ESET NOD32 Smart Security

Интегрированные компоненты:
Антивирус ESET NOD32
Антишпион ESET NOD32
Персональный файервол ESET
Антиспам ESET

Новое поколение технологии NOD32

Руководство пользователя

we protect your digital world

Содержание

ESET NOD32 Smart Security

Международная техническая поддержка: www.eset.com/support
Техническая поддержка (Европа): www.eset.eu/support
Русскоязычная техническая поддержка
тел: +7 (495) 727-35-48
e-mail: support@esetnod32.ru

Лицензионное соглашение

ВАЖНО: Перед загрузкой, установкой, копированием или использованием продукта прочитайте изложенные ниже положения о применении этого программного продукта. **ЗАГРУЖАЯ, УСТАНАВЛИВАЯ, КОПИРУЯ ИЛИ ИСПОЛЬЗУЯ ЭТОТ ПРОДУКТ, ВЫ ВЫРАЖАЕТЕ СВОЕ СОГЛАСИЕ С ИЗЛОЖЕННЫМИ УСЛОВИЯМИ И ПОЛОЖЕНИЯМИ.**

Лицензионное соглашение об использовании программного обеспечения конечными пользователями

Это соглашение об использовании программного обеспечения («Соглашение») заключено и исполняется: компанией ESET, spol. s r. o., зарегистрированной по адресу Pionierska 9/A, 831 02 Bratislava в коммерческом регистре окружного суда Bratislava I. Section Sro, Insertion No 3586/B, BIN: 31 333 535 («Поставщик») и Вами, физическим или юридическим лицом, выступающим в качестве конечного пользователя (далее просто «Пользователь»), и подтверждает предоставленное Вам право на использование Программного обеспечения, определенного в статье 1 настоящего Соглашения. Экземпляр Программного обеспечения, определенного в статье 1 настоящего Соглашения, может храниться на носителях формата CD-ROM или DVD, быть отправлен по электронной почте, загружен через Интернет, загружен с серверов Поставщика или получен из других источников, которые удовлетворяют положениям и условиям, перечисленным ниже.
ЭТОТ ДОКУМЕНТ НЕ ЯВЛЯЕТСЯ КОНТРАКТОМ НА ЗАКУПКУ, НО ЯВЛЯЕТСЯ СОГЛАШЕНИЕМ НА ПРАВО ИСПОЛЬЗОВАНИЯ КОНЕЧНЫМ ПОЛЬЗОВАТЕЛЕМ. Поставщик остается владельцем экземпляра Программного обеспечения и материального носителя, если таковой присутствует, на котором Программное обеспечение было поставлено в торговой упаковке, а также всех копий Программного обеспечения, на которые Пользователь имеет право в соотвествии с настоящим Соглашением.
Нажатие кнопки «Я согласен» в процессе загрузки, установки, копирования или использования этого Программного обеспечения выражает Ваше согласие с положениями и нормами, утвержденными в Соглашении. Если Вы не согласны с каким-либо из положений этого Соглашения, нажмите кнопку «Не согласен» или «Отклонить», прекратите процесс загрузки или установки.
ИСПОЛЬЗОВАНИЕ ВАМИ ЭТОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОЗНАЧАЕТ, ЧТО ВЫ ПРОЧЛИ ЭТО СОГЛАШЕНИЕ, ПОНЯЛИ ЕГО ПОЛОЖЕНИЯ И СОГЛАСНЫ ПРИНЯТЬ ОПИСАННЫЕ В НЕМ ОБЯЗАТЕЛЬСТВА.

1. Программное обеспечение. Программное обеспечение, относительно которого заключено настоящее Соглашение, включает в себя (а) экземпляр компьютерной программы компании ESET и все её части, (б) содержимое материального носителя: дисков, компакт-дисков, DVD-дисков, отчетов по электронной почте и их вложений, если таковые существуют, а также других носителей, с которыми поставляется это Соглашение, включая Программное обеспечение, поставляемое в виде объектного кода на компакт-дисках, DVD-дисках или посредством электронной почты через Интернет, (в) любые руководства и документации, которые относятся к Программному обеспечению, что включает в себя следующий список (но не ограничивается им): любое описание Программного обеспечения, его спецификации, описания параметров, руководства по использованию, описание интерфейса Программного обеспечения, инструкции по эксплуатации и установке и любые другие описания по использованию Программного обеспечения («Документация»), (г) копии Программного обеспечения, исправления ошибок в коде Программного обеспечения, если таковые существуют, дополнения Программного обеспечения, расширения Программного обеспечения, усовершенствованные версии Программного обеспечения, новые версии Программного обеспечения, а также все обновления любых частей Программного обеспечения, если таковые поставляются, в отношении которых Поставщик дает вам право на использование этой Лицензии в соответствии со статьей 4 настоящего документа. Поставщик поставляет Программное обеспечение только в форме исполняемого кода.

2. Отправка зараженных файлов и информации Поставщику. Программное обеспечение содержит функции для сбора образцов новых компьютерных вирусов и других вредоносных программ (далее просто «Вирусы») и последующей отправки их Поставщику, совместно с информацией о компьютере и/или платформе, на которой установлено Программное обеспечение («Информация»). Информация может содержать данные, в том числе регистрационные данные о пользователе или других пользователях компьютера, на котром установлено Программное обеспечение, данные о самом компьютере и операционной системе, информацию о файлах компьютера, на котором установлено Программное обеспечение и о файлах, подвергшихся заражению, а также подробную информацию о зараженных файлах. Поставщик обязуется использовать полученную Информацию и Вирусы только для изучения Вирусов и принимает все разумные меры для сохранения Информации в тайне от третьих лиц. Если Вы принимаете положения этого Соглашения и включаете описанную выше функцию Программного обеспечения, Вы согласны передавать Вирусы и Информацию Поставщику. В то же время Вы даете право Поставщику обрабатывать полученную информацию в рамках соответствующих законодательных норм.

3. Установка. Программное обеспечение поставляется на материальном носителе: компакт-дисках, DVD-дисках; отправляется посредством электронной почты, загружается через Интернет, загружается с серверов Поставщика или из других источников. Перед использованием Программного обеспечения необходимо провести установку. Установка Программного обеспечения должна происходить на настроенном компьютере, конфигурация которого соответствует минимальным требованиям, изложенным в комплекте Документации. Способ установки описан в Документации. Компьютер, на который устанавливается Программное обеспечение, не должен содержать программное или аппаратное обеспечение, которое может негативно повлиять на его работу.

4. Лицензия. Получив настоящий документ, тем самым Вы соглашаетесь с пунктами Соглашения и оплачиваете, при необходимости, Лицензионный сбор, описанный в статье 16, при предоставлении Поставщиком неисключительного и не подлежащего передаче права на установку Программного обеспечения на жесткий диск компьютера или на аналогичный носитель постоянного хранения данных, на установку и хранение Программного обеспечения в памяти компьютера и на исполнение, хранение и отображение данных Программного обеспечения на компьютерах, число которых не превышает число, указанное Пользователем в заказе и оплаченное в соответствующем объеме Лицензионного сбора («Лицензия»). Под одним пользователем подразумевается: (1) установка Программного обеспечения на один компьютер, (2) в случае распределенной лицензии с привязкой к количеству почтовых ящиков, означает одного пользователя компьютера, получающего электронную почту посредством Пользовательского почтового агента. Если Пользовательский почтовый агент принимает электронную почту и распределяет ее автоматически среди нескольких пользователей, количество пользователей должно быть определено из расчета количества реальных пользователей, получающих электронную почту. Если почтовый сервер функционирует в режиме почтового шлюза, количество пользователей приравнивается количеству почтовых серверов, к которым предоставляется доступ через этот шлюз. Если какое-либо количество электронных адресов (например, вследствие использования псевдонимов) принадлежит одному пользователю и один пользователь принимает почту по ним, а почта не распределяется автоматически на стороне клиента по другим пользователям, Лицензия необходима только для одного компьютера.

5. Использование прав Пользователя. Как Пользователь Вы можете использовать Программное обеспечение только для защиты своих действий и компьютеров, на которые получена и оплачена соответствующая Лицензия.

6. Ограничения прав Пользователя. Не разрешается копировать, распространять, разделять на части или создавать дочерние версии Программного обеспечения за исключением следующих оговоренных случаев:

(а) Вы можете создавать одну резервную копию Программного обеспечения на носителе данных, не используя эту архивную резервную копию для установки и использования Программного обеспечения на других компьютерах. Создание копий Программного обеспечения в других целях является нарушением этого Соглашения.

(б) Вы не должны использовать, изменять, толковать, воспроизводить или передавать права на использование Программного обеспечения или копий Программного обеспечения иным образом, отличным от описанного в настоящем Соглашении.

(в) Вы не должны продавать, сдавать в аренду или передавать во временное пользование другим лицам Программное обеспечение или права на его использование.

(г) Запрещается анализировать, декомпилировать или разбирать код приложения, а также искать пути получения исходного кода Программного обеспечения способами, противоречащими действующему законодательству.

(е) Вы соглашаетесь использовать Программное обеспечение только способом, соответствующим всем существующим законодательным нормам и правилам, которые применимы к случаям использования этого Программного обеспечения, в том числе нормам, установленным международным законом об авторском праве, внутренними нормативными актами Российской Федерации об авторском праве и смежных правах, а также другими законами по защите интеллектуальной собственности.

(ж) Запрещается использование Программного обеспечения, полученного в виде пробной версии или версии категории «Не для продажи» в целях избежания уплаты Лицензионного сбора (статья 16).

7. Авторское право. Программное обеспечение и все права, включая (без ограничений) право собственности и право интеллектуальной собственности принадлежат компании ESET. Права компании ESET защищены международными соглашениями и прочими соответствующими законодательными нормами стран, в которых используется Программное обеспечение. Внутренняя структура, устройство и код Программного обеспечения являются коммерческой тайной и конфиденциальной информацией, принадлежащей компании ESET. Запрещается копирование Программного обеспечения, кроме случаев, описанных в статье 6 (а). Любые копии, создаваемые в соответствии с Соглашением, должны содержать оригинальные отметки о защите авторских прав и наименование оригинального Программного обеспечения. Если Вы анализируете, декомпилируете или разбираете код Программного обеспечения или ищете пути получения исходного кода способами, нарушающими положения этого Соглашения, любая информация, полученная таким образом, автоматически и безоговорочно должна быть передана Поставщику, так как принадлежит Поставщику изначально.

8. Сохранение прав. Все права на Программное обеспечение закреплены за Поставщиком, кроме тех прав, которые в явной форме передаются Вам, как Пользователю, этим Соглашением.

9. Несколько языковых версий, версии для разных операционных систем, несколько копий. Если Программное обеспечение поддерживает несколько платформ или языков или если Вы получили несколько копий программного обеспечения, запрещается установка большего количества копий или версий Программного обеспечения, чем было указано в заказе и чем было оплачено соответствующими Лицензионными сборами в соответствии со статьей 16 настоящего Соглашения. Запрещается продавать, сдавать в аренду или напрокат, выдавать сублицензии, передавать во временное или постоянное пользование другим лицам любые версии или копии Программного обеспечения, даже если оно не используется вами.

10. Момент вступления в силу и продолжительность действия Соглашения. Настоящее Соглашение вступает в законную силу и действует с момента установки Программного обеспечения, принятия условия настоящего Соглашения и подтверждения Поставщиком правильности ключа. Завершить действие Соглашения можно, необратимо удалив, разрушив или вернув за свой счет Программное обеспечение, все резервные копии (если таковые делались) и все дополнительные материалы, которые были получены от Поставщика или от одного из его коммерческих партнеров. Ваши права как Пользователя автоматически и немедленно аннулируются, без предупреждений со стороны Поставщика, если любое из положений настоящего Соглашения будет нарушено Вами. В этом случае Вы обязаны без промедления удалить, разрушить или вернуть за свой счет Программное обеспечение, все резервные копии (если таковые делались) и все дополнительные материалы, которые были получены от компании ESET или от одного из ее коммерческих партнеров.
Настоящее Соглашение заключается на срок один или два года (или иной согласованный срок), как указано в вашем заказе на Программное обеспечение в качестве периода использования, и его действие может быть продлено на период продолжительностью один или два года (или иной согласованный срок) в случае оплаты вами соответствующих Лицензионных сборов, как описано в статье 16 настоящего Соглашения.
Независимо от способа окончания действия текущего Соглашения, положения статей 7, 8, 11, 13 и 19 остаются действительными без ограничения по времени

11. ПРЕДОСТАВЛЕНИЕ ГАРАНТИИ. ВЫСТУПАЯ В КАЧЕСТВЕ ПОЛЬЗОВАТЕЛЯ, ВЫ ПОДТВЕРЖДАЕТЕ СВОЮ ОСВЕДОМЛЕННОСТЬ В ТОМ, ЧТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПОСТАВЛЯЕТСЯ НА УСЛОВИЯХ «КАК ЕСТЬ», БЕЗ ПРЯМОЙ ИЛИ ВМЕНЕННОЙ ГАРАНТИИ ЛЮБОГО ТИПА, И, НАСКОЛЬКО ЭТО ПОЗВОЛЯЮТ СООТВЕТСТВУЮЩИЕ ЗАКОНОДАТЕЛЬНЫЕ НОРМЫ, НИ ПОСТАВЩИК, НИ ЕГО ПАРТНЕРЫ, ВЫСТУПАЮЩИЕ В КАЧЕСТВЕ ПОСТАВЩИКОВ ЛИЦЕНЗИЙ, НИ ПРАВООБЛАДАТЕЛИ НЕ ПРЕДОСТАВЛЯЮТ НИКАКИХ ПРЯМЫХ ИЛИ ВМЕНЕННЫХ ОБЯЗАТЕЛЬСТВ ИЛИ ГАРАНТИЙ, В ЧАСТНОСТИ ГАРАНТИЙ ПРОДАЖ ИЛИ ГАРАНТИЙ СООТВЕТСТВИЯ КАКОМУ-ЛИБО НАЗНАЧЕНИЮ, ИЛИ ГАРАНТИЙ ТОГО, ЧТО ЭТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НЕ НАРУШАЕТ НИКАКИХ ПАТЕНТОВ, АВТОРСКИХ ПРАВ, ПРАВ НА ТОВАРНЫЕ МАРКИ ИЛИ ДРУГИХ ПРАВ ТРЕТЬИХ СТОРОН. ПОСТАВЩИК И ЕГО ПАРТНЕРЫ НЕ ГАРАНТИРУЮТ, ЧТО ФУНКЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ БУДУТ ПОЛНОСТЬЮ СООТВЕТСТВОВАТЬ ВАШИМ ТРЕБОВАНИЯМ, ИЛИ ЧТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ БУДЕТ РАБОТАТЬ БЕЗ СБОЕВ И ОШИБОК. ВСЯ ОТВЕТСТВЕННОСТЬ И РИСК ПРИ ВЫБОРЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ДОСТИЖЕНИЯ ОПРЕДЕЛЕННЫХ РЕЗУЛЬТАТОВ, КОТОРЫЕ НЕОБХОДИМЫ ВАМ, А ТАКЖЕ ПРИ УСТАНОВКЕ, ИСПОЛЬЗОВАНИИ И ПОЛУЧЕНИИ РЕЗУЛЬТАТОВ, КОТОРЫЕ ВЫ БУДЕТЕ ДОСТИГАТЬ С ПОМОЩЬЮ ЭТОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ЛЕЖИТ НА ВАС. ВЫ ДОЛЖНЫ БЫТЬ ОСВЕДОМЛЕНЫ О МИНИМАЛЬНЫХ СИСТЕМНЫХ ТРЕБОВАНИЯХ ВАШЕГО КОМПЬЮТЕРА, КОТОРЫЕ ПОЗВОЛЯТ ФУКЦИОНИРОВАТЬ ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ.

12. Отказ от дальнейших обязательств. Настоящее Соглашение не накладывает никаких обязательств на Поставщика, за исключением тех, что изложены в настоящем Соглашении.

13. ОГРАНИЧЕННАЯ ГАРАНТИЯ. В ТОЙ СТЕПЕНИ, НАСКОЛЬКО ЭТО ДОПУСКАЕТСЯ ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, ПОСТАВЩИК, ЕГО СОТРУДНИКИ И ПАРТНЕРЫ, ВЫСТУПАЮЩИЕ В КАЧЕСТВЕ ПОСТАВЩИКОВ ЛИЦЕНЗИЙ, НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА ЛЮБЫЕ ПОТЕРИ ПРИБЫЛИ, ДОХОДОВ ИЛИ ОБОРОТА С ПРОДАЖ, ИЛИ ЗА УТРАТУ ДАННЫХ, ИЛИ ПО ЗАТРАТАМ НА ДОПОЛНИТЕЛЬНЫЕ ЗАПАСНЫЕ ЧАСТИ И ОБСЛУЖИВАНИЕ, ЗА ПОРЧУ ИМУЩЕСТВА, ВРЕД ЗДОРОВЬЮ, ПЕРЕРЫВЫ В КОММЕРЧЕСКОЙ ДЕЯТЕЛЬНОСТИ, ПОТЕРЮ КОММЕРЧЕСКОЙ ИНФОРМАЦИИ ИЛИ ДРУГИЕ СЛУЧАИ УЩЕРБА, В ТОМ ЧИСЛЕ СПЕЦИАЛЬНОГО, НАМЕРЕННОГО, НЕНАМЕРЕННОГО, СЛУЧАЙНОГО, ЭКОНОМИЧЕСКОГО, ПОКРЫВАЕМОГО, ПРЕСТУПНОГО, ПРЯМОГО ИЛИ ОПОСРЕДОВАННОГО, ПРОИЗОШЕДШЕГО КАКИМ-ЛИБО ЕЩЕ СПОСОБОМ, НЕЗАВИСИМО ОТ ДЕЙСТВИЯ ДОПОЛНИТЕЛЬНЫХ КОНТРАКТОВ, УМЫШЛЕННЫХ ДЕЙСТВИЙ, НЕБРЕЖНОСТИ ИЛИ ДРУГИХ ФАКТОРОВ, КОТОРЫЕ МОГУТ ВЫЗВАТЬ ОТВЕТСТВЕННОСТЬ, ВКЛЮЧАЯ ПОВРЕЖДЕНИЯ ВСЛЕДСТВИЕ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИЛИ НЕВОЗМОЖНОСТИ ЕГО ИСПОЛЬЗОВАНИЯ, ДАЖЕ ЕСЛИ ПОСТАВЩИК ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИЛИ ЕГО ПАРТНЕР, ПОСТАВЛЯЮЩИЙ ЛИЦЕНЗИЮ, БЫЛ ПРЕДУПРЕЖДЕН О ВОЗМОЖНОСТИ ТАКОГО УЩЕРБА. ТАК КАК ЗАКОНОДАТЕЛЬСТВО НЕКОТОРЫХ СТРАН И ОТДЕЛЬНЫЕ ЗАКОНЫ НЕ ПОЗВОЛЯЮТ ИСКЛЮЧАТЬ ТАКУЮ ОТВЕТСТВЕННОСТЬ, НО РАЗРЕШАЮТ ОГРАНИЧИВАТЬ ЕЕ, ОТВЕТСТВЕННОСТЬ ПОСТАВЩИКА, ЕГО СОТРУДНИКОВ ИЛИ ЕГО ПАРТНЕРОВ, ПОСТАВЛЯЮЩИХ ЛИЦЕНЗИИ, ОГРАНИЧИВАЕТСЯ РАЗМЕРОМ СУММЫ, ВЫПЛАЧЕННОЙ ВАМИ ПРИ ПРИОБРЕТЕНИИ ЛИЦЕНЗИИ.
ВАЖНОЕ ЗАМЕЧАНИЕ ДЛЯ ПОЛЬЗОВАТЕЛЯ. ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НЕ ОТКАЗОУСТОЙЧИВО И НЕ ПРЕДНАЗНАЧЕНО ДЛЯ РАБОТЫ В ОПАСНЫХ УСЛОВИЯХ, ТРЕБУЮЩИХ БЕСПЕРЕБОЙНОЙ РАБОТЫ. ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НЕ ПРЕДНАЗНАЧЕНО ДЛЯ ИСПОЛЬЗОВАНИЯ В СИСТЕМАХ НАВИГАЦИИ САМОЛЕТОВ, В ЯДЕРНЫХ ЦЕНТРАХ ИЛИ СИСТЕМАХ СВЯЗИ, В СИСТЕМАХ ВООРУЖЕНИЙ, В СИСТЕМАХ ПРЯМОГО ИЛИ НЕПРЯМОГО ЖИЗНЕОБЕСПЕЧЕНИЯ, В УПРАВЛЕНИИ ПОЛЕТАМИ ИЛИ В ЛЮБЫХ ДРУГИХ ВИДАХ ДЕЯТЕЛЬНОСТИ, ГДЕ ОШИБКА МОЖЕТ ПОВЛЕЧЬ ЗА СОБОЙ СМЕРТЬ, СЕРЬЕЗНЫЕ ПОВРЕЖДЕНИЯ ИЛИ БОЛЬШОЙ УЩЕРБ.

14. Ни одно из положений настоящего Соглашения не затрагивает права той стороны, для которой закон обозначает права и положение в качестве потребителя. Поставщик со своей стороны, стороны своих сотрудников и со стороны поставщиков лицензий, выступает с позиции отказа, исключения или ограничения любых обязательств, ответственности и гарантий, как указано в статье 13, что исключает любую другую позицию и не преследует иных причин.

15. Поддержка. Поставщик обязан оказывать техническую поддержку для наиболее свежих версий Программного обеспечения. В соответствии с положениями Лицензии, Пользователь имеет право использовать следующие службы:

(а) **Помощь по техническим вопросам.** Поставщик обязан обеспечивать помощь и поддержку во время поиска неисправностей и отладке в случае использования наиболее свежих версий Программного обеспечения в заранее объявленное рабочее время. Любые запросы помощи и поддержки, полученные в нерабочее время, рассматриваются как полученные в начале следующего рабочего дня. Запросы помощи и поддержки могут быть доставлены Поставщику посредством телефонной связи, факса или электронной почты с использованием отдельных телефонных линий или адресов электронной почты, указанных в Документации или на веб-сайтах Поставщика. Запросы помощи и поддержки должны быть достаточно осмысленными и обязаны содержать достаточно данных для воспроизведения возникшей проблемы. При необходимости Пользователь обязан предоставить необходимую помощь в решении описываемой проблемы.

(б) **Обновление.** Обновления включают в себя все новые версии или изменения Программного обеспечения или отдельных его частей, о выпуске которых объявлено на сайтах Поставщика или сайтах его коммерческих партнеров. Поставщик обязуется предоставить Пользователю доступ к Обновлению в защищенной области своего веб-сайта посредством сети Интернет. Доступ к обновлениям предоставляется при указании имени пользователя и пароля («Идентификация»). Данные Идентификации Пользователя содержат случайную комбинацию алфавитно-цифровых символов и автоматически генерируются системой Поставщика. Данные Идентификации должны быть предоставлены Пользователю в форме электронного письма, или вложены в торговую упаковку Лицензированного продукта или доставлены любым другим подходящим способом. Пользователь обязан принять меры для сохранности данных Идентификации и защитить их от повреждения, потери или неверного использования. Вы признаете, что Программное обеспечение и связанные с ним серийный номер, регистрационный ключ и код активации являются производственной тайной и важной конфиденциальной информацией компании ESET («Конфиденциальная информация»). Вы соглашаетесь не предоставлять третьим лицам и не раскрывать перед ними эту конфиденциальную информацию, за исключением (если Вы представляете Компанию) собственных работников и независимых консультантов, давших стандартные для отрасли подписки о неразглашении. При обнаружении первого случая неверного использования данных Идентификации Пользователя Поставщик имеет право отменить действие данных Идентификации и предоставить новые данные Идентификации для пользователя («Замена идентификации»). Пользователь обязан предоставить Поставщику все данные, необходимые для расследования случаев неверного использования данных Идентификации, в том числе записи действий компьютерных систем, записи доступа к файлам и другие необходимые данные. В случаях, когда обнаружено неверное использование данных Замены идентификации, поставщик по своему усмотрению и в результате своего решения может предоставить новую Замену идентификации для Пользователя, или прекратить действие Лицензии немедленно без какой-либо компенсации Пользователю. Право Поставщика компенсировать ущерб не противоречит немедленной отмене действия Лицензии. Пользователь обязуется получать обновления только с веб-сайтов Поставщика или его официальных партнеров («Авторизованные источники»). Пользователь согласен устанавливать каждую новую версию или изменение Лицензированного продукта сразу же после получения или не позже, чем указано Поставщиком в Программном обеспечении, Документации к нему или на веб-сайтах Поставщика или его коммерческих партнеров. Поставщик не может нести ответственность за ущерб, произошедший вследствие нарушения Пользователем последовательности получения новых версий Программного обеспечения и/или установки обновлений из Авторизованных источников.

(в) **Отказ в поддержке.** Поставщик не обязан обеспечивать поддержку в следующих случаях:

I. ошибка произошла вследствие постороннего вмешательства в структуру Программного обеспечения, его исходный код или при использовании неверных параметров или установок Программного обеспечения;

II. ошибка произошла по вине обслуживающего персонала Пользователя, или при использовании Программного обеспечения в условиях, не соответствующих описанным в Документации;

III. ошибка устраняется путем установки Обновления, которое Пользователь не может установить;

IV. Лицензионный сбор не оплачен Пользователем, как того требует статья 16 настоящего Соглашения;

V. другие случаи, описанные в настоящем Соглашении.

(г) **Обучение.** Настоящее Соглашение не влечет за собой обязательств по предоставлению услуг обучения или практики по эксплуатации и установке Программного обеспечения.

