программных продуктов ESET, таких как ESET Mail Security и прочие. После покупки лицензионные ключи доставляются вместе с именем пользователя и паролем. Для добавления или удаления лицензионного ключа нажмите соответствующую кнопку в окне менеджера лицензий. Менеджер лицензий можно открыть через дерево расширенных параметров в разделе **Разное** > **Лицензии**.



Лицензионный ключ представляет собой текстовый файл, содержащий информацию о приобретенном продукте: владелец лицензии, количество лицензий и дата окончания срока действия.
В окне менеджера лицензий можно загрузить и просмотреть содержимое лицензионного ключа, нажав кнопку **Добавить...**, после чего на экран будет выведена соответствующая информация. Для того чтобы удалить файлы лицензии из списка, нажмите **Удалить**.
Если срок действия лицензионного ключа истек и вы хотите продлить лицензию, нажмите кнопку **Заказать...**, после чего вы перейдете в наш интернет-магазин.

5. Глоссарий

5.1 Типы заражений

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

5.1.1 Вирусы

Компьютерный вирус — это такой вид заражения, который повреждает существующие файлы на компьютере. Название было выбрано из-за сходства с биологическими вирусами, так как 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 концу заражаемого файла. Компьютерный вирус функционирует следующим способом: 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, так как могут целенаправленно удалять файлы с жесткого диска. С другой стороны, некоторые вирусы не причиняют никакого вреда. Они просто раздражают пользователя и демонстрируют возможности своих авторов.
Важно отметить, что количество вирусов постоянно снижается по сравнению с троянскими и шпионскими программами, так как 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.

5.1.2 Черви

Компьютерные черви — это содержащие злонамеренный код программы, которые атакуют главные компьютеры и распространяются через сеть. Основное различие между вирусами и червями заключается в том, что черви могут реплицироваться и распространяться самостоятельно, так как они не зависят от зараженных файлов или загрузочных секторов. Черви распространяются, используя адресную книгу пользователя или уязвимости в системе безопасности сетевых приложений.
Поэтому черви намного более подвижны, чем компьютерные вирусы. Благодаря широкой популярности Интернета они могут распространяться по всему земному шару за считаные часы или даже минуты после запуска. Эта способность быстро самостоятельно реплицироваться делает черви более опасными, чем другие типы вредоносных программ.
Действующий в системе червь может доставить множество неудобств пользователю: он может удалять файлы, снижать производительность системы или даже отключать другие программы. По сути компьютерный червь может служить в качестве «транспортного средства» для других типов заражений.
Если компьютер заражен червем, рекомендуется удалить зараженные файлы, поскольку они с большой вероятностью содержат злонамеренный код.
Примеры широко известных червей: Lovsan/Blaster, Stration/Warezov, Bagle и Netsky.

5.1.3 Троянские программы

Исторически троянскими программами называли такой класс заражений, которые пытаются маскироваться под полезные программы, тем самым заставляя пользователя 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 как можно более простое 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.
Так как эта категория весьма широка, ее часто разбивают на несколько подкатегорий.

- **Загрузчик** — вредоносная программа, способная загружать другие заражения из Интернета.
- **Dropper** — тип троянской программы, которая предназначена для заражения компьютеров другими вредоносными программами.
- **Backdoor** — приложение, которое обменивается данными со злоумышленниками, позволяя 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, которая предназначена 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, которые 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, так как он с большой вероятностью содержит злонамеренный код.
Примеры широко известных троянских программ:: NetBus, Trojandownloader. Small.ZL, Slapper.

5.1.4 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 не активны. Многие системы защиты от вирусов способны устранить руткиты на этом уровне (при условии, что они действительно обнаруживают такие файлы как зараженные).
2) Обнаружение при попытке скрыться во время обычной проверки. В распоряжении пользователей ESET Mail Security есть преимущества технологии Anti-Stealth, которая позволяет обнаружить и устранить активные руткиты.

5.1.5 Рекламные программы

Под рекламной программой понимается программное обеспечение, поддерживаемое рекламой. Программы, демонстрирующие пользователю рекламные материалы, относятся к этой категории. Частыми признаками работы рекламных программ являются появление всплывающих окон с рекламой в веб-браузере или изменение домашней страницы. Рекламные программы часто распространяются в комплекте с бесплатными программами. Это позволяет их создателям покрывать расходы на разработку полезных (как правило) программ.
Сами по себе рекламные программы не опасны, но они раздражают пользователей. Опасность заключается в том, что в рекламных программах могут быть реализованы дополнительные функции слежения, подобно шпионским программам.
Если пользователь решает использовать бесплатный программный продукт, ему следует уделить особое внимание установке. Чаще всего программа установки предупреждает об установке дополнительной рекламной программы. Часто пользователь имеет возможность отказаться от ее установки и установить только сам программный продукт без рекламной программы.
Некоторые программы нельзя установить без рекламных модулей либо их функциональность будет ограничена. Это приводит к тому, что рекламная программа часто получает доступ к системе на «законных» основаниях, так как пользователь дал согласие на ее установку. В этом случае лучше перестраховаться. В случае обнаружения на компьютере файла, классифицированного как рекламная программа, рекомендуется удалить его, так как скорее всего он содержит злонамеренный код.