16. Лицензионный сбор и порядок оплаты. Размер Лицензионного сбора за полноценную версию Программного обеспечения определяется на основе текущего прейскуранта Поставщика в соответствии с количеством компьютеров, для которых предназначено Программное обеспечение («Лицензионный сбор»). Перед оплатой Лицензионного сбора Вы можете ознакомиться с положениями и условиями Соглашения и сроком, на который передается право на использование этого Программного обеспечения. Если на счете или другом документе, предоставленном Поставщиком или его коммерческим партнером, не указано иной даты погашения, Лицензионный сбор уплачивается в момент доставки Программного обеспечения. Вы обязаны оплатить все налоги и иные пошлины, начисленных в отношении оплаты Лицензионного сбора вследствие действия текущего законодательства, исключая налоги на доход Поставщика. Если Вы не оплачиваете Лицензионный сбор до указанной даты, Ваша Лицензия на использование Программного обеспечения отменяется, и Вы обязаны компенсировать все операционные расходы, включая расходы на юридические услуги и судебные пошлины. Под обязательство оплаты Лицензионного сбора не попадают случаи использования Программного обеспечения, поставленного под категорией «Не для продажи» и пробных версий. Факт оплаты Лицензионного сбора является подтверждением Пользователем принятия данного лицензионного соглашения.

17. Пробные версии и версии не для продажи. Вы можете использовать Программное обеспечение, поставляемое не для продажи или поставляемое в качестве пробных версий, которые предназначены для проверки и тестирования функций Программного обеспечения. Кроме того, Вы можете использовать Программное обеспечение категории «Не для продажи» в демонстрационных целях.

18. Данные пользователя и защита прав. Вы, как Пользователь, разрешаете Поставщику передавать, обрабатывать и сохранять данные, позволяющие Поставщику устанавливать Вашу личность. Вы согласны с тем, что поставщик может своими средствами проверить правильность использования Программного обеспечения в соответствии с настоящим Соглашением. Вы согласны, что посредством обмена данными между Программным обеспечением и компьютерами Поставщика или его коммерческих партнеров будут передаваться данные, которые удостоверяют право на использование Программного обеспечения и обеспечивают защиту прав Поставщика.

19. Экспортная и реэкспортная проверка. Программное обеспечение, Документация или ее часть, включая информацию о Программном обеспечении и его частях, являются объектом, попадающим под действие надзорных правил по импорту и экспорту в соответствии с действующим законодательством. Вы согласны строго следовать всем действующим нормам и правилам по экспорту и импорту и подтверждаете, что Вы ответственны за получение лицензий на экспорт, реэкспорт, перевозку и импорт Программного обеспечения.

20. Примечания. Все замечания, возвращаемое Программное обеспечение и Документация должны быть доставлены по адресу: ESET, spol. s r. o., Svoradova 1, 811 03 Bratislava, Slovak Republic.

21. Регулирующее законодательство. Пользователь и Поставщик согласны, что решение конфликтов производится в соответствии с государственным законодательством Российской Федерации, а Конвенция ООН о контрактах по международной торговле товарами (United Nations Convention on Contracts for the International Sale of Goods) неприменима. Вы явным образом соглашаетесь с тем, что эксклюзивная юрисдикция по решению любых споров и вопросов с Поставщиком или относительно способа использования Программного обеспечения принадлежит окружному суду в Братиславе (District Court Bratislava I., Slovakia), и Вы выражаете персональное согласие в настоящем и будущем и явным образом подчиняетесь юридическим процедурам этого суда (District Court Bratislava I., Slovakia) в связи с любым спором или конфликтом такого рода.

22. Общие положения. Если любое положение настоящего Соглашения оказывается недействительным или невыполнимым, это не отражается на действительности остальных положений Соглашения. Они остаются в силе в соответствии с условиями и сроками, изложенными в этом документе. Любые поправки к этому документу могут иметь место только в письменной форме и должны быть подписаны действующим на основе закона компетентным и уполномоченным представителем Поставщика.

Настоящее Соглашение между Вами и Поставщиком является единым и неделимым Соглашением, применимым к Программному обеспечению, и полностью отменяющим любые предыдущие изложения фактов, результаты переговоров, обязательства, отчеты или объявления относительно Программного обеспечения.

1. ESET NOD32 Smart Security

Программный пакет ESET NOD32 Smart Security — это новый подход, к обеспечению безопасности путем глубокой интеграции всех компонентов решения. ESET NOD32 Smart Security использует быстродействие антивируса ESET NOD32 на основе технологии сканирующего модуля ThreatSense®, в совокупности с уникальными модулями персонального файервола и антиспама. Интеллектуальная система постоянно готова противостоять атакам и вредоносным программам, подвергающим опасности компьютеры пользователей.

ESET NOD32 Smart Security – не просто собранные в один пакет разнообразные продукты, что характерно для предложений других поставщиков. Это результат продолжительной работы, направленной на достижение максимального уровня интеграции средств защиты при минимальном использовании системных ресурсов. Передовые технологии, основанные на искусственном интеллекте, обеспечивают проактивную защиту от вирусов, шпионских и троянских программ, червей, рекламного ПО, руткитов, а также от сетевых атак. При этом не происходит снижение производительности системы или нарушения работы компьютера.

1.1 Новые возможности

В результате длительной работы наших экспертов разработана совершенно новая архитектура программы ESET NOD32 Smart Security, которая гарантирует максимальный уровень обнаружения угроз при минимальных требованиях к системе. Комплексное программное решение по безопасности включает модули с несколькими расширенными опциями. В приведенном ниже списке представлен краткий обзор этих модулей.

■ Защита от вирусов и шпионских программ

Этот модуль построен на основе ядра сканирования ThreatSense®, впервые использованного в системе NOD 32. Ядро ThreatSense® оптимизировано и улучшено благодаря новой архитектуре ESET NOD32 Smart Security.

Характеристика	Описание
Улучшенная очистка	Теперь «интеллектуальная» антивирусная система способнаочищать файлы и удалять большинство из обнаруженных вирусов, проникших в систему, без вмешательства пользователя.
Режим фонового сканирования	Запуск фонового сканирования компьютера без снижения производительности системы.
Файлы обновления меньшего объема	Благодаря процессам оптимизации уменьшен размер файлов обновления по сравнению с версией 2.7. Кроме того, была улучшена защита файлов обновления от повреждений.
Защита популярных почтовых клиентов	Возможность сканирования входящей почты не только в MS Outlook, но и в Outlook Express и Windows Mail.
Дополнительные улучшения	– Прямой доступ к файловым системам в целях обеспечения быстродействия и высокой производительности. – Запрет доступа к зараженным файлам – Оптимизация для центра безопасности Windows, включая Vista.

■ Персональный файервол

Персональным файерволом отслеживается весь трафик между защищаемым компьютером и другими машинами в сети, а также интернет.

Персональный файервол ESET имеет расширенные функции, описанные ниже

Характеристика	Описание
Сканирование сетевых соединений на уровне канала	Сканирование сетевых соединений на уровне канала данных позволяет персональному файерволу ESET противодействовать многочисленным атакам, которые при других условиях нельзя обнаружить.
Поддержка IPv6	Персональный файервол ESET отображает адреса IPv6 и позволяет создавать для них правила.
Мониторинг выполняемых файлов	Отслеживание изменений в исполняемых файлах для борьбы с заражением. Имеется возможность разрешить изменения в файлах для выбранных приложений.
Сканирование файлов, интегрированное с HTTP и POP3	Сканирование файлов, интегрированное в протоколы приложений HTTP и POP3. Пользователи защищены как при просмотре ресурсов в интернете, так и при загрузке электронной почты.
Система обнаружения вторжений	Возможность распознавать характер сетевой связи и различные типы сетевых атак и автоматически запрещать такие связи.
Поддержка интерактивного и автоматического режимов, режима на основе политик	Пользователи могут выбрать автоматический режим работы файервола или самостоятельного задавать правила в интерактивном режиме. Режим на основе политик позволяет пользователю или сетевому администратору установить и применить для файервола настраиваемую конфигурацию политик.
Замена интегрированному брандмауэру Windows	Заменяет интегрированный брандмауэр Windows, а также взаимодействует с центром безопасности Windows, поэтому пользователь всегда осведомлен о своем статусе безопасности. Установка ESET NOD32 Smart Security отключает стандартный брандмауэр Windows.

■ Защита от спама

Система защиты от спама автоматически отфильтровывает нежелательные сообщения электронной почты, повышая таким образом безопасность и удобство работы с электронными средствами связи.

Характеристика	Описание
Рейтинг входящей почты	Входящие сообщения получают рейтинг от 0 (сообщение не является спамом) до 100 (спам) и переносятся в папку для спама (Junk Mail) или в специальную папку, созданную пользователем. Имеется возможность одновременного сканирования входящих писем.
Поддержка многочисленных методик сканирования	Анализ Бейеса Сканирование на основе правил Проверка по глобальной базе данных отпечатков
Полная интеграция с почтовыми клиентами	Компонент защиты от спама доступен для пользователей Microsoft Outlook, Outlook Express и Windows Mail.
Возможность отбора спама вручную	Имеется опция отбора спама вручную (можно пометить письмо как спам или снять эту пометку, а также выбрать доверенных отправителей или заблокировать отправителей вне белого списка

1.2 Системные требования

Для бесперебойной работы ESET NOD32 Smart Security система должна удовлетворять следующим программным и аппаратным требованиям.

■ ESET NOD32 Smart Security:

Windows 2000, XP	400 МГц 32-разрядный / 64-разрядный (x86 / x64) процессор 128 МБ оперативной памяти 35 МБ свободного пространства Super VGA (800 x 600)
Windows Vista	1 ГГц 32-разрядный / 64-разрядный (x86 / x64) процессор 512 МБ оперативной памяти 35 МБ свободного пространства Super VGA (800 x 600)

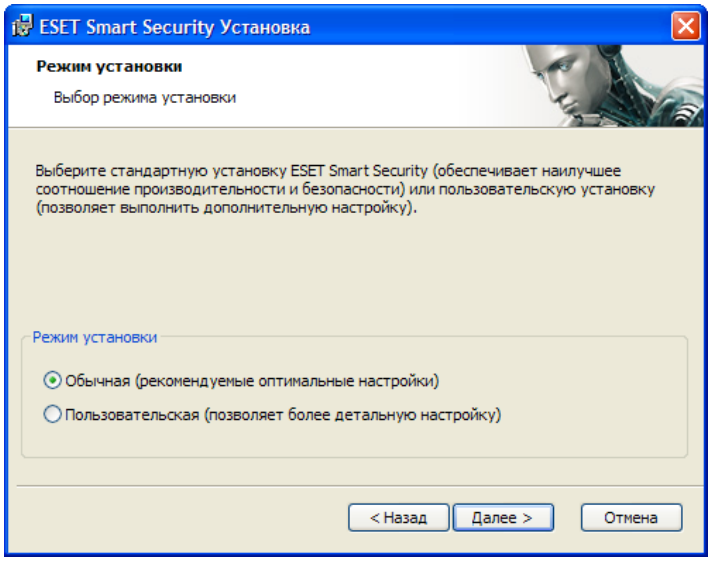
■ ESET NOD32 Smart Security, версия для корпоративных клиентов

Windows 2000, XP	400 МГц 32-разрядный / 64-разрядный (x86 / x64) процессор 128 МБ оперативной памяти 35 МБ свободного пространства Super VGA (800x600)
Windows Vista	1 ГГц 32-разрядный / 64-разрядный (x86 / x64) процессор 512 МБ оперативной памяти 35 МБ свободного пространства Super VGA (800 x 600)

2. Установка

После приобретения лицензии программа для установки ESET NOD32 Smart Security может быть загружена с сайта компании ESET. Программа находится в пакетах ess_nt**_***.msi (для ESET NOD32 Smart Security) или essbe_nt**_***.msi (для ESET NOD32 Smart Security Business Edition (версия для корпоративных клиентов). Запустите программу установки и задайте основные настройки, следуя указаниям мастера установки. Доступны два типа установки, различающиеся уровнем детализации настройки:

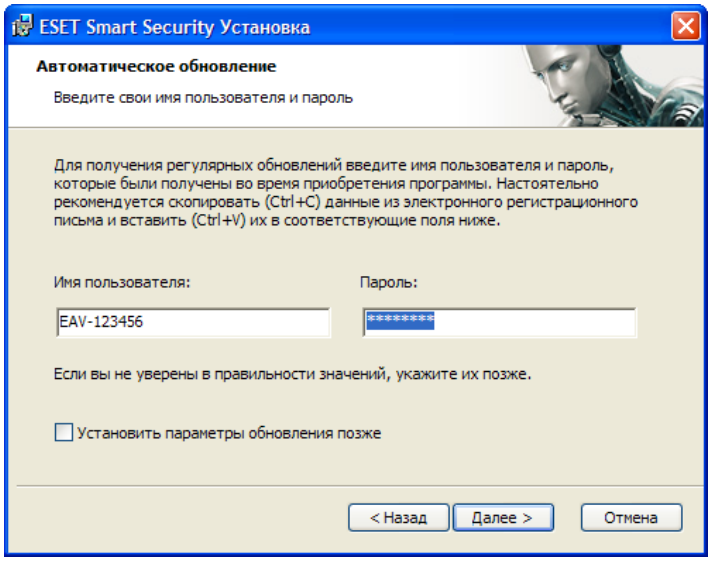
- обычная установка
- выборочная установка



2.1 Обычная установка

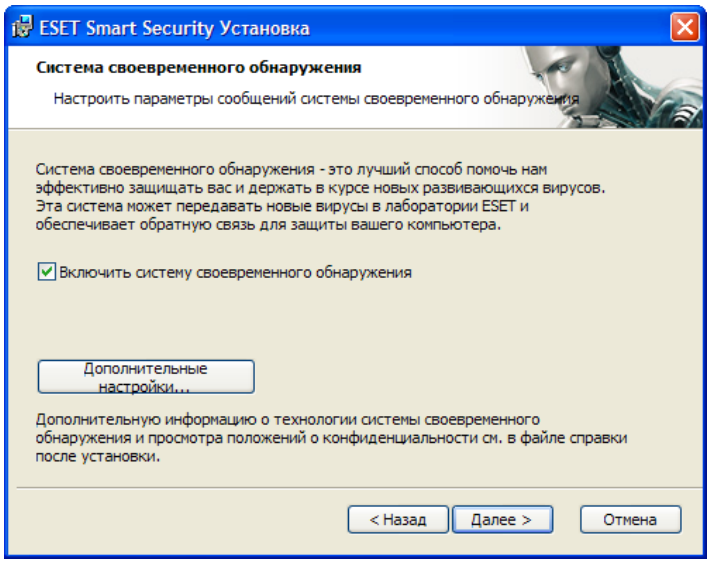
Обычная установка рекомендована для пользователей, желающих установить ESET NOD32 Smart Security с настройками по умолчанию. Этот вариант обеспечивают максимальный уровень защиты и удобства.

Первый (очень важный) шаг потребует ввода имени пользователя и пароля для автоматического обновления программы. Это играет важную роль в обеспечении поддержки уровня безопасности для системы.



Введите ваше **Имя пользователя** (User name) и **Пароль** (Password), то есть данные аутентификации, которые Вы получили при покупке или регистрации продукта, в соответствующие поля. Если вы еще не получили имя пользователя и пароль, выберите пункт **Выполнить настройку параметров обновления позже** (Set update parameters later). Данные аутентификации можно ввести в любое время непосредственно из программы.

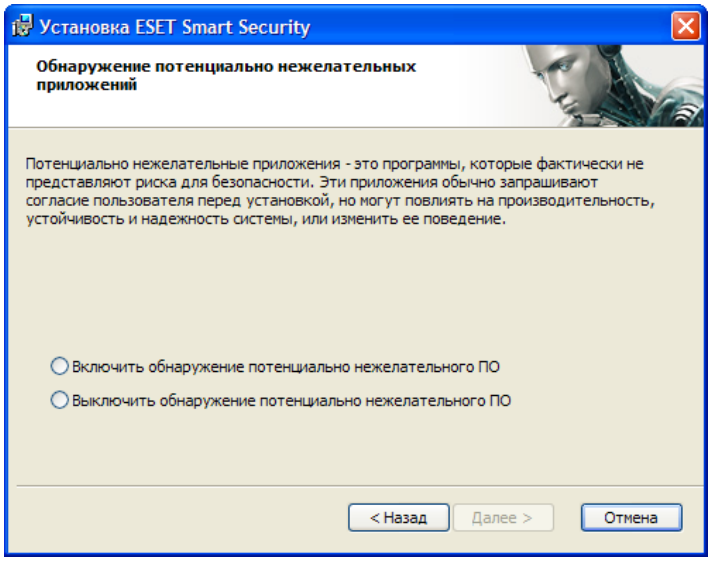
Следующий шаг установки – настройка системы быстрого оповещения ThreatSense.NET. Система раннего оповещения ThreatSense.NET помогает обеспечивать незамедлительное и регулярное оповещение компании ESET о новых угрозах, что дает возможность своевременно защищать пользователей. Система позволяет передавать информацию о новых угрозах в вирусную лабораторию компании ESET, где эти сведения анализируются, обрабатываются и добавляются в базу данных вирусных сигнатур.



По умолчанию флажок **Включить систему быстрого оповещения ThreatSense.NET** (Enable ThreatSense.Net Early Warning System), активизирующий эту возможность, установлен. Нажмите кнопку **Расширенная настройка...** (Advanced setup...) для изменения точных настроек передачи информации о подозрительных файлах.

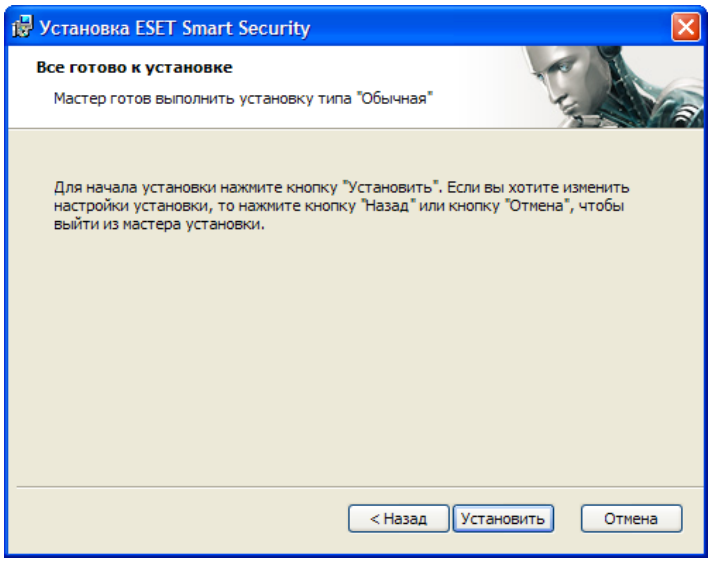
Следующий шаг установки – определение настроек для функции **Обнаружение потенциально нежелательных приложений** (Detection of potentially unwanted applications). Потенциально нежелательные приложения не всегда преднамеренно вредоносны, но могут негативно влиять на поведение системы.

Эти приложения связаны с другими программами, и их бывает сложно обнаружить при установке. Несмотря на то, что обычно при установке эти приложения выводят уведомление на экран, они могут быть установлены и без вашего согласия.



Выберите опцию **Включить обнаружение потенциально нежелательных приложений** (Enable detection of potentially unwanted applications), это поможет программе ESET NOD32 Smart Security выявлять угрозу данного типа (рекомендовано).

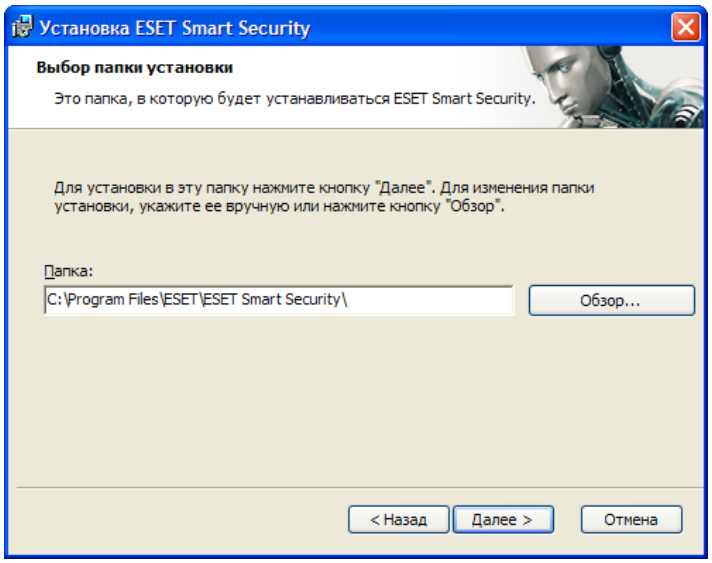
Последний шаг установки в обычном режиме – подтверждение установки нажатием кнопки **Установить** (Install).



2.2 Выборочная установка

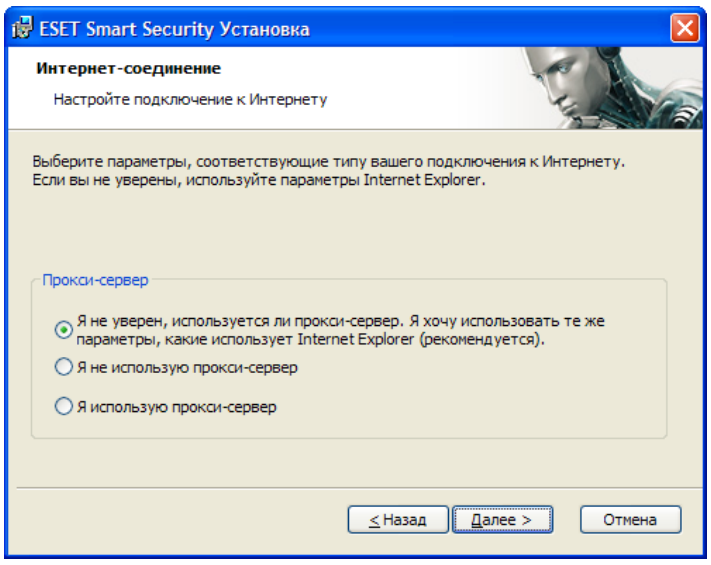
Выборочная установка разработана для пользователей, имеющих опыт в тонкой настройке программ и желающих вносить изменения в расширенные настройки в ходе установки.

Первый шаг – выбор пути для установки. По умолчанию программа устанавливается в каталог C:\Program Files\ESET\ESET NOD32 Smart Security\. Изменить путь (не рекомендуется), можно с помощью кнопки **Обзор...** (Browse...).

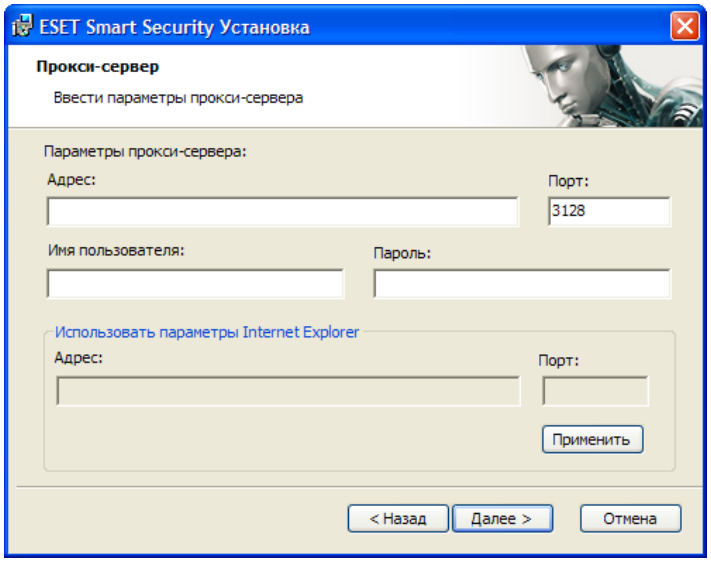


Затем потребуется ввести Имя пользователя и Пароль. Этот шаг аналогичен действиям при обычной установке (см. страницу 5).

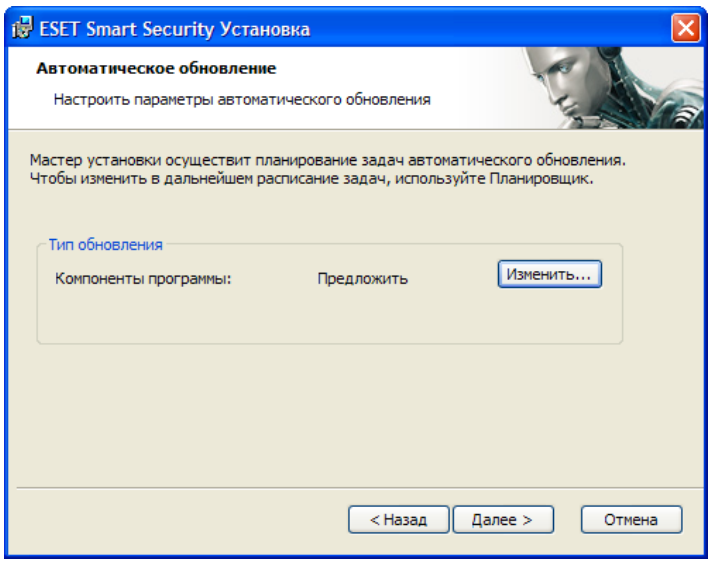
После ввода имени пользователя и пароля нажмите **Далее** (Next) для перехода к окну **Настройка подключения к интернету** (Configure your Internet connection).



Если используется прокси-сервер, его необходимо верно настроить, чтобы обновления вирусных сигнатур проходили без ошибок. Если неизвестно, используется ли прокси-сервер для подключения к интернету, оставьте установку по умолчанию: **Я не уверен, используется ли прокси-сервер. Я хочу использовать те же параметры, какие использует Internet Explorer** (I am unsure if my Internet connection uses a proxy server. Use the same settings as Internet Explorer) и нажмите кнопку **Далее** (Next). Если прокси-сервер не используется, выберите соответствующую опцию.

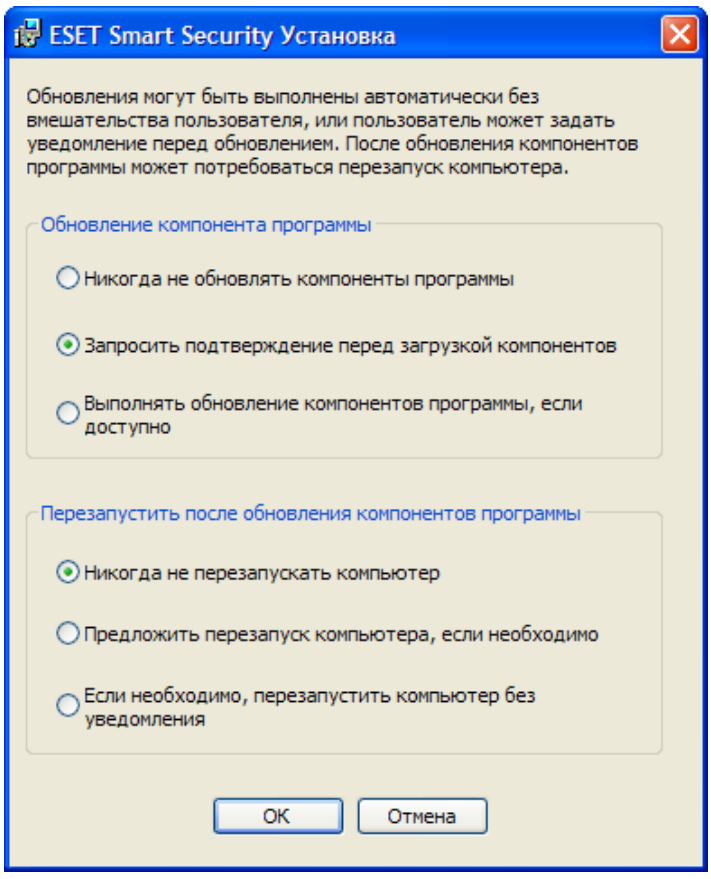


Для настройки установок вашего прокси-сервера выберите Подключение через прокси-сервер (I use a proxy server) и нажмите **Далее** (Next). Введите IP- или URL-адрес вашего прокси-сервера в поле Адрес (Address:). В поле Порт (Port:) укажите порт подключения к прокси-серверу (по умолчанию 3128). Если прокси-сервер требует аутентификацию, для получения доступа необходимо указать действующее имя пользователя и пароль. При необходимости настройки прокси-сервера можно скопировать из Internet Explorer. Для этого нажмите кнопку **Применить** (Apply) и подтвердите выбор.

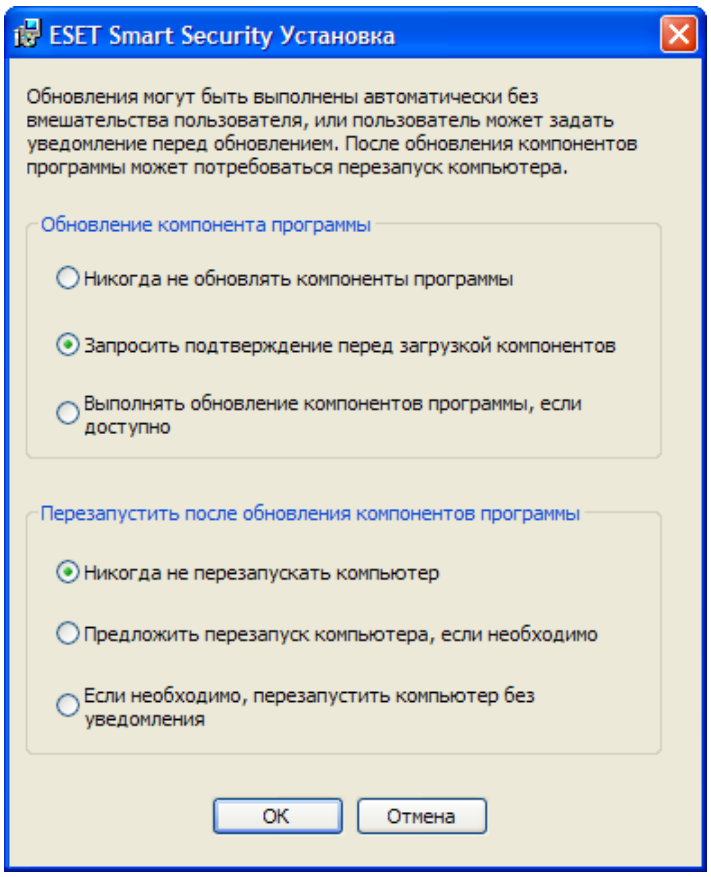


Щелкните **Далее** (Next) чтобы перейти к окну **Настройка автоматического обновления установок** (Configure automatic update settings). На этом шаге можно установить, каким образом в системе будет обрабатываться автоматическое обновление компонентов программы. Нажмите **Изменить...** (Change...) для перехода к расширенным настройкам.

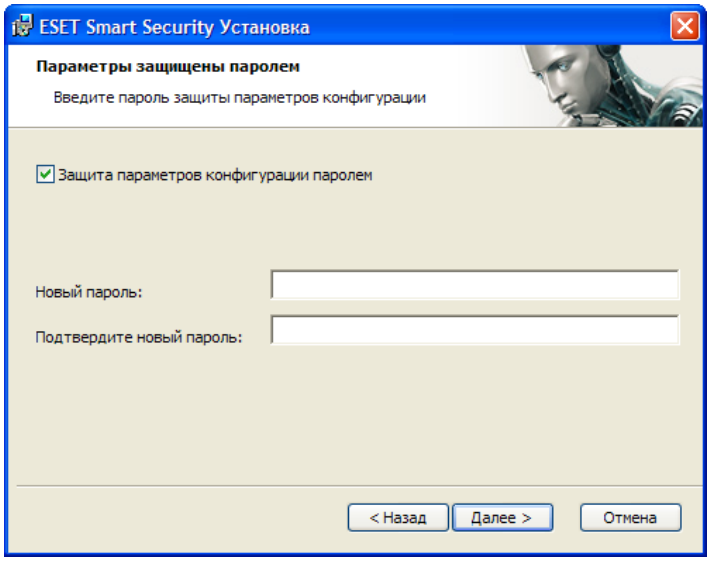
Чтобы отказаться от обновления компонентов программы, выберите **Никогда не обновлять компоненты программы** (Never update program components). Если включена опция **Запросить подтверждение перед загрузкой компонентов** (Ask before downloading program components), перед загрузкой компонентов программы будет выводиться окно подтверждения. Для автоматической загрузки обновления компонентов программы без подтверждения выберите опцию **Выполнять обновление компонентов программы, если доступно** (Perform program component upgrade if available).



Примечание. Обычно после обновления компонентов программы требуется перезагрузка. Рекомендуется выбрать настройку: по умолчанию



Следующий шаг установки – введение пароля для защиты параметров программы. Выберите пароль для защиты программы и введите его повторно для подтверждения.



Шаги **Настройка системы быстрого оповещения ThreatSense.NET** (Configuration of the ThreatSense.Net Early Warning System) и **Обнаружение потенциально нежелательных приложений** (Detection of potentially unwanted applications) выполняются так же, как и при обычной установке (см. страницу 5).

Последний шаг выборочной установки – выбор режима фильтрации для персонального файервола. Имеются три режима:

- **автоматический** (Automatic)
- **интерактивный** (Interactive)
- **на основе политик** (Policy-based)

Автоматический режим рекомендован для большинства пользователей. Все стандартные исходящие подключения разрешены (автоматически анализируются в соответствии с предварительно определенными

установками), а непредусмотренные входящие подключения автоматически блокируются.

Интерактивный режим подходит для опытных пользователей. Подключения обрабатываются по задаваемым пользователем правилам. Если правило для подключения не задано, программа запрашивает у пользователя, разрешить или запретить это подключение.

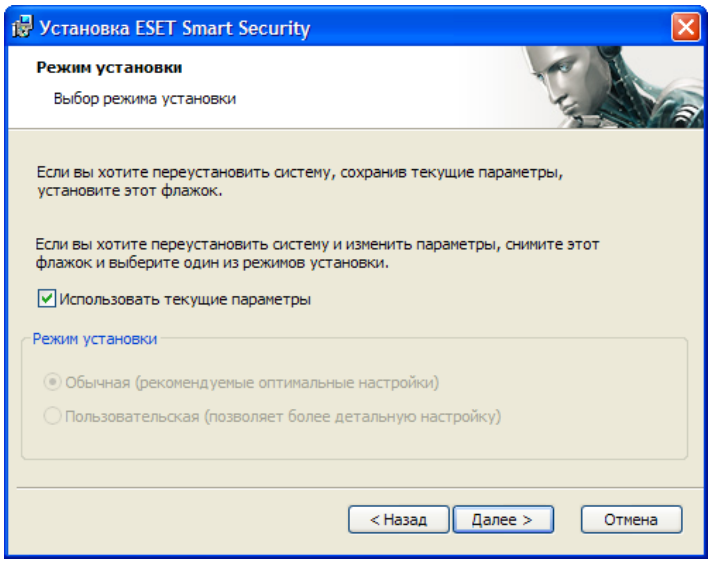
Если задан режим **На основе политик**, подключение оценивается в соответствии с предварительно заданными правилами, созданными администратором. Если доступных правил нет, подключение автоматически блокируется без уведомления пользователя.

Данный режим рекомендуется только для администраторов, устанавливающих настройки сетевых подключений.

На последнем шаге выводится окно с запросом подтверждения установки программы.

2.3 Использование текущих параметров

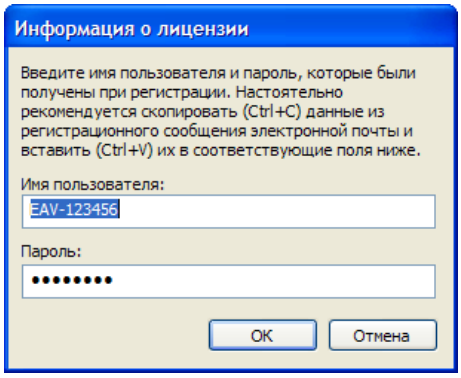
При переустановке ESET NOD32 Smart Security, предлагается выбрать **Использовать текущие параметры** (Use current settings). Выберите эту опцию для переноса параметров настройки из предыдущей установки.



2.4 Ввод имени пользователя и пароля

Для оптимальной работы важно автоматическое обновление программы. Это возможно, только если в настройках обновления указаны действующие имя пользователя и пароль.

Если имя пользователя и пароль не были введены при установке, это можно сделать во время работы. В главном окне программы щелкните **Обновить** (Update), а затем нажмите **Настройка имени пользователя и пароля...** (User name and Password Setup...) Введите данные, полученные вместе с лицензией на использование продукта в окне **Информация о лицензии** (License details).



2.5 Сканирование компьютера по требованию

После установки ESET NOD32 Smart Security необходимо провести сканирование компьютера на наличие вредоносного программного кода. Для быстрого запуска сканирования выберите в основном меню **Сканирование компьютера** (Computer scan), а затем – **Обычное сканирование** (Standard scan). Более подробную информацию о сканировании компьютера см. в главе «Сканирование компьютера».

3. Руководство для начинающих

Эта глава содержит описание ESET NOD32 Smart Security и базовые настройки.

3.1 Описание пользовательского интерфейса – режимы

Главное окно ESET NOD32 Smart Security делится на две большие части. Слева располагается основное меню пользователя. В программном окне справа отображается информация об опции, выбранной из основного меню.

Ниже описаны кнопки основного меню:

Состояние защиты (Protection status) – информация о состоянии защиты ESET NOD32 Smart Security, представленная в удобном для пользователя виде. В расширенном режиме показывается статус всех защитных модулей. Для просмотра текущего состояния модуля щелкните по нему кнопкой мыши.

Сканирование компьютера (Computer scan). Данная опция позволяет настраивать параметры и запускать сканирование компьютера по требованию пользователя.

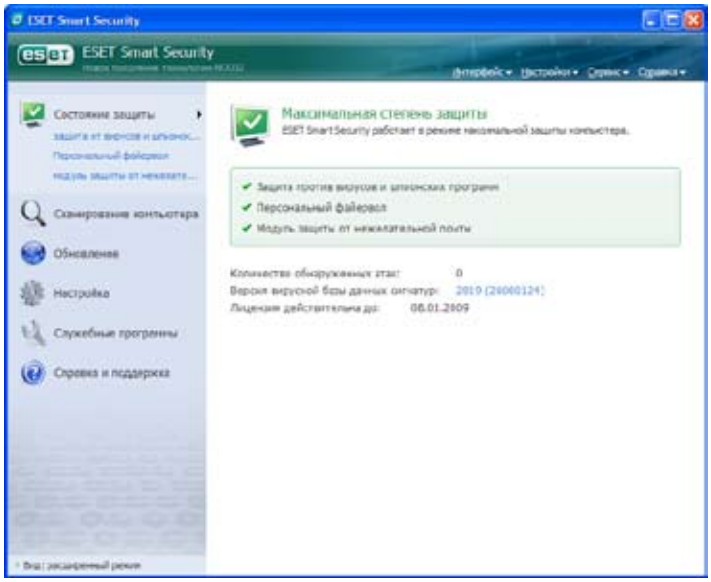
Обновление (Update). Выберите данную опцию для доступа к модулю обновлений базы данных вирусных сигнатур.

Настройка (Setup) позволяет настроить уровень безопасности вашего компьютера. В расширенном режиме появляются подменю антивирусной/антишпионской защиты, персонального файервола и модуля защиты от спама.

Инструменты (Tools). Данная опция доступна только в расширенном режиме. Она позволяет получить доступ к файлам журнала, области карантина и опциям планировщика

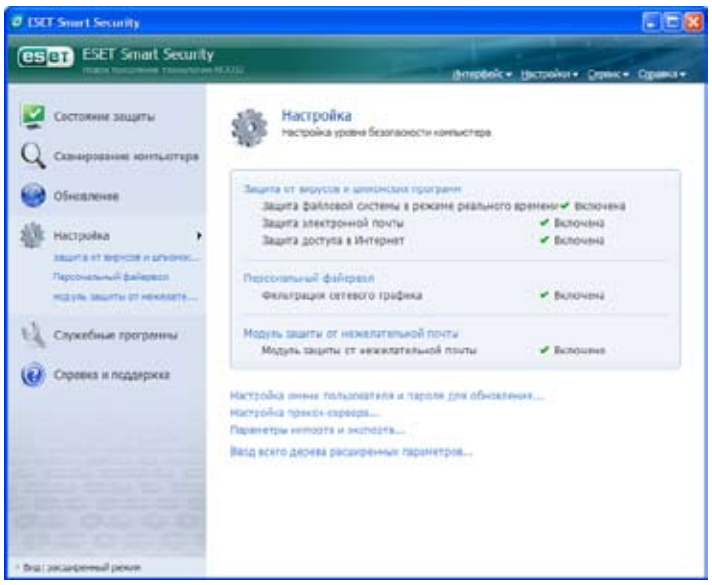
Справка и поддержка (Help and support). С ее помощью вы сможете просматривать справочные файлы, базу данных и веб-страницу ESET, а также отправить запрос для технической поддержки.

В пользовательском интерфейсе ESET NOD32 Smart Security можно переключать стандартный и расширенный режимы. Для того чтобы выбрать необходимый режим, щелкните по индикатору **Отображение** (Display) в нижнем левом углу главного окна ESET NOD32 Smart Security.



Стандартный режим позволяет получить доступ к функциям, необходимым для основных операций. В нем не отображаются дополнительные опции.

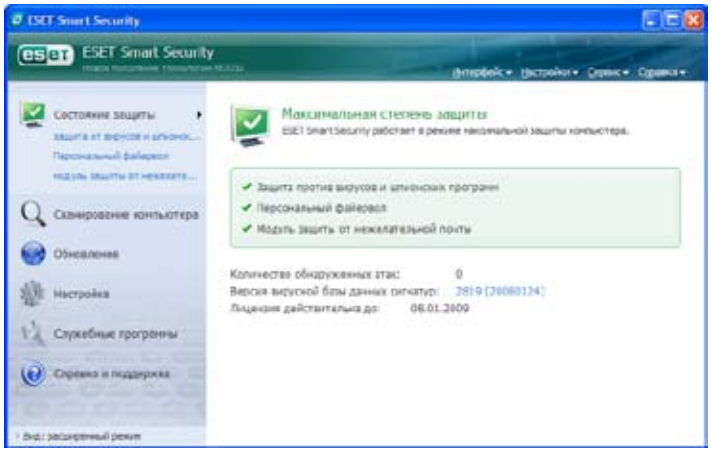
При переключении в расширенный режим в основном меню появляется опция **Инструменты** (Tools). Благодаря ей пользователь получает доступ к опциям планирования, области карантина и файлам журнала ESET NOD32 Smart Security.



Примечание. Остальные инструкции настоящего руководства относятся к расширенному режиму.

3.1.1 Проверка работы системы

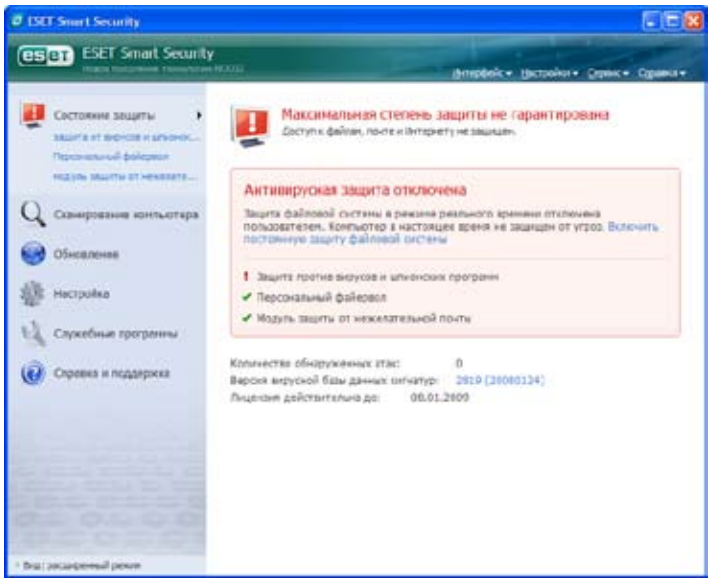
Чтобы просмотреть **Состояние защиты** (Protection status), щелкните по этой опции в верхней части основного меню. В правой части окна появится краткое описание работы ESET NOD32 Smart Security и подменю с тремя пунктами: з**ащита против вирусов и шпионских программ** (Antivirus and antispyware), **персональный файервол** (Personal firewall) и **модуль защиты от спама** (Antispam module). Щелкнув по любому из них, вы получите более подробную информацию о выбранном защитном модуле.



О правильной работе модуля говорит зеленая галочка. Красный восклицательный знак или оранжевая уведомляющая отметка сигнализируют о сбое в работе. В верхней части окна появляется дополнительная информация о данном модуле и предлагается способ решения возникшей проблемы. Для того чтобы изменить статус модуля, выберите опцию **Настройка** (Setup) в основном меню и щелкните по модулю, который хотите изменить.

3.1.2 Что делать, если программа работает неправильно

В случае обнаружения проблемы в одном из защитных модулей ESET NOD32 Smart Security, сообщение об этом появляется в окне **Состояние защиты** (Protection status). Там же предлагается возможное решение проблемы.

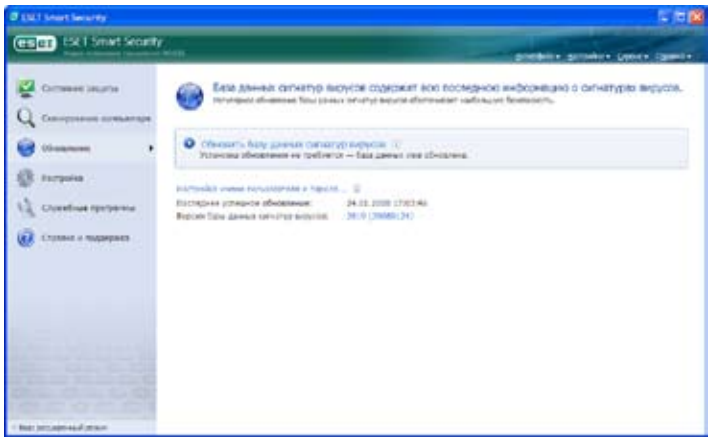


Если в представленном списке известных проблем и способов их решения нет Вашей, выберите опцию **Справка и поддержка** (Help and support) для поиска информации в справочных файлах и базе данных. Если все равно не получается найти решение, Вы можете отправить запрос в службу технической поддержки ESET. Наши специалисты быстро ответят на все ваши вопросы и подскажут наиболее подходящий способ решения проблемы.

3.2 Настройка обновлений

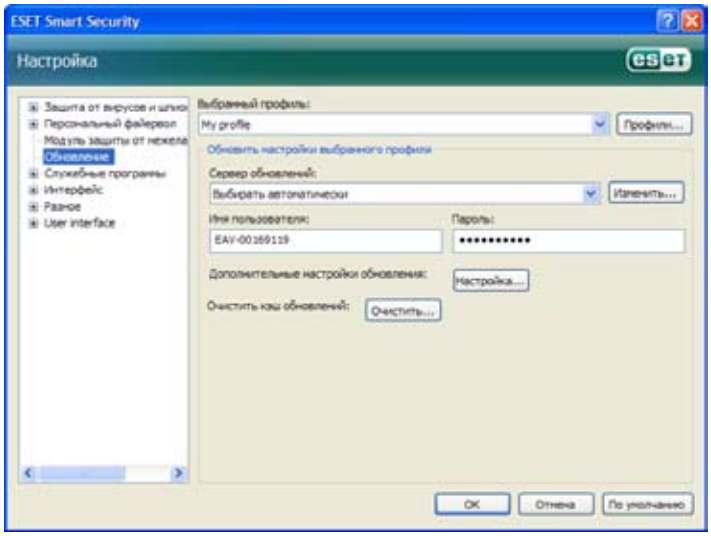
Для полной защиты от вредоносного кода очень важно обновлять базу данных вирусных сигнатур и компоненты программы. Особое внимание следует уделить их работе и настройкам. В основном меню выберите опцию **Обновление** (Update) и нажмите команду **Обновить базу данных вирусных сигнатур** (Update virus signature database) в главном программном окне для того, чтобы проверить наличие обновлений для базы данных. При выборе опции **Настройка имени пользователя и пароля** (User name and Password setup) появляется диалоговое окно, в котором необходимо ввести имя пользователя и пароль, полученные при покупке.

Если вы ввели их во время установки ESET NOD32 Smart Security, то на данном этапе этого делать не требуется.



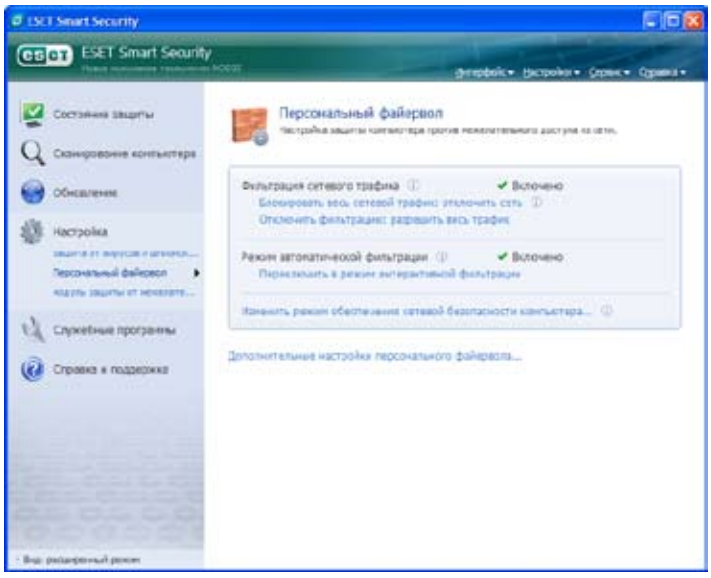
В окне **Расширенная настройка** (Advanced Setup) (для доступа к нему нажмите F5) представлены другие опции обновлений.

Обновление (Update server): из ниспадающего меню должна быть выбрана команда **Выбрать автоматически** (Choose automatically). Для настройки расширенных опций обновления: обновления режима, доступа к прокси-серверу, подключения к обновлениям на локальном сервере и создания копий вирусных сигнатур (ESET NOD32 Smart Security Business Edition), нажмите кнопку **Настройка** (Setup).