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

Примерами хорошо известных бесплатных программных продуктов, вместе с которыми поставляются шпионские программы, могут служить клиентские приложения пиринговых (P2P) сетей. Программы Spyfalcon и Spy Sheriff (и многие другие) относятся к особой подкатегории шпионских программ. Утверждается, что они предназначены для защиты от шпионских программ, но на самом деле они сами являются таковыми.
В случае обнаружения на компьютере файла, классифицированного как шпионская программа, рекомендуется удалить его, так как с высокой вероятностью он содержит злонамеренный код.

5.1.7 Потенциально опасное ПО

Существует множество нормальных программ, предназначенных для упрощения администрирования подключенных к сети компьютеров. Однако злоумышленники могут использовать их для причинения вреда. Программное обеспечение ESET Mail Security позволяет обнаруживать такие угрозы.
В качестве «потенциально опасных приложений» выступает нормальное коммерческое программное обеспечение. В эту категорию входят такие программы, как средства удаленного доступа, приложения для взлома паролей и клавиатурные шпионы 114 (программы, регистрирующие 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.

5.1.8 Потенциально нежелательное ПО

Потенциально нежелательные приложения не обязательно являются вредоносными, но могут отрицательно влиять на производительность компьютера. Обычно для установки 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 перечислены далее.

- Открываются новые окна, которые не появлялись ранее.
- Активируются и выполняются скрытые процессы.
- Повышается уровень потребления системных ресурсов.
- Появляются изменения в результатах поиска.
- Приложение обменивается данными с удаленными серверами.

5.2 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 незаконных действий, таких 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.

5.2.1 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.

5.2.2 Мистификации

Мистификацией называется ложная информация, распространяющаяся через Интернет. Обычно мистификации рассылаются по электронной почте или с помощью таких средств общения, как ICQ и Skype. Собственно сообщение часто представляет собой шутку или городскую легенду.
Связанные с компьютерными вирусами мистификации направлены на то, чтобы вызвать в получателях страх, неуверенность и мнительность, побуждая их верить в то, что «не поддающийся обнаружению вирус» удаляет их файлы, крадет пароли или выполняет какие-либо другие крайне нежелательные действия с компьютерами.
Некоторые мистификации работают, предлагая получателям переслать сообщение своим знакомым, 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.

5.2.3 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 (такой как финансового учреждения или страховой компании). Сообщение может казаться благонадежным и содержать изображения и текст, которые могли изначально быть получены от источника, якобы являющегося отправителем данного сообщения. Под разными предлогами (проверка данных, финансовые операции) предлагается предоставить какую-либо личную информацию, такую как номера банковских счетов, имена пользователя, пароли и т. д. Если такие данные предоставляются, они легко могут быть украдены и использованы в преступных целях.
Банки, страховые компании и другие легитимные организации никогда не запрашивают имена пользователей и пароли в незапрошенных сообщениях электронной почты.

5.2.4 Распознавание мошеннических сообщений

Вообще существует несколько признаков, которые могут помочь распознать спам (нежелательные сообщения) в почтовом ящике. Если сообщение соответствует хотя бы нескольким из этих критериев, оно, наиболее вероятно, является нежелательным.

- Адрес отправителя отсутствует в адресной книге получателя.
- Предлагается получить большую сумму денег, но сначала нужно оплатить небольшую сумму.
- Под разными предлогами (проверка данных, финансовые операции) предлагается предоставить какие-либо личные данные, такие как номера банковских счетов, имя пользователя, пароль и т. д.
- Сообщение написано на иностранном языке.
- Предлагается 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.

5.2.4.1 Правила

В контексте решений для защиты от спама и почтовых клиентов под правилами понимаются инструменты обработки электронной почты. Правило состоит из двух логических частей:
1) условие (например, получение сообщения с определенного адреса);
2) действие (например, удаление сообщения, перемещение его в указанную папку).
Количество и сочетания правил зависят от конкретного решения по защите от спама. Правила предназначены для борьбы со спамом (нежелательными сообщениями). Стандартные примеры приведены далее.

- 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.

5.2.4.2 Байесовский фильтр

Байесовская фильтрация спама 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 байесовский фильтр может присвоить каждому сообщению определенный «индекс спама», показывающий, является ли данное сообщение спамом.
Основным преимуществом байесовского фильтра 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.

5.2.4.3 «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[119] назначением. «Белые» списки сравнительно просто поддерживать, значительно проще, чем «черные». Для большей эффективности фильтрации спама рекомендуется использовать и «белый», и «черный» списки.

5.2.4.4 «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»[118], и «черный» список, чтобы максимально эффективно отфильтровывать спам.

5.2.4.5 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.