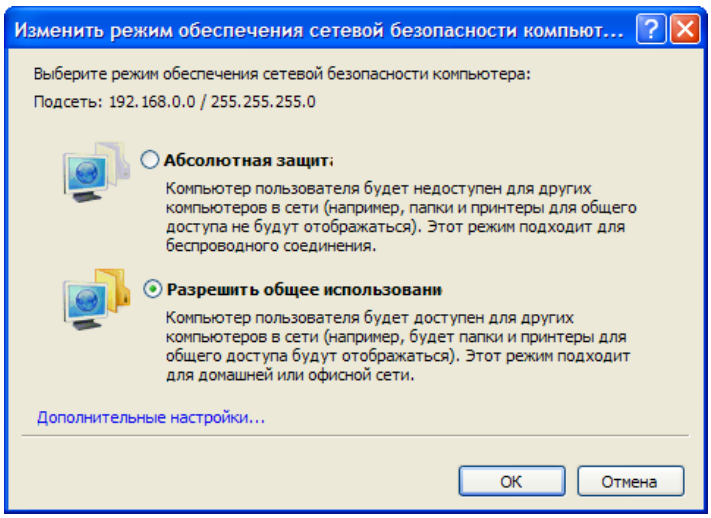


3.3 Настройка доверенных зон

Конфигурация доверенных зон имеет большое значение для обеспечения безопасности вашего компьютера в сетевой среде. У других пользователей будет доступ к вашему компьютеру, если Вы включите функцию совместного использования в настройках доверенной зоны. Для этого выберите команду **Настройка** – **Персональный файервол** – **Изменить режим защиты компьютера в сети** ... (Setup - Personal firewall - Change the protection mode of your computer in the network...) Появится окно, в котором вы сможете менять настройки режима защиты компьютера в фактической сети/зоне.



Обнаружение доверенной зоны производится после установки ESET NOD32 Smart Security, независимо от того, подключен ли компьютер к новой сети. Таким образом, в большинстве случаев нет необходимости определять доверенную зону. По умолчанию при обнаружении доверенной зоны появляется окно, в котором можно установить уровень защиты для нее.

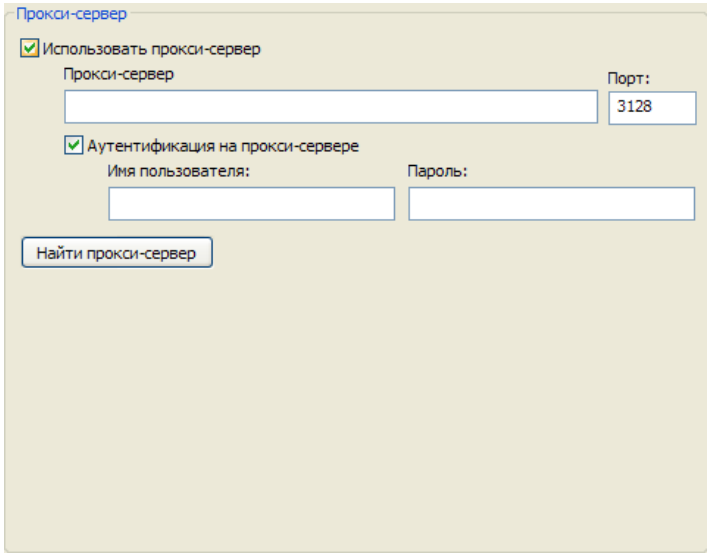


Внимание! Неправильная настройка доверенной зоны может подвергнуть риску безопасность вашего компьютера.

Примечание: По умолчанию рабочие станции из доверенной зоны получают доступ к коллективным файлам и принтерам, включена функция вызова удаленных процедур и возможно коллективное пользование экранной средой.

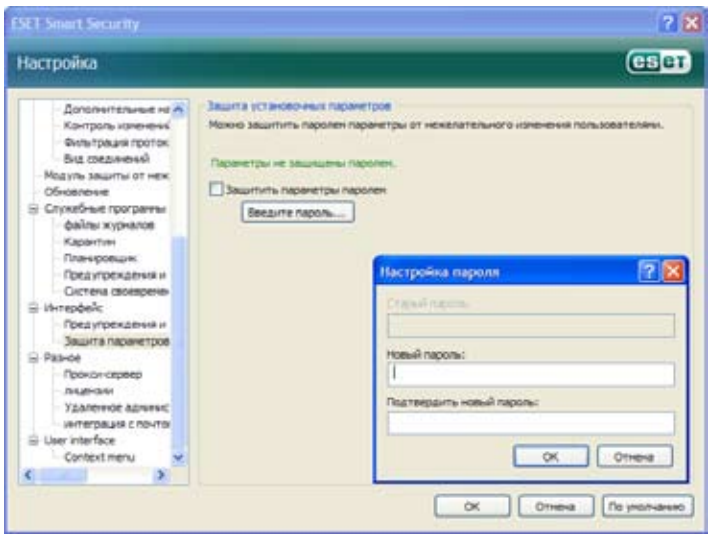
3.4 Настройка прокси-сервера

Если вы используете прокси-сервер для выхода в Интернет в системе, использующей ESET NOD32 Smart Security, она должна быть обозначена в расширенных настройках (F5). Для того чтобы попасть в окно настроек Прокси-сервера (Proxy server), из дерева расширенной настройки выберите команду **Разное** – **Прокси-сервер** (Miscellaneous > Proxy server). Установите флажок **Использовать прокси-сервер** (Use proxy server), затем введите IP адрес, номер порта прокси-сервера и его аутенфикационные данные.



При отсутствии данной информации нажмите кнопку **Найти прокси-сервер** (Detect proxy server), чтобы автоматически обнаружить настройки прокси-сервера для ESET NOD32 Smart Security.

Примечание: Опции прокси-сервера в разных профилях обновлений могут различаться. В таком случае задайте конфигурацию прокси-сервера в расширенных настройках.



3.5 Защита настроек

Настройки ESET NOD32 Smart Security Settings очень важны. Несанкционированное изменение настроек может представлять угрозу для стабильности и безопасности вашей системы. Чтобы защитить параметры настроек паролем, выберите команду **Настройка** – **Дополнительные настройки**... - **Интерфейс** – **Настройка параметров** (Setup – Enter entire advanced setup tree ... - User interface - Settings protection), а затем нажмите кнопку **Ввести пароль** ... (Enter password...).

Введите пароль, подтвердите его, набрав еще раз, и нажмите OK (OK). В дальнейшем чтобы изменить настройки ESET NOD32 Smart Security нужно будет ввести данный пароль.

4.1 Защита от вирусов и шпионских программ

Антивирусная защита охраняет компьютер от атак вредоносных программ, контролируя файлы, электронную почту и связь с Интернетом. В случае обнаружения вредоносного кода модуль антивирусной защиты сначала блокирует его, а затем очищает, удаляет или помещает его в карантин.

4.1.1 Защита файловой системы в режиме реального времени

Защита файловой системы в режиме реального времени контролирует все процессы в системе, связанные с защитой от вирусов. Все файлы сканируются на обнаружение вредоносного кода в момент открытия, создания и запуска в компьютере. Защита файловой системы в режиме реального времени начинает работать в момент запуска системы.

4.1.1.1 Настройки контроля

Защита файловой системы в режиме реального времени проверяет все типы носителей данных и реагирует на различные события. При контроле используются методы технологии ThreatSense (это описано в настройках параметров механизма ThreatSense). Уровень контроля для вновь созданных и уже существующих файлов может быть разным. Для недавно созданных файлов можно применить более высокий уровень контроля.

4.1.1.1.1 Сканирование носителей данных

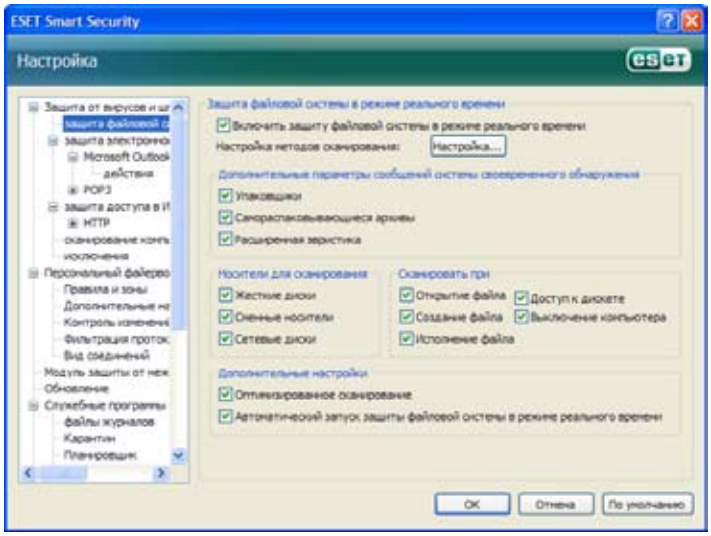
По умолчанию сканируются все носители, могущие содержать потенциальную угрозу.

Локальные диски (Local drives) – контроль над всеми системными жесткими дисками

Сменные носители (Removable media) – дискеты, внешние USB-устройства и т.п.

Сетевые диски (Network drives) – сканирование всех отображаемых дисков

Рекомендуется сохранить настройки «по умолчанию» и менять их только в конкретных случаях, так, например, при сканировании отдельных носителей значительно замедляется передача данных.



4.1.1.1.2 Сканирование в режиме реального времени (сканирование по событию)

По умолчанию все файлы сканируются при открытии, создании и исполнении. Рекомендуется сохранить настройки «по умолчанию», таким образом, вы обеспечите максимальный уровень защиты для своего компьютера.

Опция **Доступ к дискете** (Diskette access) контролирует загрузочный центр на дискете во время доступа к данному диску. Опция **Выключение компьютера** (Computer shutdown) осуществляет контроль над загрузочным центром на жестком диске во время выключения компьютера. Несмотря на то, что загрузочные вирусы сегодня используются очень редко, рекомендуется оставить эти опции включенными, так как есть вероятность заражения загрузочным вирусом из альтернативного источника.

4.1.1.1.3 Дополнительные параметры ThreatSense для вновь созданных файлов

Вероятность заражения вновь созданных файлов намного выше, чем уже существующих. Именно поэтому для проверки этих файлов программой используются дополнительные параметры сканирования. Помимо основных методов на уровне сигнатур, применяются расширенная эвристика, что в значительной степени увеличивает эффективность обнаружения угроз. Наряду с вновь созданными файлами, сканированию подвергаются архивированные файлы (self-extracting files, SFX) и исполняемые архивы (сжатые исполняемые файлы).

4.1.1.1.4 Расширенная настройка

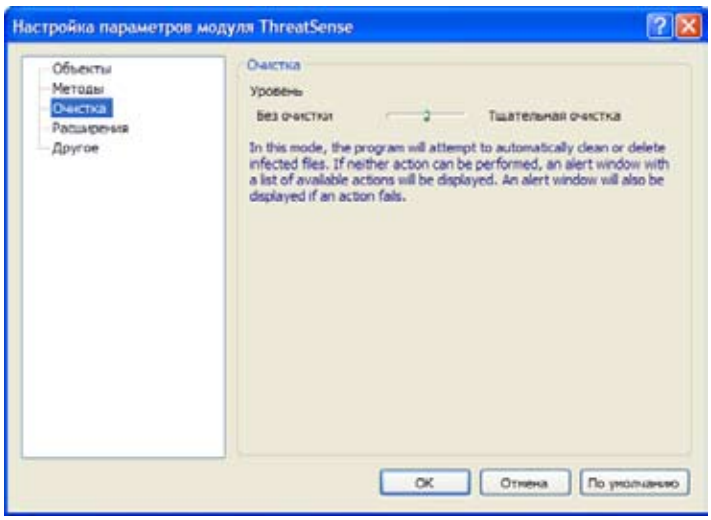
Для минимального использования системных ресурсов во время защиты в реальном времени файлы, которые уже прошли сканирование, будут сканироваться повторно только в том случае, если они изменяются. Однако после обновления базы данных вирусных сигнатур эти файлы будут сканироваться повторно. Данная функция может быть изменена с помощью опции **Оптимизированное сканирование** (Optimized scanning). Если она отключена, то сканирование будет происходить при каждом доступе к файлу.

По умолчанию защита в реальном времени запускается при загрузке операционной системы и производит непрерывное сканирование. В особых случаях, например, при конфликте с другим сканирующим устройством в режиме реального времени, работу защиты в реальном времени можно приостановить, отключив опцию **Автоматический запуск защиты файловой системы в режиме реального времени** (Automatic real-time file system protection startup).

4.1.1.2 Уровни очистки

У защиты в реальном времени имеется три уровня очистки (для выбора зайдите в секцию **Защита в режиме реального времени** (Real-time file system protection), выберите команду **Настройка**... (Setup...) и щелкните по сегменту **Очистка** (Cleaning).

- Первый уровень отображает окно предупреждения с возможными опциями для каждого обнаруженного проникновения. Пользователю нужно выбрать действие для каждого из них. Этот уровень предназначен для более опытных пользователей, которые знают, какие меры необходимо принимать в случае обнаружения вируса.
- Средний уровень (по умолчанию) автоматически выбирает и производит действия, установленные по-умолчанию (в зависимости от типа проникновения) Об обнаружении и действии с зараженным файлом говорится в информационном сообщении, расположенном в нижнем правом углу экрана. Однако автоматическое действие не производится, если проникновение находится в архиве, где содержатся чистые файлы, или если для какого-то объекта не существует предопределенного действия.
- Третий уровень самый «жесткий» - очищаются все зараженные объекты. Использование данного уровня может привести к потере важных файлов, поэтому рекомендуется включать его только в исключительных случаях.



4.1.1.3 Изменение конфигурации защиты в режиме реального времени

Защита в реальном времени является основным условием безопасности системы. Поэтому менять ее параметры следует с большой осторожностью. Рекомендуется вносить изменения только в конкретных случаях. Например, при конфликте с определенным приложением, сканером в реальном времени или другой антивирусной программой.

При установке ESET NOD32 Smart Security подобраны оптимальные настройки для обеспечения максимального уровня системной безопасности. Для восстановления настроек «по умолчанию» в нижнем правом углу окна **Защита файловой системы в реальном времени** (Real-time file system protection) нажмите кнопку **По умолчанию** (Default) (**Расширенная настройка** – **Защита от вирусов и шпионских программ** – **Защита файловой системы в режиме реального времени** (Advanced Setup - Antivirus and antispyware - Real-time file system protection))

4.1.1.4 Проверка режима реального времени

Чтобы проверить, как защита в режиме реального времени работает и обнаруживает вирусы, используйте тестовый файл с сайта eicar.com. Это специальный безопасный файл, обнаруживаемый большинством антивирусных программ. Он был создан Европейским институтом по исследованию антивирусных программ (EICAR, European Institute for Computer Antivirus Research) для проверки их работы. Загрузить файл eicar.com можно с веб-сайта http://www.eicar.org/download/eicar.com

Примечание. Прежде чем начать проверку защиты в режиме реального времени, необходимо отключить файервол. В противном случае он обнаружит тестовый файл и не даст его загрузить.

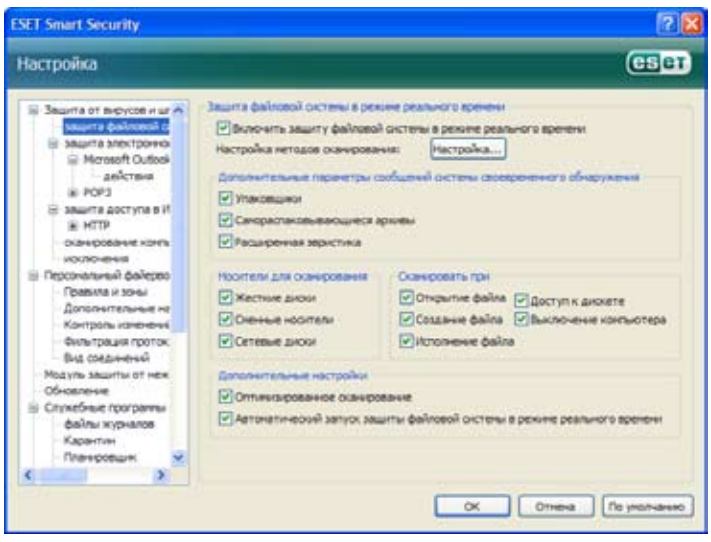
4.1.1.5 Что делать, если защита в режиме реального времени не работает

Ниже описаны основные проблемы, которые могут возникнуть при использовании защиты в режиме реального времени, а также способы их решения.

Защита в режиме реального времени отключена

Если защита в режиме реального времени была случайно отключена, необходимо вновь запустить ее. Для этого нажмите **Настройка** — **Защита от вирусов и шпионских программ** (Setup - Antivirus and antispyware), затем в секции **Защита в режиме реального времени** (Real-time file system protection) в главном программном окне щелкните **Включить** (Enable).

Если защита в режиме реального времени не запускается при загрузке операционной системы, возможно, отключена функция **Автоматический запуск защиты в режиме реального времени** (Automatic real-time file system protection startup). Для того чтобы включить эту опцию, выберите в дереве расширенной настройки опцию **Расширенная настройка** (Advanced setup, F5). Убедитесь, что в нижней части окна в разделе **Расширенная настройка** (Advanced setup) установлен флажок **Автоматический запуск защиты файловой системы в режиме реального времени** (Automatic real-time file system protection startup).



Защита в режиме реального времени не обнаруживает вирусы

Проверьте, нет ли на вашем компьютере другой антивирусной программы. Если две защиты в режиме реального времени включены одновременно, между ними может произойти конфликт. Рекомендуется удалить любые другие антивирусные программы с компьютера.

Защита в режиме реального времени не запускается

Если защита в режиме реального времени не запускается при включении системы (опция **Автоматический запуск защиты файловой системы в режиме реального времени** (Automatic real-time file system protection startup) включена), возможно, произошел конфликт с другими программами. В таком случае необходимо проконсультироваться со специалистами службы технической поддержки ESET.

4.1.2 Защита электронной почты

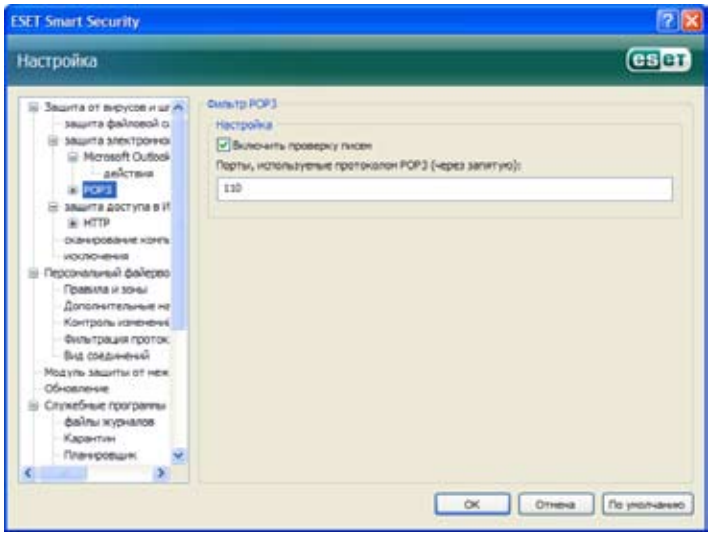
Защита электронной почты контролирует информацию в электронной почте, полученную через протокол POP3. Используя подключаемые программы для Microsoft Outlook, ESET NOD32 Smart Security контролирует все сообщения от клиентов POP3, MAPI, IMAP, HTTP. Во время проверки входящих сообщений программа применяет все расширенные методы сканирования, предоставленные сканирующим механизмом ThreatSense. Это означает, что обнаружение вредоносных программ происходит даже раньше, чем их сопоставление с базой данных вирусных сигнатур. На сканирование данных, передаваемых через протокол POP3, не влияет тип используемого клиента электронной почты.

4.1.2.1 Проверка POP3

Протокол POP3 - самый распространенный протокол для получения сообщений по электронной почте в клиентском приложении. ESET NOD32 Smart Security защищает данный протокол независимо от того, какой клиент электронной почты был использован.

Модуль, осуществляющий контроль, автоматически включается при запуске операционной системы и остается активным. Для правильной работы модуля проверьте, что он включен. Проверка POP3 производится автоматически, для этого не нужно перенастраивать клиент электронной почты. По умолчанию сканируется передача данных через порт 110, но в случае необходимости можно добавить и другие порты. Для разграничения номеров портов необходимо использовать запятую.

Зашифрованная передача данных не контролируется.



4.1.2.1.1 Совместимость

У некоторых программ электронной почты могут быть проблемы с фильтрацией POP3 (например, во время принятия сообщений при медленном интернет соединении - из-за проверки могут быть остановки). В таком случае попробуйте изменить способ осуществления контроля. Понижение уровня контроля может увеличить скорость процесса. Чтобы изменить уровень контроля фильтрации POP3, выберите команду З**ащита от вирусов и шпионских программ** – **Защита электронной почты** - **POP3** – **Совместимость** (Antivirus and antispyware - Email protection - POP3 - Compatibility).

Если включена **Максимальная эффективность** (Maximum efficiency), то вирусы удаляются из зараженных сообщений, а информация о них

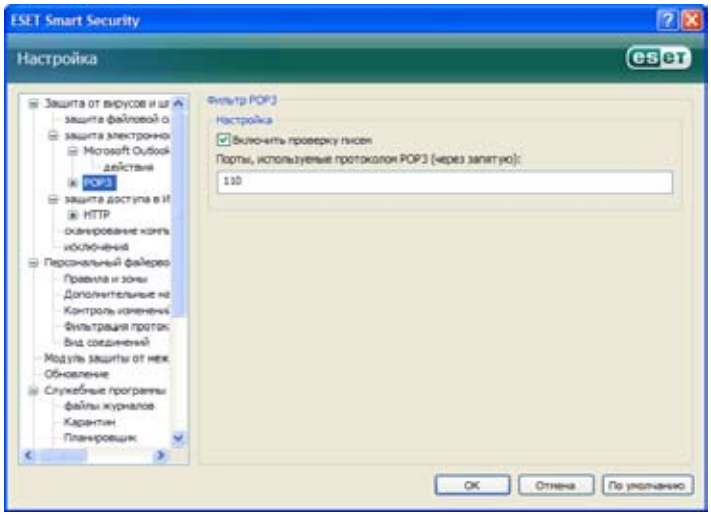
выносится перед исходной темой сообщения (должны быть включены опции **Удалить** (Delete) или **Очистить** (Clean), уровень очистки должен быть **Строгий** (Strict) или **По умолчанию** (Default)).

Средняя совместимость (Medium compatibility) меняет способ получения сообщений. Сообщения постепенно посылаются клиенту электронной почты, после передачи последней части сообщения оно будет просканировано на обнаружение вирусов.

Однако при данном уровне контроля увеличивается риск заражения. Уровень очистки и обработка теговых сообщений (уведомлений об опасности, которые добавляются в строку темы письма или к самому сообщению) тот же, что и при Максимальной эффективности.

Если включена **Максимальная совместимость** (Maximum compatibility), то каждый раз при получении зараженного сообщения будет появляться окно предупреждения.

В строке темы письма или в тексте полученного сообщения пометок о заражении не появляется. Обнаруженные вирусы не удаляются автоматически. Пользователь клиента электронной почты должен сам это делать.



4.1.2.2 Интеграция с Microsoft Outlook, Outlook Express и Windows Mail

Интеграция ESET NOD32 Smart Security с клиентами электронной почты увеличивает уровень активной защиты от вредоносного кода в электронных сообщениях.

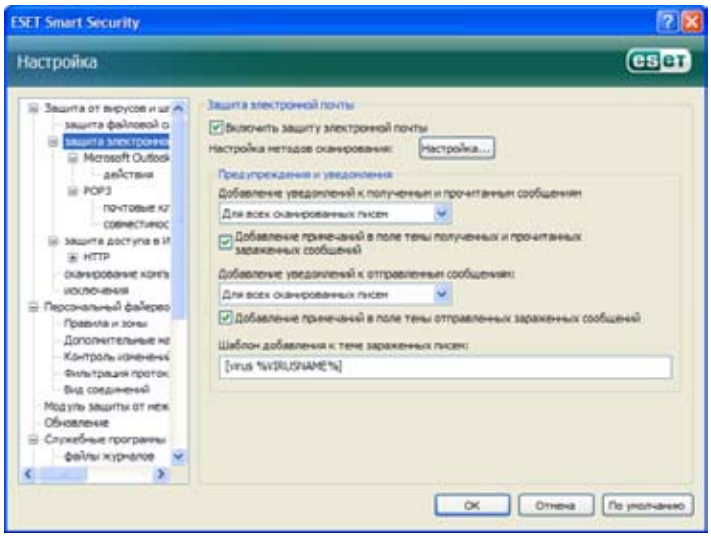
Если ESET NOD32 Smart Security поддерживает ваш клиент электронной почты, то можно произвести интеграцию. Тогда панель инструментов антиспама ESET NOD32 Smart Security будет находиться непосредственно в клиенте электронной почты. Таким образом, защита электронной почты будет более эффективна. Для настройки интеграции выберите команду **Настройка** – **Дополнительные настройки**... –**Разное** – **Интеграция с почтой** (Setup - Enter entire advanced setup tree... - Miscellaneous - Email client integration). В диалоговом окне можно активировать интеграцию с поддерживаемыми клиентами электронной почты. В настоящее время поддерживаются такие клиенты электронной почты, как Microsoft Outlook, Outlook Express и Windows Mail

Поле установки флажка **Включить защиту электронной почты** (Enable email protection) (**Расширенная настройка** (F5) – **Защита от вирусов и шпионских программ** – **Защита электронной почты** (Advanced Setup (F5) - Antivirus and antispyware - Email protection)), защита почты будет включена.

4.1.2.2.1 Добавление теговых сообщений к тексту письма

Каждое письмо, контролируемое ESET NOD32 Smart Security можно пометить, прибавив теговое сообщение к теме или тексту письма. Данная функция позволяет адресату чувствовать себя в большей безопасности, - в случае обнаружения вируса он получает ценную информацию об уровне опасности сообщения/отправителя.

Данную опцию можно активировать, выбрав команду **Расширенная настройка** – **Защита от вирусов и шпионских программ** – **Защита электронной почты** (Advanced setup - Antivirus and antispyware protection - Email protection). В программе можно **Добавить теговые сообщения к полученным и прочитанным сообщениям** (Append tag messages to received and read mail), а также **Добавить теговые сообщения к отправленным письмам** (Append tag messages to sent mail). Пользователь сам решает, к каким письмам необходимо добавить теговое сообщение. В ESET NOD32 Smart Security есть функция добавления сообщений к исходному содержанию зараженных сообщений. Для этого выберите одну из опций **Добавить теговые сообщения к полученным и прочитанным зараженным сообщениям** (Append tag messages to the subject of received and read infected mail) или **Добавить теговые сообщения к отправленным зараженным письмам** (Append tag messages to the subject of sent infected mail).



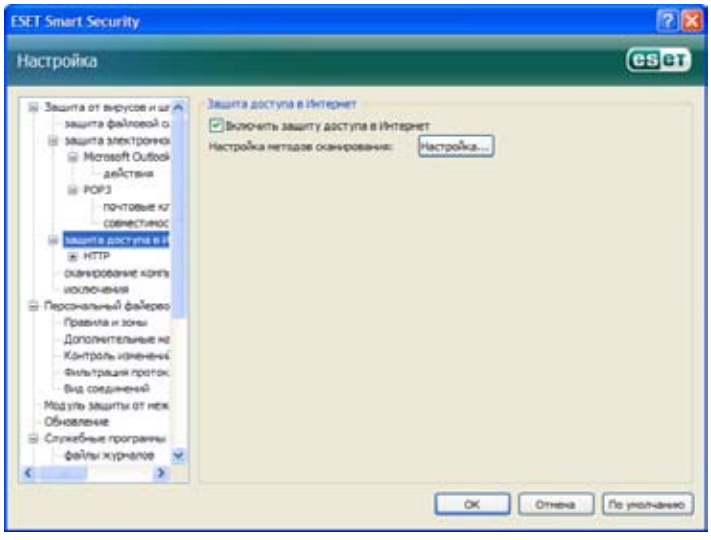
Содержание уведомлений можно изменять в поле образца, присоединенного к зараженному сообщению. Перечисленные выше настройки помогут автоматизировать процесс фильтрации зараженных сообщений, так как письма с определенной темой перемещаются в отдельную папку (при условии, что данная функция поддерживается вашим клиентом электронной почты).

4.1.2.3 Удаление вирусов

При получении зараженного сообщения появляется окно предупреждения. В нем указывается имя отправителя, текст сообщения и название вируса. В нижней части окна располагаются опции **Очистить** (Clean), **Удалить** (Delete), и **Оставить** (Leave). В большинстве случаев рекомендуется выбрать либо **Очистить** (Clean), либо **Удалить** (Delete). В случае если вы хотите принять зараженный файл, нажмите **Оставить** (Leave). Если включена функция **Строгой очистки** (Strict cleaning), то появится информационное окно, однако какие либо операции с зараженными объектами невозможны.

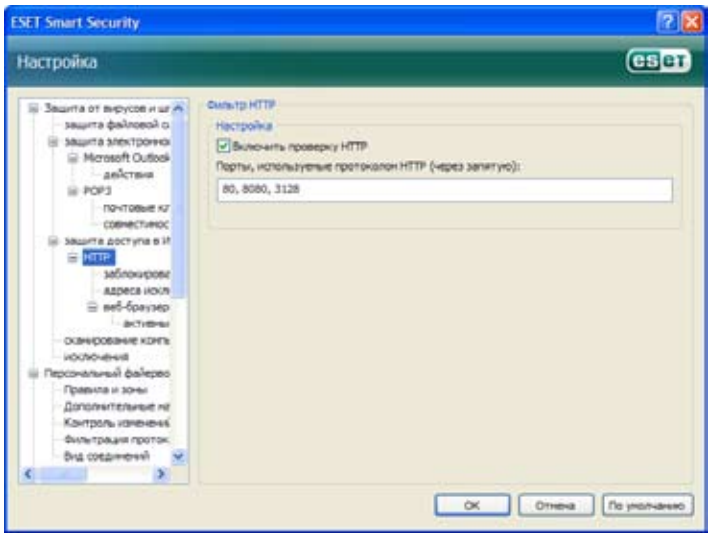
4.1.3 Защита веб-доступа

Функция подключения к Интернету имеется у каждого персонального компьютера. К сожалению, Интернет - это основное средство передачи вредоносных кодов. Вот почему защита веб-доступа играет очень большую роль. Настоятельно рекомендуется активировать функцию **Включить защиту доступа в Интернет** (Enable web access protection). Это можно сделать, выбрав путь **Расширенная настройка** - **Защита от вирусов и шпионских программ** – **Защита доступа в Интернет** (Advanced Setup (F5) > Antivirus and antispyware protection > Web access protection).



4.1.3.1 HTTP

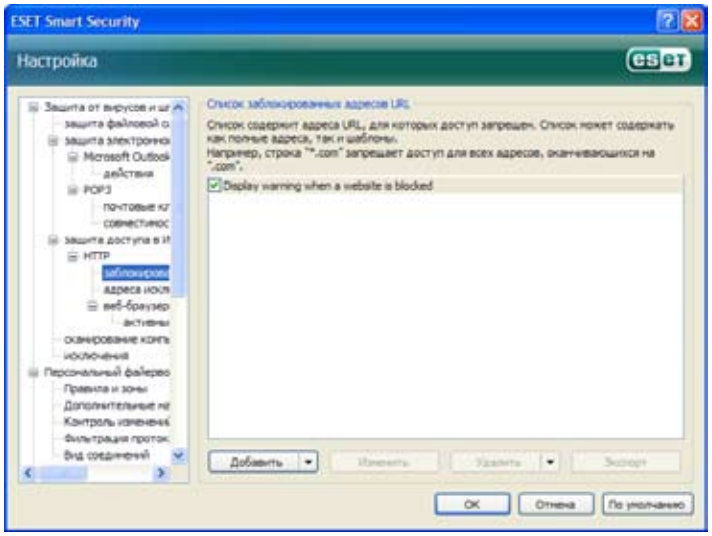
Основной функцией защиты доступа в Интернет является мониторинг соединений между интернет-браузерами и удаленными серверами в соответствии с правилами протокола HTTP (Hypertext Transfer Protocol, протокол передачи гипертекста). По умолчанию ESET NOD32 Smart Security использует HTTP-стандарты большинства интернет-браузеров. Однако часть параметров настройки HTTP-проверки можно изменить в разделе **Защита доступа в Интернет** - **HTTP** (Web access protection - HTTP). В окне **Настройка HTTP-фильтрации** (HTTP filter Setup) можно включать и отключать HTTP-проверку с помощью опции **Включить HTTP-проверку** (Enable HTTP checking). Здесь также можно определить номера портов, используемых системой для HTTP-соединений. По умолчанию используются порты 80, 8080 и 3128. Можно задать автоматическое обнаружение и сканирование HTTP-трафика любого порта, добавив дополнительные номера портов через запятую.

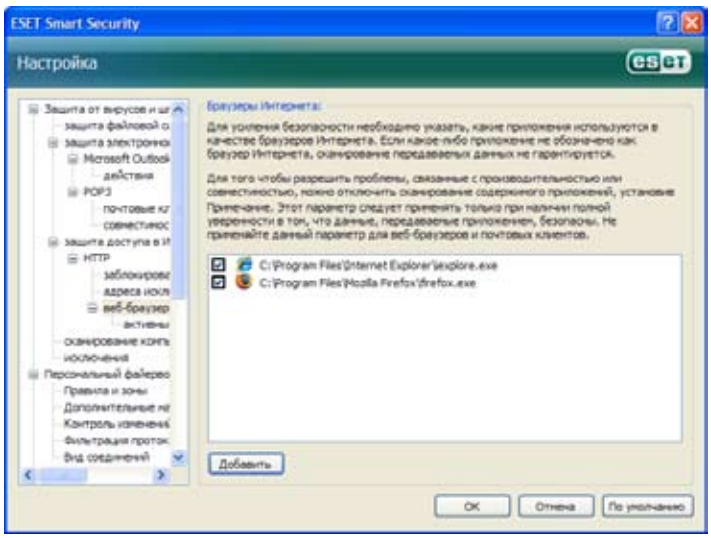


4.1.3.1.1 Заблокированные и исключенные адреса

Настройка HTTP-проверки позволяет создавать **списки для заблокированных адресов** (Blocked addresses) или **исключения** (Excluded addresses) URL-адресов (унифицированных указателей информационных ресурсов).

Оба диалоговых окна содержат кнопки **Добавить** (Add), **Изменить** (Edit), **Удалить** (Remove) и **Экспорт** (Export), позволяющие с легкостью управлять списками указанных адресов. Если запрашиваемый пользователем адрес включен в список заблокированных, доступ к соответствующему ресурсу будет невозможен. Если же адрес входит в список исключений, доступ к ресурсу будет предоставлен без проверки на предмет наличия вредоносных программ. В обоих списках можно использовать специальные символы «*» (звездочка) и «?» (вопросительный знак). Вопросительный знак заменяет собой любой символ, а звездочка – строку символов. Списку исключаемых адресов следует уделять особое внимание, включая в него только надежные и безопасные адреса. Также следует убедиться, что символы «*» и «?» используются в этом списке корректно.



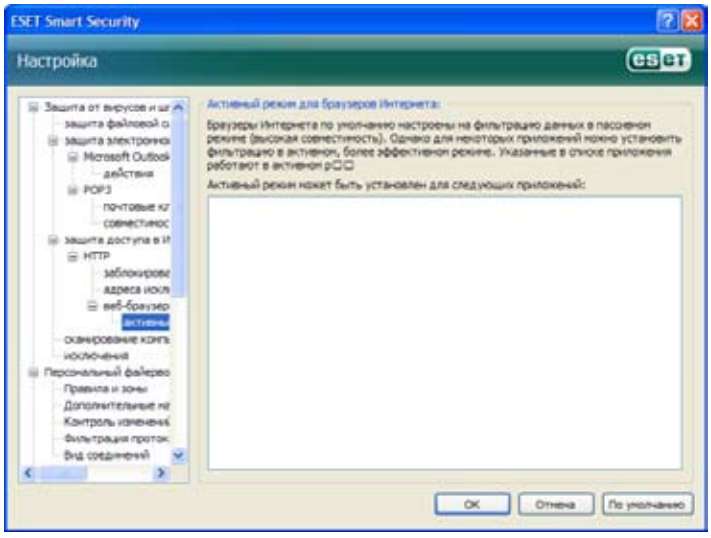


4.1.3.1.2 Веб-браузеры

ESET NOD32 Smart Security также содержит функцию **Веб-браузеры** (Web browsers), позволяющую пользователю указывать, является ли некое приложение браузером. Если приложение отмечается как браузер, все его соединения отслеживаются вне зависимости от номеров портов, участвующих в соединении.

Функция Веб-браузеры дополняет функцию HTTP-проверки, поскольку действие последней распространяется только на заранее заданные порты, при этом многие интернет-службы используют динамически изменяющиеся или неизвестные номера портов. Функция «Веб-браузеры» позволяет осуществлять контроль над соединениями портов вне зависимости от параметров подключения.

Список приложений, отмеченных как браузеры, можно открыть прямо из подменю **Веб-браузеры** (Web browsers) ветки HTTP. Этот раздел также содержит подменю **Активный режим** (Active mode), определяющее режим проверки для интернет-браузеров. Активный режим полезен тем, что передаваемые данные проверяются как единое целое. Если же он не включен, соединения приложений отслеживаются постепенно, пакетами. Это снижает эффективность процесса проверки данных, зато повышает совместимость включенных в список приложений. Если использование активного режима проверки не вызывает никаких проблем, рекомендуется включить именно его, установив флажок рядом с нужным приложением.



4.1.4 Сканирование компьютера

Если есть подозрение, что компьютер заражен (то есть его поведение необычно), выполните его сканирование по требованию, чтобы обнаружить возможные угрозы. С точки зрения безопасности, важно периодически выполнять сканирование компьютера. Регулярное сканирование обеспечивает обнаружение угроз, которые не были обнаружены при сканировании в реальном времени при сохранении на диск. Такое мо-

жет случиться, если сканер реального времени был отключен во время заражения или если устарела база данных вирусных сигнатур.

Сканирование по требованию рекомендуется выполнять по меньшей мере раз или два в месяц. Настроить его плановое выполнение можно с помощью пункта меню Инструменты - Планировщик (Tools - Scheduler).

4.1.4.1 Тип сканирования

Доступно сканирование двух видов. **Стандартное сканирование** (Standard scan) – это быстрое сканирование системы без необходимости дополнительной настройки параметров. **Выборочное сканирование** (Custom scan...) позволяет пользователю выбрать один из профилей сканирования по-умолчанию, а также указать для него объекты из древовидной структуры.

4.1.4.1.1 Стандартное сканирование

Стандартный режим сканирования является удобным для пользователя методом, позволяющим быстро запустить сканирование компьютера для обнаружения и очистки любых зараженных файлов без необходимости вмешательства пользователя. Его основными преимуществами является простота в обращении и отсутствие подробной настройки. При стандартном сканировании проверяются все файлы на локальных дисках (исключая файлы электронной почты и архивы), а обнаруженные файлы с угрозами автоматически очищаются или удаляются. Для уровня очистки автоматически задается значение по умолчанию. Для получения более подробных сведений о типах очистки см. раздел «Очистка» на странице 18.

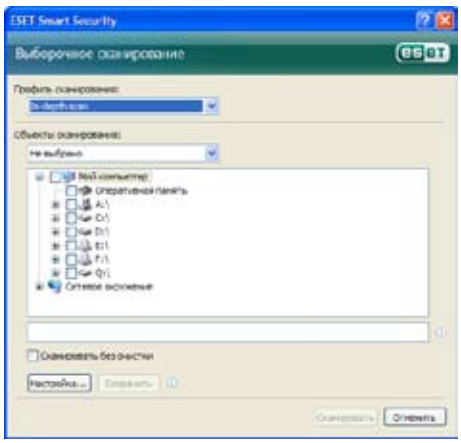
Профиль стандартного сканирования предусмотрен для пользователей, желающих быстро и легко просканировать свои компьютеры. Он предоставляет эффективное решение по сканированию и очистке, не требующее подробной настройки.

4.1.4.1.2 Выборочное сканирование

Выборочный режим сканирования является оптимальным решением при необходимости указать параметры сканирования, такие как объекты и методы сканирования. Преимуществом выборочного режима является возможность подробной настройки параметров. Эти настройки могут быть затем сохранены как определяемые пользователем профили сканирования и использованы в дальнейшем для повторения сканирования с теми же параметрами.

Для выбора объектов сканирования можно воспользоваться раскрывающимся меню функции быстрого выбора объектов либо выбрать объекты из древовидной структуры, в которой представлены все доступные устройства компьютера. Кроме того, имеются три уровня очистки, которые можно выбрать при помощи команды **Настройка** - **Очистка** (Setup - Cleaning). Если требуется выполнить только сканирование системы без дополнительных действий, следует установить флажок **Сканирование без очистки** (Scan without cleaning).

Выполнение выборочного сканирования предназначено для более опытных пользователей, имеющих опыт работы с антивирусными программами.



4.1.4.2 Объекты сканирования

Раскрывающееся меню **Объекты сканирования** (Scan targets) позволяет выбирать файлы, папки и устройства (диски) для антивирусного сканирования.

С помощью пунктов меню быстрого выбора объектов сканирования можно выбрать следующие объекты:

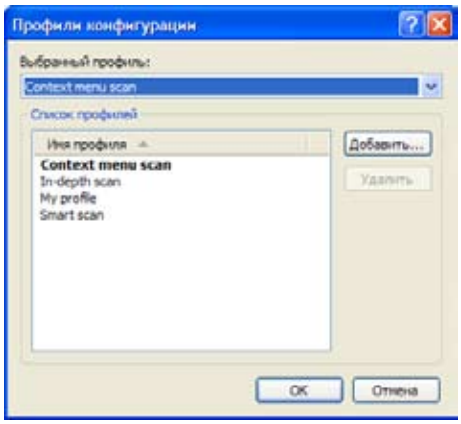
- **локальные диски** (Local drives) – все жесткие диски в системе.
- **съемные носители** (Removable media) – дискеты, запоминающие устройства USB, компакт-диски и DVD-диски.
- **сетевые диски** (Network drives) – все отображенные диски.

Объект сканирования также можно указать более точно, задав путь к папке или файлам, которые требуется проверить. Для этого выберите объекты из древовидной структуры, где представлены все доступные устройства компьютера.

4.1.4.3 Профили сканирования

Предпочтительные параметры сканирования компьютера можно сохранять в виде профилей. Преимуществом создания профилей сканирования является возможность их регулярного использования в дальнейшем. Рекомендуется создать столько профилей с различными объектами, методами и другими параметрами сканирования, сколько его вариантов регулярно используется.

Чтобы создать новый профиль сканирования, который можно будет повторно использовать в будущем, выберите пункт меню **Расширенная настройка** (F5) - **Сканирование компьютера по требованию** (Advanced setup - On-demand computer scan). Нажмите расположенную справа кнопку **Профили**... (Profiles...), чтобы открыть список существующих профилей сканирования и опцию создания нового профиля. В следующем разделе («Настройка параметров ядра ThreatSense») будут подробно описаны все параметры настройки сканирования. Это поможет создавать необходимые профили сканирования.



Пример:

Предположим, необходимо создать собственный профиль сканирования, и настройки профиля «Интеллектуальное сканирование» частично совпадают с нужными. Только вот сканирование архивов, вызываемых во время выполнения, или потенциально опасных приложений не нужно и, кроме

того, хотелось бы применять полную очистку. В окне **Профили настроек** (Configuration profiles) нажмите кнопку **Добавить**... (Add...). В поле **Имя профиля** (Profile name) введите имя создаваемого профиля и выберите пункт **Интеллектуальное сканирование** (Smart scan) в раскрывающемся меню **Скопировать параметры из профиля** (Copy settings from profile). Затем настройте остальные параметры по собственному усмотрению.

4.1.5 Настройка параметров ядра ThreatSense

ThreatSense – это название технологии, включающей в себя комплекс методов обнаружения угроз. Это проактивная технология, что означает предоставление ею защиты даже в первые часы распространения новой угрозы. В ней используется комбинация нескольких методов (анализ кода, эмуляция кода, родовые сигнатуры, вирусные сигнатуры), работающих в сочетании, что значительно повышает безопасность системы. Ядро сканирования способно контролировать несколько потоков данных одновременно, максимально увеличивая эффективность и уровень обнаружения. Также технология ThreatSense успешно детектирует руткиты.

Опции настройки технологии ThreatSense позволяют пользователю задавать различные параметры сканирования:

- Типы и расширения файлов, которые необходимо сканировать.
- Сочетание различных методов обнаружения.
- Уровни очистки и т.д.

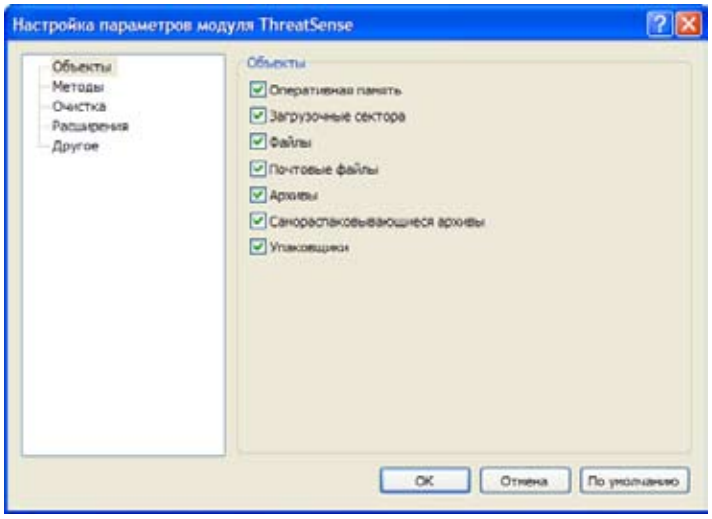
Чтобы открыть окно настройки, нажмите кнопку **Настройка**... (Setup...), расположенную в окнах настройки всех модулей, использующих технологию ThreatSense (см. ниже). Для разных сценариев безопасности могут требоваться различные настройки. Поэтому ThreatSense может индивидуально настраиваться для следующих модулей системы безопасности:

- защита файловой системы в реальном времени.
- проверка файлов при запуске системы.
- защита электронной почты.
- защита веб-доступа.
- сканирование компьютера по требованию.

Параметры ThreatSense для каждого модуля имеют высокую степень оптимизации, поэтому их изменение может существенно повлиять на производительность системы. Например, если задать параметр сканирования архивов, вызываемых во время выполнения, или включить расширенную эвристику в модуле защиты файловой системы в реальном времени, быстродействие системы может снизиться (обычно с помощью этих методов сканируются только создаваемые файлы). Поэтому рекомендуется не изменять заданные по умолчанию параметры ThreatSense для всех модулей, кроме сканирования компьютера.

4.1.5.1 Настройка объектов

Раздел **Объекты** (Objects) позволяет определять, какие компоненты компьютера и файлы будут сканироваться на предмет наличия проникновений:



Оперативная память (Operating memory) – сканирование на предмет угроз, нацеленных на оперативную память системы.

Загрузочные секторы (Boot sectors) – сканирование загрузочных секторов на предмет наличия вирусов в основной загрузочной записи.

Файлы (Files) – сканирование всех обычных типов файлов (программы, картинки, звуковые файлы, видеофайлы, файлы баз данных и т.д.).

Файлы электронной почты (Email files) – сканирование специальных файлов, где хранятся сообщения электронной почты.

Архивы (Archives) – сканирование файлов, сжатых в архивы (RAR, ZIP, ARJ, TAR и т.д.).

Самораскрывающиеся архивы (Self-extracting archives) – сканирование файлов, содержащих самораскрывающиеся архивы, но обычно имеющих расширение EXE.

Упаковщики (Runtime packers) – сканирование архивов, распаковываемых в памяти (в отличие от обычных архивов), и стандартных статических упаковщиков (UPX, yoda, ASPack, FGS и т.д.).

4.1.5.2 Методы

В разделе **Методы** (Options) пользователь может выбрать методы, которые будут использоваться при сканировании системы на предмет наличия проникновений. Доступны следующие варианты:

Сигнатуры (Signatures) – точное и надежное обнаружение и определение проникновений по записям с помощью вирусных сигнатур.

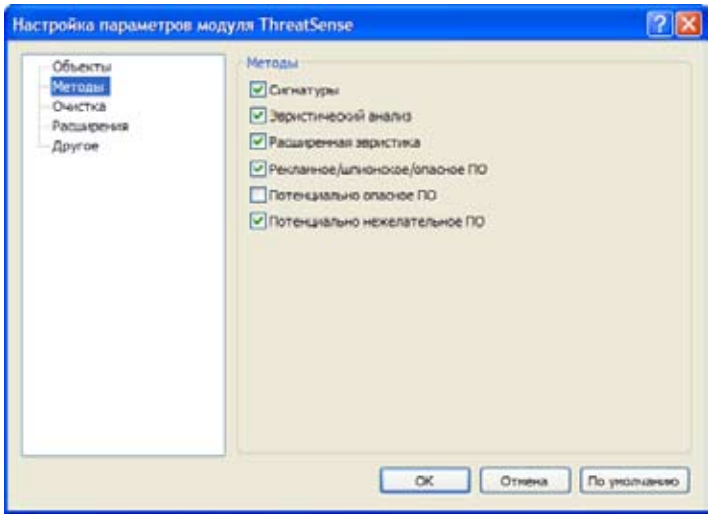
Эвристический анализ (Heuristics) – использование алгоритма анализа функционирования программ в поисках вредоносного ПО. Основным преимуществом эвристической проверки является возможность обнаружения нового вредоносного ПО, которое ранее не существовало или не было внесено в список известных вирусов (в базу данных вирусных сигнатур).

Расширенная эвристика (Advanced heuristics) – оптимизированный вариант уникального эвристического алгоритма, разработанный ESET и предназначенный для обнаружения компьютерных червей и троянов, написанных на языках программирования высокого уровня. Возможности расширенной эвристики значительно повышают уровень «интеллекта» программы при обнаружении угроз.

Рекламное, шпионское, опасное ПО (Adware/Spyware/Riskware). К этой категории относится ПО, собирающее различную конфиденциальную информацию о пользователях без их уведомления и согласия. Сюда также включается ПО, отображающее рекламные материалы.

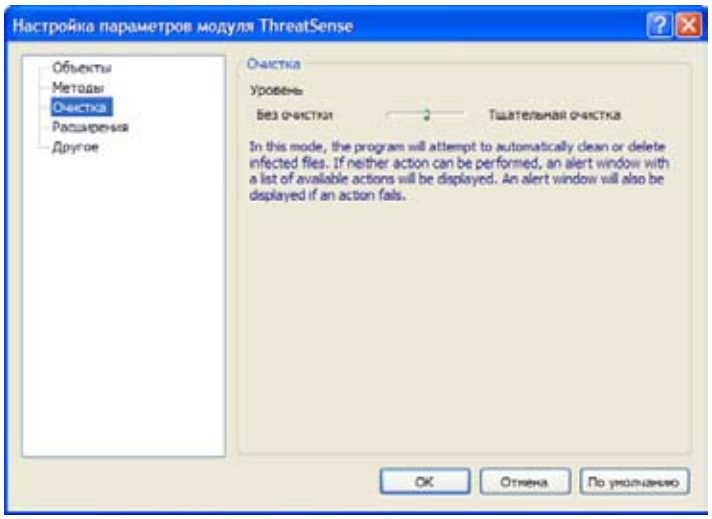
Потенциально опасное ПО (Potentially unsafe applications) – категория, включающая в себя допустимое коммерческое ПО, такое как средства удаленного доступа. Поэтому по умолчанию эта опция отключена.

Потенциально нежелательное ПО (Potentially unwanted applications) не обязательно считаются вредоносными, но могут снизить быстродействие компьютера. Для установки таких приложений обычно требуется согласие пользователя. Если они уже установлены на компьютере, система ведет себя иначе по сравнению с тем, что было до установки. Наиболее значительные изменения включают в себя появление нежелательных всплывающих окон, активацию и выполнение скрытых процессов, увеличение использования системных ресурсов, изменение результатов поиска и возникновение соединений приложений с удаленными серверами.



4.1.5.3 Очистка

Параметры очистки определяют поведение сканера при очистке зараженных файлов. Существует три уровня очистки:



Без очистки (No cleaning)

Автоматическая очистка зараженных файлов не производится. Выводится окно оповещения, и пользователь может сам выбрать нужное действие.

Уровень по умолчанию

Выполняется попытка автоматически очистить или удалить зараженный файл. Если автоматический выбор правильного действия невозможен, выбор последующих действий предлагается пользователю. Также, предлагается действие на выбор , если предопределенное действие не может быть выполнено.

Полная очистка (Strict cleaning)

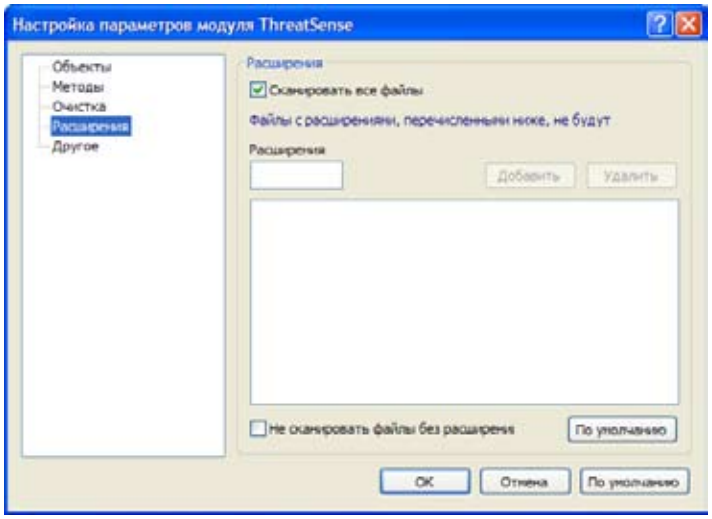
Все зараженные файлы, включая архивы, очищаются или удаляются программой. Единственное исключение составляют системные файлы. Если их не удается очистить, пользователю с помощью окна оповещения предлагается выполнить нужное действие.

Внимание!

В режиме по умолчанию файл архива удаляется целиком, только если инфицированы все находящиеся в нем файлы. Если в него входят и нормальные файлы, он не удаляется. Если же зараженный архив обнаруживается в режиме полной очистки, он удаляется целиком, даже если содержит и чистые файлы тоже.

4.1.5.4 Расширения

Расширение – это часть имени файла, отделенная точкой. Расширение определяет тип и содержимое файла. Раздел **Расширения** (Extensions) параметров настройки ThreatSense позволяет определять, какие типы файлов следует сканировать.



По умолчанию сканируются все файлы независимо от расширений. При этом в список файлов, исключаемых из сканирования, можно добавить любые расширения.

Если снять флажок **Сканировать все файлы** (Scan all files), открывается список, включающий в себя все расширения файлов, которые сканируются в настоящее время.

С помощью кнопок **Добавить** (Add) и **Удалить** (Remove) можно разрешить или запретить сканирование файлов с нужными расширениями.

Чтобы сделать невозможным сканирование файлов без расширений, выберите опцию **Не сканировать файлы без расширений** (Scan extensionless files).

Исключение файлов из сканирования имеет смысл в том случае, если сканирование файлов определенных типов мешает нормальной работе программ, использующих их. Например, при использовании MS Exchange Server целесообразно исключить из сканирования файлы с расширениями EDB, EML и TMP.

4.1.6 Обнаружение проникновения

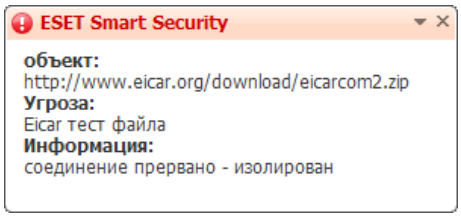
Угрозы могут проникать в систему разными путями: с веб-страниц, из совместно используемых папок, по электронной почте или через съемные носители, такие как USB-устройства, внешние диски, компакт-диски, DVD-диски, дискеты и т.д.

Если компьютер подает признаки заражения, то есть работает медленнее, часто «подвисает» и т.д., рекомендуется выполнить следующие действия:

- Откройте ESET NOD32 Smart Security и щелкните пункт меню **Сканирование компьютера** (Computer scan).
- Щелкните опцию **Стандартное сканирование** (Standard scan) (для получения более подробных сведений см. раздел «Стандартное сканирование»).
- По завершении сканирования просмотрите журнал, чтобы узнать число просканированных, зараженных и очищенных файлов.

Если требуется просканировать только определенную часть диска, выберите опцию **Выборочное сканирование** (Custom scan) и укажите объекты для антивирусного сканирования.

Чтобы понять, как ESET NOD32 Smart Security обрабатывает проникновения, представьте себе, что угроза была обнаружена при мониторинге файловой системы в реальном времени с использованием уровня очистки по умолчанию. Будет выполнена попытка очистить или удалить файл. Если предопределенное действие для модуля защиты в реальном времени не задано, пользователь получит запрос на выбор действия в окне оповещения. Обычно доступны опции Очистить (Clean), Удалить (Delete) и Оставить (Leave). Выбор опции «Оставить» не рекомендуется, так как в этом случае зараженные файлы остаются нетронутыми. Исключение составляют ситуации, когда есть уверенность в том, что эти файлы безопасны и обнаружены по ошибке.



Очистка и удаление

Очистку следует применять, если чистый файл был атакован вирусом, присоединившим к нему вредоносный код. В этом случае сначала следует попытаться очистить зараженный файл, чтобы восстановить его исходное состояние. Если файл состоит исключительно из вредоносного кода, он будет удален.

Если зараженный файл заблокирован или используется каким-либо системным процессом, он обычно удаляется после того, как становится доступен (как правило, после перезагрузки системы).

Удаление файлов из архивов

В режиме очистки по умолчанию архив целиком удаляется в том случае, если он содержит только зараженные файлы, без чистых. Другими словами, архивы не удаляются, если в них есть безопасные чистые файлы. При сканировании с полной очисткой следует соблюдать осторожность, поскольку в этом случае архив удаляется, даже если содержит всего один зараженный файл, независимо от состояния других файлов в архиве.

4.2. Персональный файервол

Персональный файервол – это средство контроля всего сетевого трафика системы, как входящего, так и исходящего. Это достигается путем разрешения или запрещения отдельных сетевых подключений на основании заданных правил фильтрации. Файервол обеспечивает защиту от атак с удаленных компьютеров и позволяет блокировать отдельные службы. Он также предоставляет антивирусную защиту для протоколов HTTP и POP3. Эта функциональная возможность представляет собой крайне важный элемент системы безопасности компьютера.

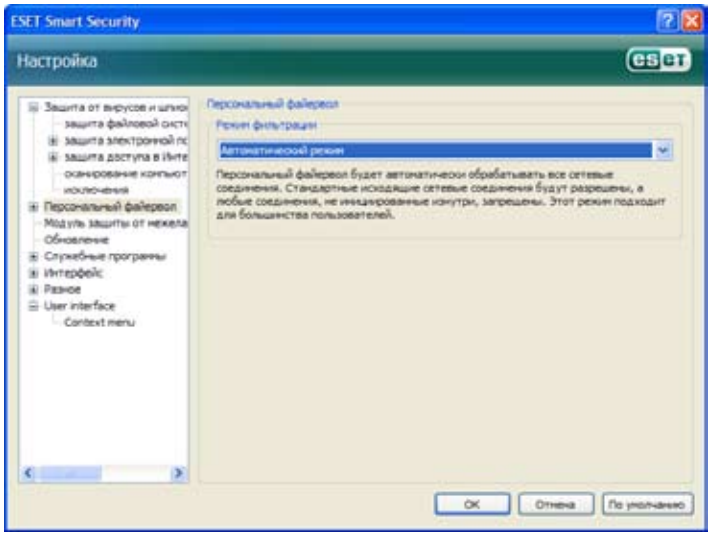
4.2.1 Режимы фильтрации

Для персонального файервола ESET NOD32 Smart Security существует три режима фильтрации. В зависимости от выбранного режима поведение файервола меняется. Режимы фильтрации также влияют на уровень необходимого участия пользователя.

Фильтрация может выполняться в одном из следующих трех режимов:

- **Автоматический режим** (Automatic mode) является режимом по умолчанию. Он предназначен для пользователей, предпочитающих простое и удобное использование файервола без необходимости определять правила. В автоматическом режиме для данной системы разрешен весь исходящий трафик и блокируются все новые соединения, запрашиваемые со стороны сети.
- **Интерактивный режим** (Interactive mode) позволяет настраивать персональный файервол. При обнаружении подключения, если не существует правила, которое можно к нему применить, открывается диалоговое окно с сообщением о неизвестном подключении. В диалоговом окне представлены опции разрешения и запрещения соединения, а принятое решение может быть запомнено в виде нового правила для персонального файервола. Если пользователь при этом выбирает создание нового правила, все будущие подключения этого типа будут разрешаться или блокироваться в соответствии с данным правилом.
- **Режим на основе политик** (Policy-based mode) блокирует все подключения, не определенные конкретными правилами, разрешающими их. Этот режим позволяет опытным пользователям определять правила, разрешающие только нужные и безопасные подключения.

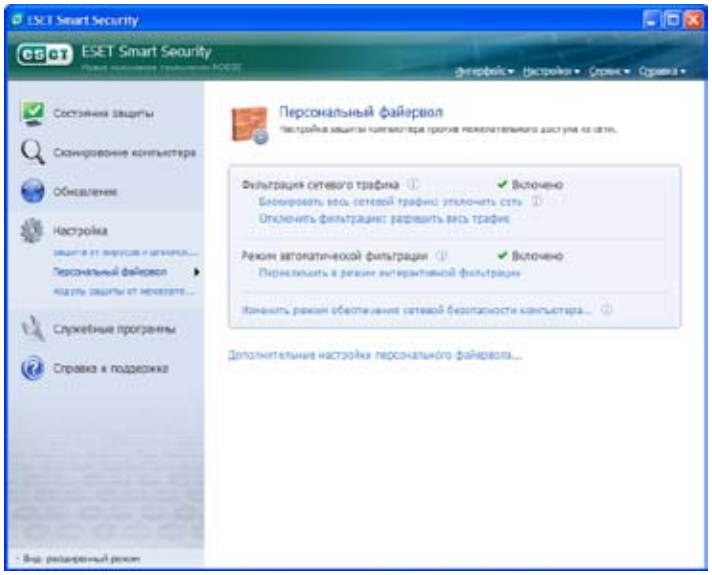
Все прочие, не указанные, подключения блокируются персональным файерволом.



4.2.2 Блокирование всего трафика: отключение сети

Единственным средством, позволяющим полностью блокировать весь сетевой трафик, является опция **Блокировать весь трафик: отключить сеть** (Block all network traffic: disconnect network). При ее использовании все исходящие соединения будут блокироваться персональным файерволом без вывода предупреждений. Эту опцию рекомендуется использовать только в случае подозрения о наличии серьезного риска для безопасности, требующего отключения системы от сети.

4.2.3 Отключение фильтрации: разрешение всего трафика

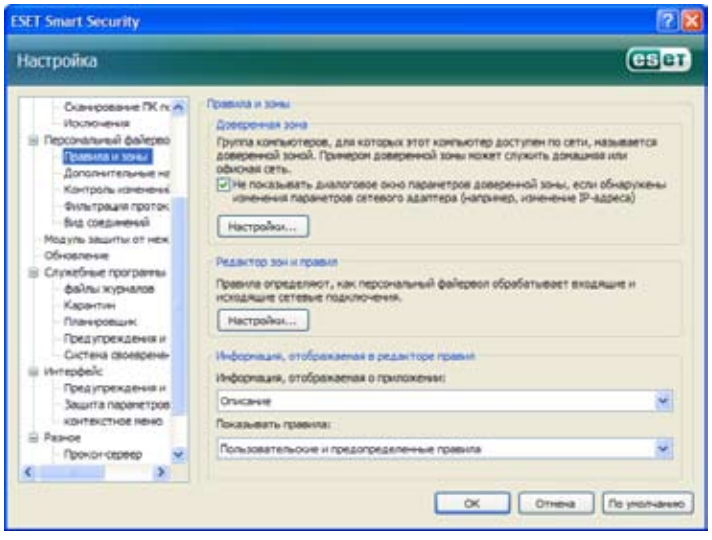


Опция **Отключить фильтрацию: разрешить весь трафик** (Disable filtering: allow all traffic) представляет собой обратную настройку по сравнению с упомянутой выше полной блокировкой всех соединений. При выборе этой опции все параметры фильтрации персонального файервола отключаются и разрешаются все входящие и исходящие соединения. С точки зрения сетевых подключений это дает такой же эффект, как если бы файервол вовсе не использовался.

4.2.4 Настройка и использование правил

Правила представляют собой набор условий, используемых для осмысленного тестирования всех сетевых подключений, и всех действий, заданных для этих условий. Для персонального файервола можно определить, какие действия будут выполняться при создании подключения, описанного правилом.

Чтобы настроить правила фильтрации, выберите пункт меню **Расширенная настройка** (F5) - **Персональный файервол** - **Правила и зоны** (Advanced setup - Personal firewall - Rules and zones). Чтобы открыть текущие настройки, щелкните **Настройка**... (Setup...) в разделе **Изменение зон и правил** (Zone and rule editor). Если для персонального файервола включен автоматический режим фильтрации, эти параметры будут недоступны.



В окне **Настройка зон и правил** (Zone and rule setup) на разных вкладках отображается обзор зон и правил. Окно разделено на две части. В верхней части кратко перечислены все правила. В нижней части выводятся подробные сведения о правиле, выбранном в верхней части. В самом низу расположены кнопки **Создать** (New), **Изменить** (Edit) и **Удалить** (Delete), позволяющие пользователю настраивать правила.

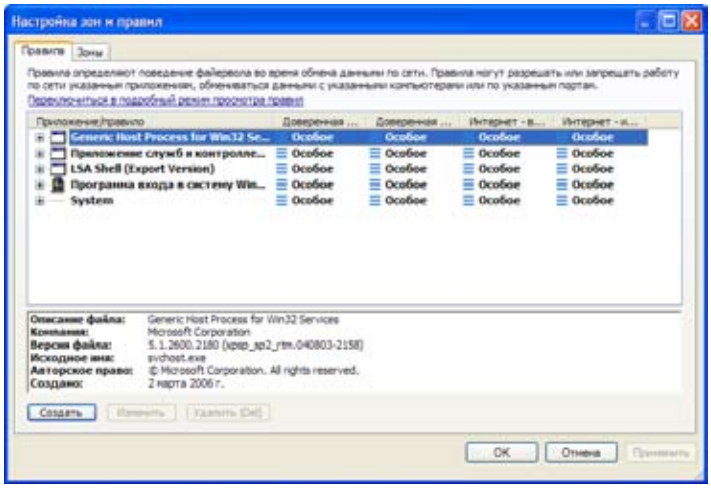
Если говорить о направлении соединений, то все подключения можно разделить на входящие и исходящие. Входящие подключения происходят по инициативе удаленного компьютера, пытающегося установить соединение с локальной системой. Исходящие подключения направлены в обратную сторону – от локального компьютера к удаленному.

При обнаружении нового неизвестного подключения необходимо с осмотрительностью решить, следует ли его разрешать или запрещать. Происходящие без запроса, незащищенные или полностью неизвестные подключения представляют собой риск для безопасности системы. При установлении такого соединения рекомендуется обратить особое внимание на его удаленную сторону и то приложение, которое пытается подключиться к компьютеру. Многие проникновения имеют целью получение и пересылку частных данных или загрузку вредоносных приложений на узловые рабочие станции. Персональный файервол позволяет пользователям обнаруживать и запрещать подобные подключения.

4.2.4.1 Создание новых правил

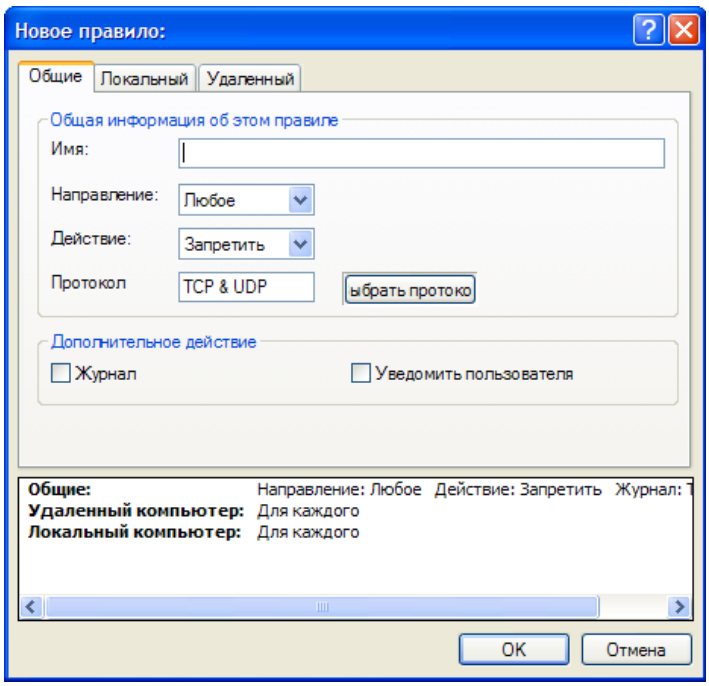
При установке нового приложения, имеющего доступ к сети, или при изменении существующего подключения (удаленной стороны, номера порта и т.д.) необходимо создать новое правило.

Чтобы добавить новое правило, выберите вкладку **Правила** (Rules). Затем нажмите кнопку **Создать** (New) в окне настройки зон и правил. Откроется новое диалоговое окно для определения создаваемого правила. Верхняя часть этого окна содержит три вкладки:



- **Общие сведения** (General). Здесь указываются имя правила, направление подключения, действие и протокол. Направление можно указать входящее (In), исходящее (Out) или любое (Both). Действие подразумевает разрешение или запрет данного подключения.
- **Локальная сторона** (Local). Здесь выводятся сведения о локальной стороне подключения, в том числе номер порта или диапазон таких номеров и имя подключающегося приложения.
- **Удаленная сторона** (Remote). Эта вкладка содержит сведения об удаленном порте или диапазоне портов. Пользователь также может задать здесь список удаленных IP-адресов или зон для данного правила.

Хорошим примером добавления нового правила является разрешение интернет-браузеру доступа к сети. Для этого необходимо выполнить следующие действия:



- На вкладке **Общие сведения** (General) разрешите входящие подключения по протоколам TCP и UDP.
- На вкладке **Локальная сторона** (Local) добавьте процесс, соответствующий используемому приложению браузера (например, iexplore.exe для Internet Explorer).
- На вкладке **Удаленная сторона** (Remote) добавьте номер порта 80 (только если необходимо включить стандартные WWW-службы).

4.2.4.2 Изменение правил

Чтобы изменить существующее правило, нажмите кнопку **Изменить** (Edit). Изменять можно все упомянутые выше параметры, описанные в разделе «Создание новых правил»).

Изменение правил необходимо при изменении любых отслеживаемых параметров. Иначе правило не будет соответствовать условиям, и заданное действие не сможет применяться. В результате данное подключение может быть отклонено, что приведет к проблемам функционирования того приложения, о котором идет речь. Примером может послужить изменение сетевого адреса или номера порта удаленной стороны.

4.2.5 Настройка зон

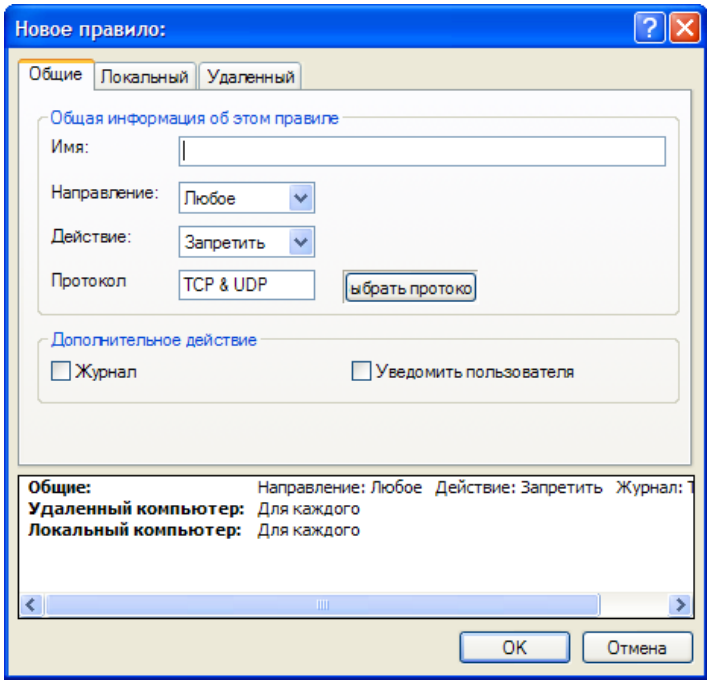
Зона – это совокупность сетевых адресов, создающих одну логическую группу. Для каждого адреса в данной группе назначаются одни и те же правила, централизованно определенные для группы в целом. Примером такой группы могут быть надежные адреса. В зону «Надежные» (Trusted) включается группа сетевых адресов, которым пользователь полностью доверяет, и они в любом случае не будут блокироваться персональным файерволом.

Зоны можно настраивать с помощью соответствующей вкладки окна настройки зон и правил, нажав кнопку Создать (New). В открывшемся окне введите имя зоны, ее описание и список входящих в нее сетевых адресов.

4.2.6 Установка подключения – обнаружение

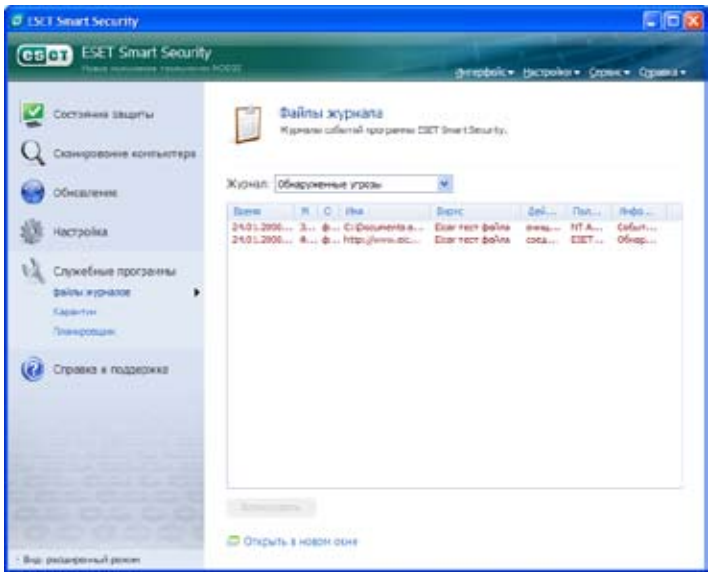
Персональный файерволл обнаруживает любое устанавливаемое сетевое подключение. Текущий режим файервола (интерактивный, автоматический или на основе политик) определяет, какие действия будут выполняться для нового правила. В автоматическом режиме или режиме на основе политик выполняются предопределенные действия без вмешательства пользователя.

В интерактивном режиме отображается информационное окно с отчетом об обнаружении нового сетевого подключения, дополненным подробной информацией об этом подключении. Пользователь может разрешить или отменить (заблокировать) это подключение. Если в диалоговом окне одно и то же подключение разрешается неоднократно, для него рекомендуется создать новое правило. Для этого выберите параметр **Сохранить действие (создать правило)** (Remember action (create rule)) и сохраните действие в виде нового правила для персонального файервола. В будущем при обнаружении этого подключения файервол применит существующее правило.



При создании новых правил необходимо соблюдать осторожность и разрешать только безопасные подключения. В случаях, когда разрешены все подключения, персональному файервол не удается выполнить свои задачи. Важные параметры подключений:

- **Удаленная сторона** (Remote side): должно быть разрешено подключение только к доверенным и известным адресам;
- **Локальное приложение** (Local application): не рекомендуется разрешать подключение к неизвестным приложениям и процессам;
- **Номер порта** (Port number): как правило, обмен данными через общие порты (например, через используемый веб-серверами порт 80) безопасен.



Для распространения программ с несанкционированным проникновением на компьютеры часто используются интернет и скрытые подключения, позволяющие этим программам инфицировать удаленные системы. Если правила настроены правильно, персональный файервол становится практичным средством для защиты от множества вредоносных программных атак.

4.2.7 Журналы

Все значительные события персональный файервол ESET NOD32 Smart Security сохраняет в файл журнала, просмотреть который можно непосредственно из главного меню. Выберите пункты меню **Инструменты** > **Файлы журналов** (Tools > Log files), а затем в раскрывающемся меню **Журнал** (Log) откройте **Журнал персонального файервола ESET** (ESET Personal firewall log).

Файлы журнала представляют собой важный инструмент по обнаружению ошибок в системе и вторжений, и заслуживают должного внимания. В журналах персонального файервола ESET содержатся следующие данные:

- дата и время события;
- имя события;
- сетевой адрес источника и целевой сетевой адрес;
- сетевой протокол обмена данными;
- примененное правило или имя червя (если определено);
- задействованное приложение.

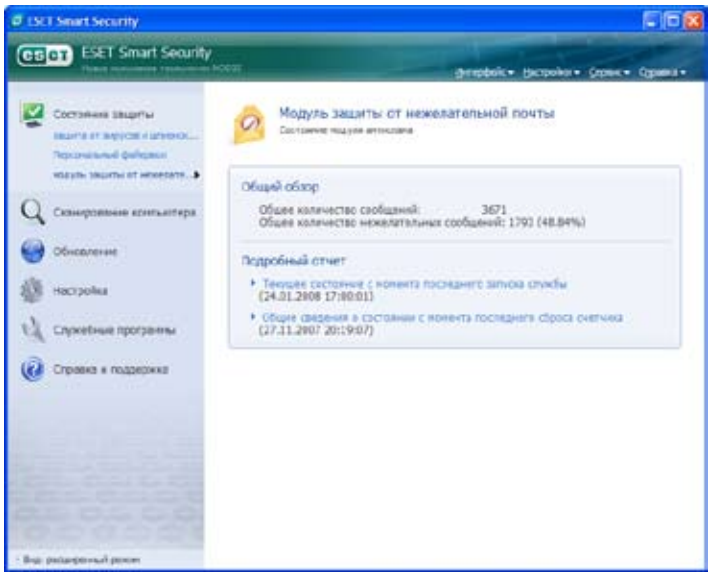
Тщательный анализ этих данных позволяет обнаружить попытки несанкционированного раскрытия системной безопасности. На потенциальные риски, связанные с нарушением безопасности, указывают многие другие факторы, позволяющие пользователям минимизировать воздействие этих рисков: слишком частые подключения с неизвестных адресов, многократные попытки установления подключения, обмен данными с неизвестными приложениями или необычные номера используемых портов.

4.3 Защита от спама

В настоящее время получение незапрашиваемых электронных сообщений – спама – считается одной из самых серьезных проблем электронного обмена данными. Спам составляет до 80% всех сообщений, передаваемых по электронной почте. Защита от спама служит для решения этой проблемы. Благодаря сочетанию нескольких очень эффективных принципов модуль защиты от спама обеспечивает отличную фильтрацию.

Одним из важных правил в обнаружении спама является возможность распознавания незатребованных электронных сообщений на основе предварительно определенных доверенных и нежелательных адресов («белый список» и «черный список»). В «белый список» автоматически заносятся все адреса из почтового клиента, а также адреса, отмеченные пользователем как безопасные.

Основной метод обнаружения спама заключается в просмотре свойств сообщений электронной почты. Полученные сообщения проверяются на соответствие основным условиям защиты от спама (анализируются определения сообщений, применяются статистические правила, алгоритмы распознавания и другие уникальные методы). Результирующее значение индекса определяет принадлежность этого сообщения к спаму.



При фильтрации применяется и фильтр Бейеса. Отмечая сообщения как спам или снимая такую отметку, пользователь создает базу данных, в которой содержатся слова, используемые в каждой из этих категорий. Чем больше эта база данных, тем точнее полученный результат.

Сочетание описанных выше методов обеспечивает высокий уровень обнаружения спама.

Защита от спама в ESET NOD32 Smart Security реализована для приложений Microsoft Outlook, Outlook Express и Windows Mail.

4.3.1 Самообучающийся механизм защиты от спама

Самообучающийся механизм защиты от спама связан с уже упомянутым фильтром Байеса. Значимость отдельных слов изменяется в процессе «изучения» того, как отдельные сообщения отмечаются как спам или не спам. Таким образом, чем больше сообщений было классифицировано (отмечено как спам или не спам), тем точнее результат применения фильтра Байеса.

Добавление известных адресов в «белый список» позволяет исключить из фильтрации сообщения, отправленные с этих адресов.

4.3.1.1 Добавление адресов в «белый список»

Адреса электронной почты лиц, с которыми пользователь часто обменивается сообщениями, можно добавить в список «безопасных» адресов (так называемый «белый список»). Таким образом можно предотвратить попадание писем, отправленные с этих адресов, в категорию «спам». Чтобы добавить в «белый список» новый адрес, щелкните этот адрес(?) электронной почты правой кнопкой мыши и в контекстном меню, в пункте ESET NOD32 Smart Security, выберите команду **Добавить в белый список** (Add to Whitelist) либо нажмите кнопку **Доверенный адрес** (Trusted address) на панели инструментов модуля ESET NOD32 Smart Security Antispam в верхней части почтового клиента.

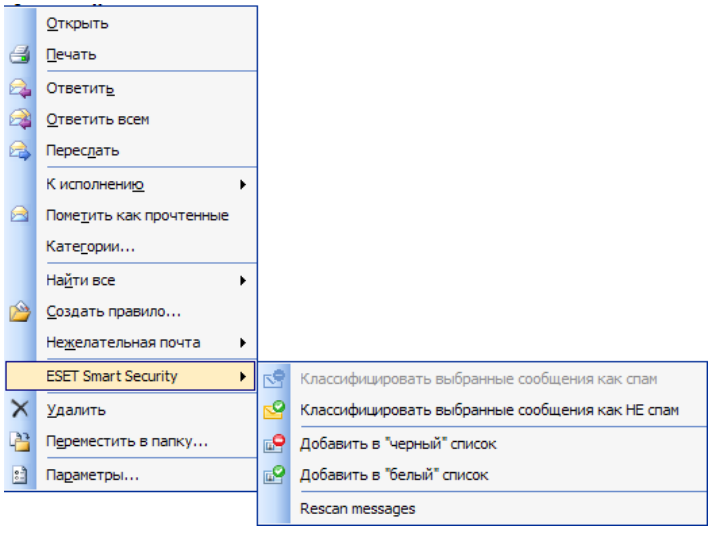
Аналогичным образом можно поступить с нежелательными адресами. Если какой-либо адрес электронной почты входит в «черный список», сообщения электронной почты, отправленные с этого адреса, будут классифицированы как спам.

4.3.1.2 Пометка сообщений как спам

Любое сообщение, просматриваемое в почтовом клиенте, может быть отмечено как спам. Для этого вызовите контекстное меню (правой кнопкой мыши) и выберите команды **ESET NOD32 Smart Security** > **Перенести выделенные сообщения в категорию спам** (ESET NOD32 Smart Security > Reclassify selected messages as spam) либо в почтовом клиенте нажмите кнопку **Спам** (Spam) на панели инструментов модуля **ESET NOD32 Smart Security Antispam**.

Переклассифицированные сообщения автоматически переносятся в папку **СПАМ** (SPAM), но адрес электронной почты отправителя в «черный список» не добавляется. Аналогичным образом сообщения можно классифицировать как «не спам». Если сообщения из папки

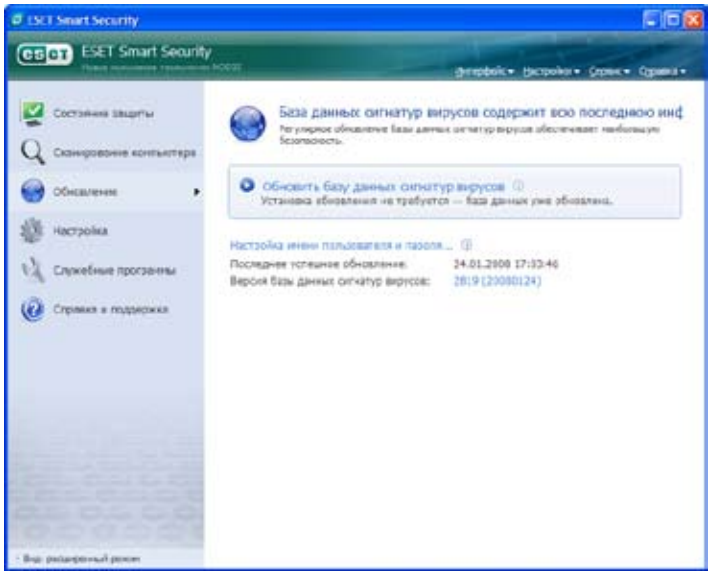
Нежелательная почта (Junk E-mail) классифицированы как «не спам», они перемещаются в исходную папку. Снятие с сообщений отметки «спам» не означает автоматическое добавление адреса отправителя в «белый список»..



4.4 Обновление версии программы

Регулярное обновление системы – это основное условие достижения максимального уровня защиты, обеспечиваемой ESET NOD32 Smart Security. Модуль **Обновления** (Update) поддерживает актуальное состояние программы. Это осуществляется двумя способами: обновлением базы данных вирусных сигнатур и обновлением всех компонентов системы.

Сведения о текущем состоянии обновления, включая данные о текущей версии базы данных вирусных сигнатур и необходимости обновления, можно найти, выбрав соответствующий пункт меню (Update). Кроме того, предусмотрены возможность немедленного запуска процесса обновления – при помощи команды **Обновить базу данных вирусных сигнатур** (Update virus signature database), – и основные параметры настройки обновления, такие как имя пользователя и пароль для доступа к серверам обновлений ESET.

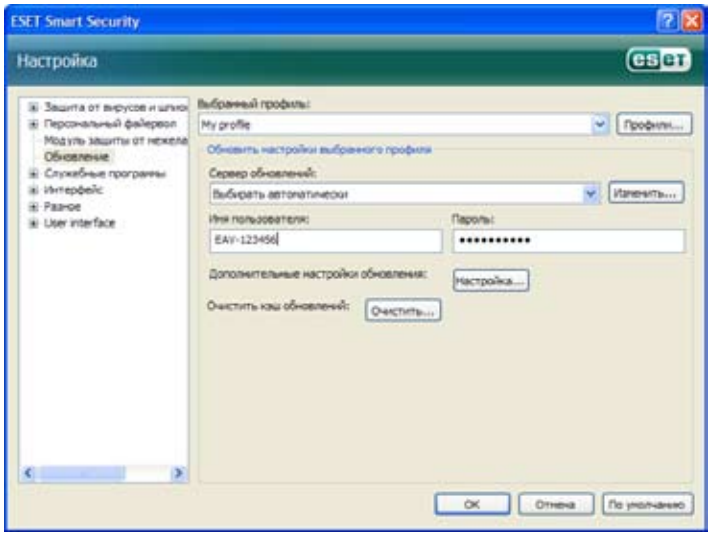


В информационном окне содержатся сведения о дате и времени последнего успешного обновления, номер базы данных вирусных сигнатур. Цифровое обозначение представляет собой действующую ссылку на веб-сайт ESET с перечислением всех сигнатур, добавленных в рамках данного обновления.

Примечание. Имя пользователя и пароль сообщаются компанией ESET после приобретения пакета ESET NOD32 Smart Security.

4.4.1 Настройка обновлений

В разделе о настройке обновлений указываются данные об источнике обновлений: серверы обновлений и учетные данные для доступа к этим серверам. По умолчанию в поле **Сервер обновления:** (Update server:) установлено значение **Выбрать автоматически** (Choose automatically). Это значение гарантирует автоматическую загрузку файлов обновления с сервера ESET с наименьшей нагрузкой на сетевой трафик. Параметры настройки обновлений находятся в разделе **Обновления** (Update) в дереве расширенной настройки, вызываемом клавишей F5.



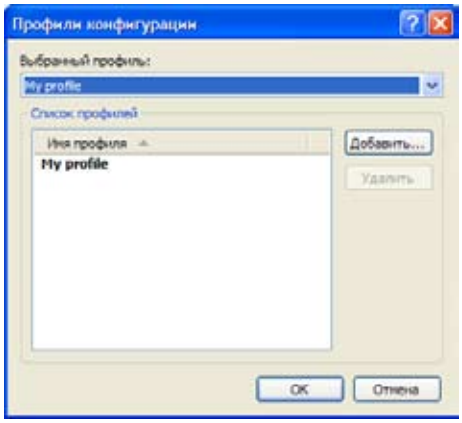
Список имеющихся в данный момент серверов обновления можно просмотреть в раскрывающемся меню **Сервер обновлений** (Update server). Чтобы добавить новый сервер обновления, в разделе **Обновить настройки выбранного профиля** (Update settings for selected profile) нажмите кнопку **Изменить**... (Edit...), а затем – кнопку **Добавить** (Add).

Для проверки подлинности серверам обновлений передаются **Имя пользователя** (User name) и **Пароль** (Password), сформированные и отправленные пользователю фирмой ESET после приобретения лицензии на продукт.

4.4.1.1 Профили обновления

Для различных конфигураций обновлений можно создать пользовательские профили обновлений, которые затем могут быть использованы для тех или иных задач обновления. Создание разных профилей обновлений особенно целесообразно для пользователей, передвижения которых приводят к регулярному изменению свойств интернет-подключения. Изменение задачи обновлений позволяет пользователям с частыми передвижениями указать альтернативный профиль, который должен использоваться для обновлений в случае невозможности обновления программы при помощи конфигурации, настроенной в разделе **Мой профиль** (My Profile).

В раскрывающемся меню **Выбранный профиль** (Selected profile) отображается профиль, выбранный в данный момент. По умолчанию в этой записи указан **Мой профиль** (My profile). Чтобы создать новый профиль, нажмите кнопку **Профили**... (Profiles...), а затем – кнопку **Добавить**... (Add...) и введите собственное **Имя профиля** (Profile name). Создавая новый профиль, вы можете скопировать настройки существующего профиля, выделив его в раскрывающемся меню **Скопировать настройки профиля:** (Copy settings from profile:).



Во время настройки профиля можно указать сервер обновлений, к которому программа будет подключаться для загрузки обновлений; вы можете использовать любой сервер из списка доступных адресов либо добавить новый. Доступ к списку существующих серверов обновлений осуществляется в раскрывающемся меню **Сервер обновлений:** (Update server:). Чтобы добавить новый сервер обновления, в разделе **Обновить настройки выбранного профиля** (Update settings for selected profile) нажмите кнопку **Изменить**... (Edit...), а затем – кнопку **Добавить** (Add).

4.4.1.2 Расширенная настройка обновлений

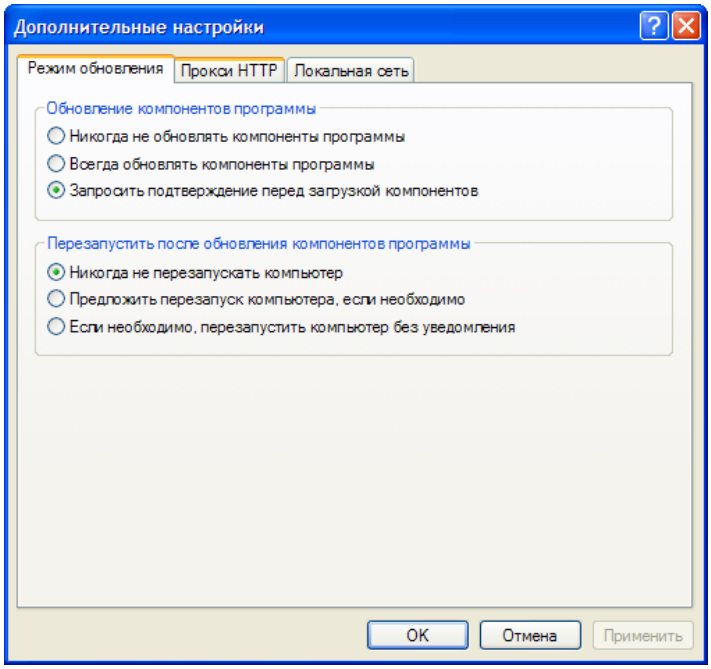
Чтобы просмотреть раздел **Расширенная настройка обновлений** (Advanced update setup), нажмите кнопку **Настроить**... (Setup...). Расширенная настройка обновлений включает в себя конфигурацию следующих элементов: **Режим обновления** (Update Mode), **Прокси-сервер HTTP** (HTTP Proxy), **Локальная сеть** (LAN) и **Зеркало** (Mirror).

4.4.1.2.1 Режим обновлений

На вкладке **Режим обновления** (Update mode) представлены параметры, имеющие отношение к обновлениям программных компонентов.

Раздел **Обновления компонентов программы** (Program component update) содержит три параметра:

- **Никогда не обновлять компоненты программы** (Never update program components)
- **Всегда обновлять компоненты программы** (Always update program components)
- **Запросить подтверждение перед загрузкой компонентов** (Ask before downloading program components)



Если выбран параметр **Никогда не обновлять компоненты программы** (Never update program components), то после выпуска компанией ESET нового обновления какого-либо программного компонента оно не будет загружено, и на указанной рабочей станции не будет произведено обновление этого программного компонента. Параметр **Всегда обновлять компоненты программы** (Always update program components) означает, что обновление программных компонентов осуществляется каждый раз, когда новые обновления доступны на серверах обновлений ESET, и программные компоненты обновляются до загруженной версии.

Выбор третьего параметра, **Запросить подтверждение перед загрузкой компонентов** (Ask before downloading program components), приводит к тому, что при наличии обновлений программных компонентов программа запрашивает подтверждение пользователя на их загрузку. В этом случае в диалоговом окне отображаются сведения о доступных обновлениях программных компонентов и предлагается возможность подтвердить или отклонить их. После подтверждения загружаются обновления, и новые программные компоненты устанавливаются на компьютер.

По умолчанию для обновления программных компонентов установлен параметр **Запросить подтверждение перед загрузкой компонентов** (Ask before downloading program components).

Чтобы после установки обновлений программных компонентов обеспечить полную функциональность всех модулей, необходимо перезагрузить систему. В разделе **Перезагрузка после обновления компонентов программы** (Restart after program component upgrade) пользователю предлагается на выбор три возможности:

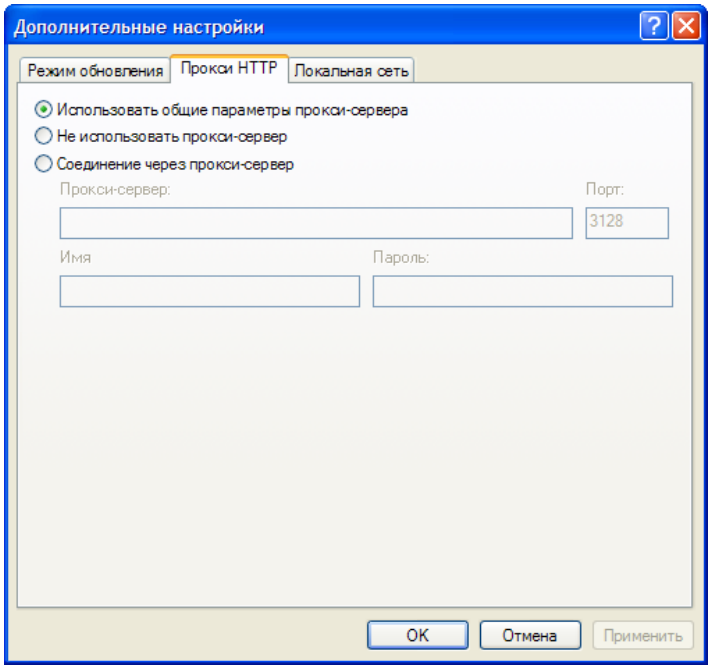
- **Никогда не перезапускать компьютер** (Never restart computer)
- **Предложить перезапуск компьютера, если необходимо** (Offer computer restart if necessary)
- **Если необходимо, перезапустить компьютер без уведомления** (If necessary, restart computer without notifying)

По умолчанию для перезагрузки компьютера установлен параметр- **Предложить перезапуск компьютера, если необходимо** (Offer computer restart if necessary). Выбор наиболее подходящих параметров для обновлений программных компонентов на вкладке **Режим обновления** (Update mode) индивидуален для каждой рабочей станции, поскольку эти настройки применяются именно на рабочих станциях. Помните о различиях между рабочими станциями и серверами: так, например, автоматическая перезагрузка сервера после обновления версии программы может привести к серьезным повреждениям.

4.4.1.2.2 Прокси-сервер

Чтобы получить доступ к параметрам настройки прокси-сервера для определенных профилей обновления: в дереве **расширенной настройки** (вызывается нажатием клавиши F5) выберите узел **Обновления** (Update) и справа от пункта **Расширенная настройка обновлений** (Advanced update setup) нажмите кнопку **Настроить**... (Setup...). Перейдите на вкладку **HTTP-прокси** (HTTP Proxy) и выберите один из следующих трех параметров:

- **Использовать общие параметры прокси-сервера** (Use global proxy server settings)
- **Не использовать прокси-сервер** (Do not use proxy server)
- **Соединение через прокси-сервер** (Connection through a proxy server, подключение определяется свойствами подключения)



Выбор параметра **Использовать общие параметры прокси-сервера** (Use global proxy server settings) приводит к использованию параметров конфигурации прокси-сервера, установленных в дереве расширенной настройки в разделе **Разное** > **Прокси-сервер** (Miscellaneous > Proxy server).

Параметр **Не использовать прокси-сервер** (Do not use proxy server) явным образом указывает на то, что обновление ESET NOD32 Smart Security должно осуществляться без использования прокси-серверов.

Параметр **Соединение через прокси-сервер** (Connection through a proxy server) следует выбрать, если для обновления ESET NOD32 Smart Security необходимо использовать прокси-сервер, отличный от указанного в глобальных настройках (**Разное** > **Прокси-сервер** (Miscellaneous > Proxy server)). В этом случае нужно будет указать следующие настройки: **адрес прокси-сервера** (Proxy server), **порт связи** (Port), а также, при необходимости, **имя пользователя** (User name) и **пароль** (Password) для доступа к прокси-серверу.

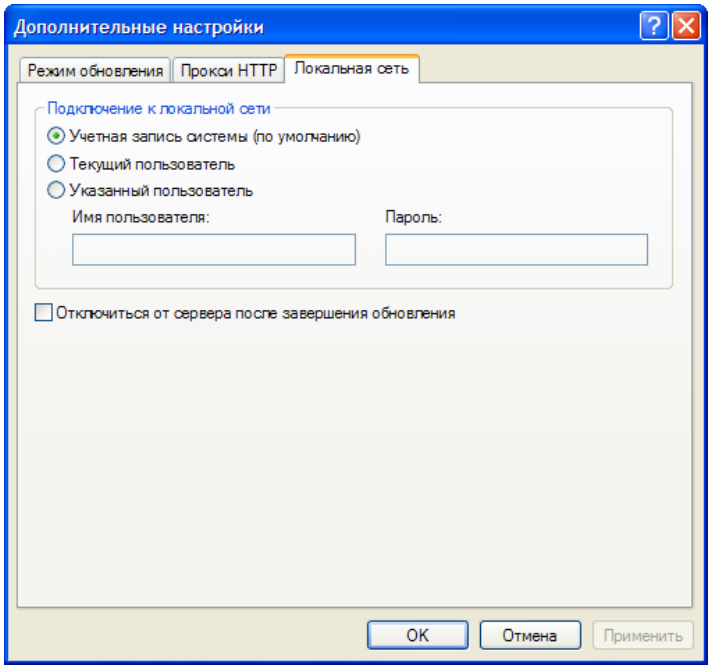
Этот вариант следует выбрать и в том случае, если настройки прокси-сервера не были заданы глобально, но система ESET NOD32 Smart Security подключается к прокси-серверу для загрузки обновлений.

По умолчанию для прокси-сервера выбран параметр **Использовать общие параметры прокси-сервера** (Use global proxy server settings).

4.4.1.2.3 Подключение к локальной сети (LAN)

Если для обновления используется локальный сервер с операционной системой на базе NT, по умолчанию для каждого сетевого подключения требуется проверка подлинности. В большинстве случаев локальные системные учетные записи не обладают необходимыми полномочиями для доступа к папке **Mirror** (в которой содержатся копии файлов обновлений). В этом случае необходимо ввести имя пользователя и пароль в разделе настройки обновлений либо указать существующую учетную запись, используемую программой для входа на сервер обновлений (зеркало).

Чтобы настроить такую учетную запись, перейдите на вкладку **Локальная сеть** (LAN). В разделе **Подключение к локальной сети** (Connect to LAN as) предлагаются варианты **Учетная запись системы (по умолчанию)** (System account (default)), **Текущий пользователь** (Current user) и **Указанный пользователь** (Specified user).



Чтобы использовать для проверки подлинности системную учетную запись, выберите параметр **Учетная запись системы** (System account). Как правило, если в разделе основных настроек обновлений никакие учетные данные не указаны, проверка подлинности не выполняется.

Чтобы программа проверила подлинность самой себя при помощи учетной записи пользователя, который в данный момент зарегистрирован в системе, выберите пункт **Текущий пользователь** (Current user). Недостаток этого решения заключается в невозможности программы подключиться к серверу обновлений, если в ней не находятся никакие пользователи.

Выберите пункт **Указанный пользователь** (Specified user), если для проверки подлинности программе будет передана учетная запись определенного пользователя.

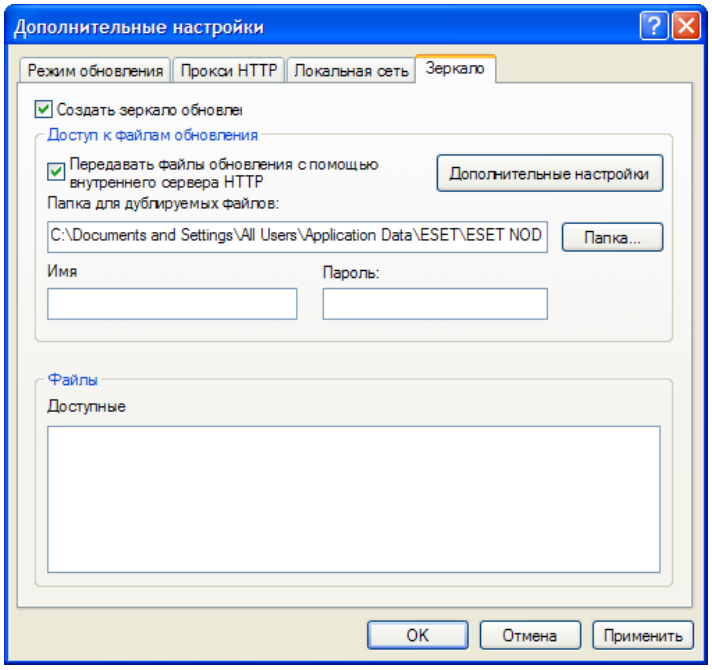
По умолчанию для подключения к локальной сети выбран пункт **Учетная запись системы** (System account).

Внимание!

При выбранных параметрах **Текущий пользователь** (Current user) или **Указанный пользователей** (Specified user) изменение пользователя программы на требуемого пользователя может привести к ошибке. Поэтому учетные данные для подключения к локальной сети рекомендуется указывать в разделе основных настроек обновлений. В этом разделе настройки обновлений указываются следующие учетные данные: имя_домена\пользователь (в случае с рабочей группой укажите имя_рабочей_группы\имя) и пароль пользователя. При загрузке обновлений с HTTP-версии локального сервера проверка подлинности не требуется.

4.4.1.2.4 Создание копий обновлений – зеркало

Версия ESET NOD32 Smart Security для корпоративных клиентов позволяет пользователям создавать копии файлов обновлений, которые могут быть использованы для обновления других рабочих станций, подключенных в сеть. Обновление клиентских рабочих станций с зеркала позволяет оптимизировать сетевую нагрузку и сохранить пропускную способность интернет-подключения.



Параметры конфигурации локального сервера-зеркала доступны в разделе **Расширенная настройка обновлений** (Advanced update setup) (клавишей F5 вызовите дерево расширенной настройки, выберите пункт **Обновления** (Update), нажмите кнопку **Настроить**... (Setup...) рядом с записью **Расширенная настройка обновлений**: (Advanced update setup:) и перейдите на вкладку **Зеркало** (Mirror)).

Первым шагом в настройке зеркала является установка флажка **Создать зеркало обновлений** (Create update mirror). Выбор этой команды активирует другие параметры конфигурации зеркала (например, способ доступа к файлам обновления и путь к зеркальным отображениям файлов).

Методы активации зеркала подробно описаны в следующей главе, «Способы доступа к зеркалу» (Variants of accessing the Mirror). Пока же следует запомнить два основных способа доступа к зеркалу: папка с файлами обновлений может быть представлена как зеркало в виде сетевой папки совместного доступа либо как зеркало в виде HTTP-сервера.

Папка, выделенная для хранения файлов обновлений в зеркальном отображении, определяется в разделе **Папка для дублируемых файлов** (Folder to store mirrored files). Нажмите кнопку **Папка**... (Folder...), чтобы найти необходимую папку на локальном компьютере или сетевую папку совместного доступа.

Если для указанной папки требуется проверка подлинности, введите учетные данные в полях **Имя пользователя** (User name) и **Пароль** (Password). **Имя пользователя** (User name) и **Пароль** (Password) должны быть указаны в формате «Домен/пользователь» или «Рабочая группа/пользователь». Не забывайте указывать соответствующие пароли!

При определении подробной конфигурации зеркала можно также указать языковые версии, для которых необходимо загружать копии обновлений. Настройка языковых версий выполняется в разделе **Файлы** – **Доступные версии**: (Files – Available versions).

4.4.1.2.4.1 Загрузка обновлений с зеркала

Зеркало может быть настроено двумя основными способами: папка с файлами обновлений может быть представлена как зеркало в виде сетевой папки совместного доступа либо как зеркало в виде HTTP-сервера.

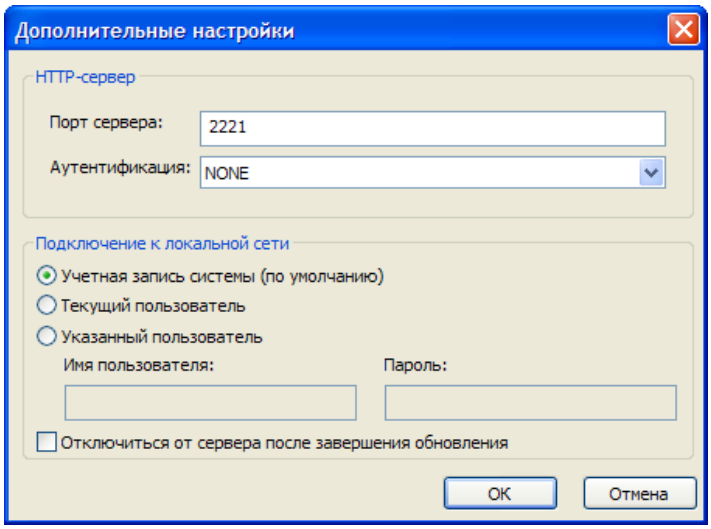
Доступ к зеркалу при помощи встроенного HTTP-сервера

Эта настройка задается по умолчанию и указана в конфигурации программы по-умолчанию. Чтобы получить доступ к зеркалу при помощи HTTP-сервера, в разделе **Расширенная настройка обновлений** (Advance update setup) перейдите на вкладку **Зеркало** (Mirror) и установите флаг **Создать зеркало обновлений** (Create update mirror).

В разделе **Дополнительные настройка** (Advanced setup) вкладки **Зеркало** (Mirror) можно указать прослушиваемый HTTP-сервером **Порт сервера** (Server Port) и в поле **Аутентификация** (Authentication) задать необходимый для этого HTTP-сервера тип проверки. По умолчанию указан порт сервера 2221. Параметр **Аутентификация** (Authentication) определяет метод проверки, используемый для доступа к файлам обновлений. Доступны следующие параметры: **Нет** (NONE), **Основная** (Basic) и **NTLM** (NTLM). Если выбрана **Основная** (Basic) проверка подлинности, то при основной проверке имени пользователя и пароля будет применено кодирование по алгоритму base64. Параметр NTLM обеспечивает кодирование безопасным методом. Для проверки подлинности при этом используется пользователь, созданный на той рабочей станции, на которой хранятся файлы обновлений для совместного доступа. По умолчанию выбран параметр **Нет** (NONE), предоставляющий доступ к файлам обновления без необходимости проверки подлинности.

Внимание!

Чтобы получить доступ к файлам обновления через HTTP-сервер, папка зеркала должна находиться на том же компьютере, что и использованный для ее создания экземпляр системы ESET NOD32 Smart Security.



По окончании настройки зеркала на рабочих станциях необходимо добавить новый сервер обновления в формате http://IP_адрес_сервера:2221. Для этого выполните следующие действия:

- Откройте раздел **Расширенная настройка ESET NOD32 Smart Security** (ESET NOD32 Smart Security Advanced Setup) и перейдите в раздел **Обновлений** (Update).
- Справа от раскрывающегося меню **Сервер обновлений** (Update server) нажмите кнопку **Изменить...** (Edit...) и добавьте новый сервер, указав его в следующем формате: http://IP_адрес_сервера:2221.
- Выберите в списке серверов обновлений этот только что добавленный сервер.

Доступ к серверу через системные папки совместного доступа

Сначала папку совместного доступа необходимо создать на локальном или сетевом устройстве. При создании такой папки для зеркала пользователю, сохраняющему файлы обновления, необходимо предоставить право записи, а всем пользователям, обновляющим системы ESET NOD32 Smart Security при помощи папки зеркала, – право чтения.

Затем настройте доступ к зеркалу в разделе **Расширенная настройка обновлений** (Advanced update setup) на вкладке **Зеркало** (Mirror), сняв флажок **Предоставить файлы обновлений через внутренний HTTP-сервер** (Provide update files via internal HTTP server). В пакете установки программы этот флажок установлен по умолчанию.

Если папка совместного доступа находится на другом компьютере в сети, потребуется указать учетные данные для доступа к этому другому компьютеру. Чтобы указать учетные данные, вызовите **расширенную настройку ESET NOD32 Smart Security** (нажатием клавиши F5) и откройте раздел **Обновления** (Update). Нажмите кнопку **Настроить**...

(Setup...) и перейдите на вкладку **Локальная сеть** (LAN). Настройка выполняется так же, как было описано в разделе «Подключение к локальной сети» (Connecting to LAN) для обновлений.

По завершении настройки зеркала на рабочих станциях нужно указать \\ПК\папка в качестве сервера обновлений. Для осуществления этой операции выполните следующие действия:

- откройте раздел **Расширенная настройка ESET NOD32 Smart Security** (ESET NOD32 Smart Security Advanced Setup) и выберите раздел **Обновления** (Update);
- рядом с полем для задания сервера обновлений нажмите кнопку **Изменить**... (Edit...) и добавьте новый сервер в формате \\ПК\ папка;
- выберите в списке серверов обновлений этот только что добавленный сервер.

Примечание. Во избежание неправильного функционирования путь к папке зеркала должен быть указан как путь UNC. Обновления, загруженные с подключенных сетевых дисков, могут не работать.

4.4.1.2.4.2 Решение проблем с обновлениями с зеркала

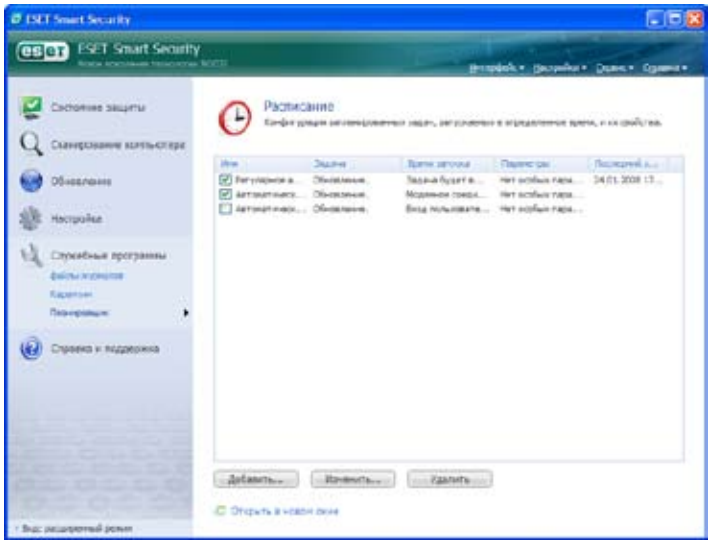
В зависимости от способа доступа к папке зеркала могут возникнуть различные типы проблем. В большинстве случаев проблемы, возникающие при обновлении с сервера-зеркала, вызваны следующими причинами: неверное определение параметров папки зеркала, неверные учетные данные для доступа к папке зеркала, неверная настройка на локальных рабочих станциях при попытке загрузить файлы обновлений с зеркала, либо сочетанием этих причин. В данном разделе приводится обзор проблем, наиболее часто возникающих при загрузке обновлений с зеркала:

- **ESET NOD32 Smart Security сообщает об ошибке подключения к северу зеркала** (ESET NOD32 Smart Security reports an error connecting to Mirror server): возможная причина заключается в неверном указании сервера обновлений (сетевого пути к папке зеркала), с которого локальные рабочие станции загружают обновления. Чтобы проверить эту папку, в **меню Windows Пуск** (Start) выберите команду **Выполнить** (Run), вставьте имя папки и нажмите кнопку **OK** (OK). Это должно привести к отображению содержимого папки;
- **Программе ESET NOD32 Smart Security необходимы имя пользователя и пароль** (ESET NOD32 Smart Security requires a user name and password): возможная причина заключается в неверном вводе учетных данных (имени пользователя и пароля) в разделе обновлений. Имя пользователя и пароль используются для предоставления доступа к серверу обновлений, с которого программа загружает свои обновления. Убедитесь, что учетные данные верны и указаны в правильном формате. Например, в формате Домен/Имя пользователя (Domain/User name) или Рабочая группа/Имя пользователя (Workgroup/User name), с указанием соответствующих паролей. Если доступ к серверу зеркала разрешен для пользователей группы «Everyone», это не означает предоставление доступа любому пользователю. Таким образом, даже если папка доступна группе пользователей «Everyone», в разделе настройки обновлений должны быть указаны имя пользователя и пароль;
- **ESET NOD32 Smart Security сообщает об ошибке подключения к серверу зеркала** (ESET NOD32 Smart Security reports an error connecting to the Mirror server): блокирована передача данных через порт, указанный для доступа к HTTP-версии зеркала.

4.4.2 Создание задач обновления

Обновления можно вызвать вручную, щелкнув ссылку **Обновить базу данных вирусных сигнатур** (Update virus signature database) в информационном окне, отображаемом при выборе раздела **Обновления** (Update) в главном меню.

Кроме того, загрузка обновлений может быть запущена как запланированная задача. Чтобы настроить запланированную задачу, выберите команды пункты меню **Инструменты** > **Планировщик** (Tools > Scheduler). По умолчанию в программе ESET NOD32 Smart Security активированы следующие задачи:



- **Регулярное автоматическое обновление** (Regular automatic update)
- **Автоматическое обновление после модемного подключения** (Automatic update after dial-up connection)
- **Автоматическое обновление после входа пользователя в систему** (Automatic update after user logon)

Каждую из названных выше задач можно изменить в соответствии с имеющимися требованиями. В дополнение к задачам обновления, предусмотренным по умолчанию, имеется возможность создания новых задач с пользовательской конфигурацией. Более подробные сведения о создании и настройке задач обновления см. в главе «Планировщик» (Scheduler).

4.5 Планировщик

Доступ к планировщику доступен в ESET NOD32 Smart Security при включенном расширенном режиме. **Планировщик** (Scheduler) находится в разделе **Инструменты** (Tools) главного меню ESET NOD32 Smart Security. Планировщик содержит сводный список всех запланированных задач и свойства их конфигурации (например, заданную дату, время и используемый профиль сканирования).

По умолчанию в разделе **Планировщик** (Scheduler) отображаются следующие задачи:

- **Регулярное автоматическое обновление** (Regular automatic update)
- **Автоматическое обновление после модемного подключения** (Automatic update after dial-up connection)
- **Автоматическое обновление после входа пользователя в систему** (Automatic update after user logon)
- **Автоматическая проверка файла запуска(?) после входа пользователя в систему** (Automatic startup file check after user logon)
- **Автоматическая проверка файла запуска(?) после успешного обновления базы данных вирусных сигнатур** (Automatic startup file check after successful update of the virus signature database)

Чтобы изменить конфигурацию имеющегося запланированного задания (предусмотренного по умолчанию или пользовательского), щелкните задачу правой кнопкой мыши и выберите команду **Изменить**... (Edit...) либо выберите задачу, которую необходимо изменить, и нажмите кнопку **Изменить**... (Edit...).

4.5.1 Цель планирования задач

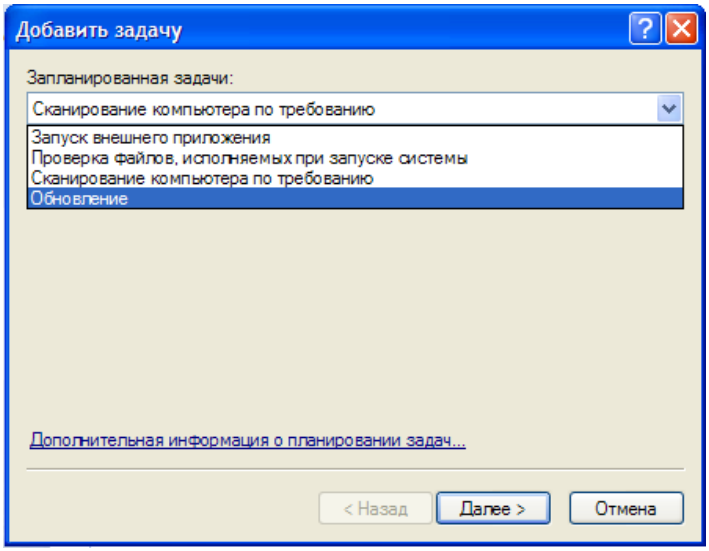
Планировщик управляет запланированными задачами с предопределенными свойствами и конфигурацией и запускает их. В конфигурации и свойствах содержатся сведения (такие как дата и время, а также определенные профили), используемые для выполнения задачи.

4.5.2 Создание новых задач

Чтобы создать в планировщике новую задачу, нажмите кнопку **Добавить**... (Add...) или щелкните правой кнопкой мыши и выберите команду **Добавить**... (Add...) в контекстном меню. Запланированные задачи подразделяются на четыре типа:

- **запуск внешнего приложения** (Run external application)
- **проверка файлов, исполняемых при запуске системы** (System startup file check)
- **сканирование компьютера по требованию** (On-demand computer scan)
- **обновление** (Update)

Поскольку задачи **Сканирование компьютера по требованию** (On-demand computer scan) и **Обновление** (Update) представляют собой наиболее часто запускаемые запланированные задачи, далее приводится объяснение добавления новой задачи обновления.



В раскрывающемся меню **Запланированная задача**: (Scheduled task:) выберите запись **Обновление** (Update). Нажмите кнопку **Далее** (Next) и в поле **Имя задачи:** (Task name:) введите имя задачи. Выберите периодичность выполнения задачи. Доступны следующие варианты: **Один раз** (Once), **Периодически** (Repeatedly), **Ежедневно** (Daily), **Еженедельно** (Weekly) и **По событию** (Event-triggered). В зависимости от выбранной периодичности будут предложены различные параметры обновлений. Затем определите действие на случай, если выполнение задачи в назначенное время будет невозможно или возможно не полностью. Доступны следующие три варианта:

- **отложить до следующего назначенного времени** (Wait until the next scheduled time)
- **выполнить задачу как можно быстрее** (Run task as soon as possible)
- **выполнить задачу немедленно, если время с момента последнего выполнения задачи превысило заданный интервал** (Run task immediately if the time since its last execution exceeds specified interval) (интервал можно задать тут же в поле с полосой прокрутки **Интервал задачи** (Task interval))

На следующем шаге будет отображено сводное окно со сведениями о текущей запланированной задаче; флажок **Выполнить задачу с указанными параметрами** (Run task with specific parameters) должен быть установлен автоматически. Нажмите кнопку **Готово** (Finish).

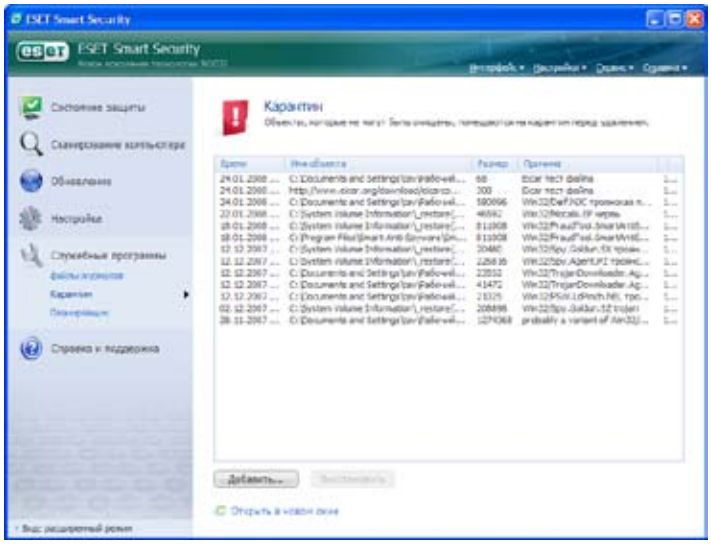
Появится диалоговое окно, позволяющее выбрать профили, используемые для данной запланированной задачи. Кроме основного, здесь можно указать альтернативный профиль, который должен применяться при невозможности выполнения задачи с использованием основного профиля. Подтвердите выбор, нажав кнопку **OK** (OK) в окне **Профили обновления** (Update profiles). Новая запланированная задача будет добавлена в список задач, запланированных в данный момент.

4.6 Карантин

Основная задача карантина – безопасное хранение зараженных файлов. Файлы помещаются в карантин, если невозможна их очистка, если невозможно их безопасное удаление или удаление рекомендованным образом или если они ошибочно были обнаружены программой ESET NOD32 Smart Security.

Пользователь может поместить в карантин любые файлы по своему усмотрению. Это целесообразно, когда поведение файла подозрительно, но он не был обнаружен сканером защиты от вирусов. Файлы, помещенные в карантин, можно отправить для исследования в вирусные лаборатории ESET.

Файлы, сохраненные в папке карантина, можно просмотреть в таблице, где также отображаются дата и время помещения в карантин, путь к исходному расположению зараженного файла, размер файла в байтах, причина (добавлен пользователем... (added by user...)) и число угроз (например, если это архивный файл с проникновением нескольких вирусов).



4.6.1 Помещение файлов в карантин

Программа автоматически помещает удаленные файлы в карантин (если эта функция не была отключена в окне-предупреждении). При необходимости любой подозрительный файл можно поместить в карантин вручную, нажав кнопку Добавить... (Add...). В этом случае исходный файл из исходного расположения не удаляется. Для этих целей также можно воспользоваться контекстным меню: щелкнуть окно карантина правой кнопкой мыши и выбрать команду Добавить... (Add...)

4.6.2 Восстановление из карантина

Помещенные на карантин файлы можно восстановить в их исходное местоположение. Для этого воспользуйтесь командой Восстановить (Restore) из контекстного меню файла (чтобы открыть его, щелкните файл в окне карантина правой кнопкой мыши).

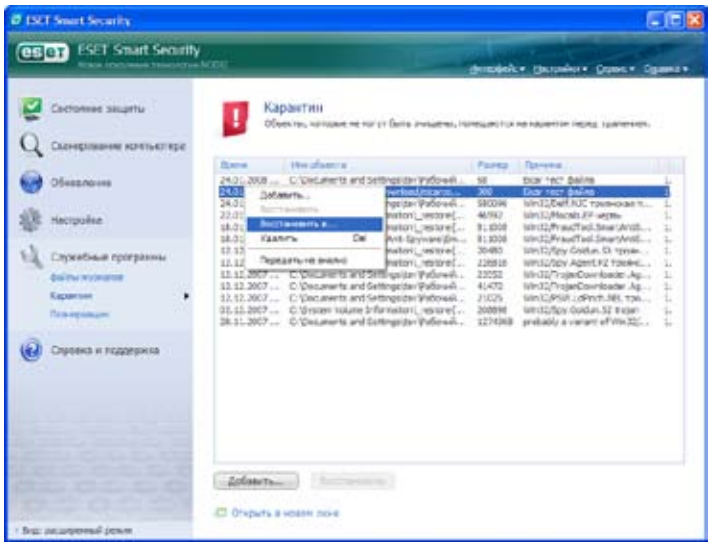
Кроме этого, контекстное меню содержит команду Восстановить в (Restore to), позволяющую восстановить файл в папку, отличную от той, из которой файл был удален.

Примечание. Если программа ошибочно поместила в карантин безвредный файл, после восстановления исключите его из сканирования и отправьте этот файл в службу технической поддержки ESET.

4.6.3 Отправка карантинного файла на изучение

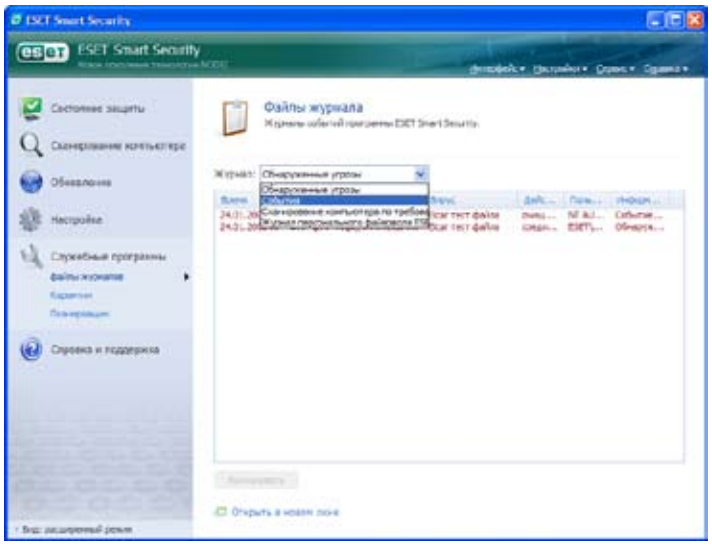
Если вы поместили в карантин подозрительный файл, не обнаруженный программой, либо если какой-либо файл был ошибочно определен как зараженный (например, в результате эвристического анализа программного кода) и помещен в карантин, отправьте этот файл в вирусную лабораторию ESET. Чтобы какой-либо помещенный в карантин файл отправить на рассмотрение, щелкните файл правой кнопкой мыши и выберите в контекстном меню команду **Отправить на анализ** (Submit for analysis).

4.7 Файлы журналов



Файлы журналов содержат сведения обо всех завершенных значительных программных событиях и предоставляют обзор обнаруженных угроз. Ведение журналов представляет собой основной инструмент для системного анализа, обнаружения угроз и решения проблем. Ведение журналов выполняется в фоновом режиме без взаимодействия с пользователем. Записываемые сведения зависят от текущих настроек словесного наполнения журнала. Текстовые сообщения и журналы можно просмотреть и заархивировать непосредственно в среде ESET NOD32 Smart Security.

Доступ к файлам журналов можно получить, выбрав в основном окне ESET NOD32 Smart Security пункты **Инструменты** > **Файлы журналов**



(Tools > Log files). В раскрывающемся списке **Журнал:** (Log:) в верхней части окна выберите необходимый тип журнала. Доступны следующие типы журналов:

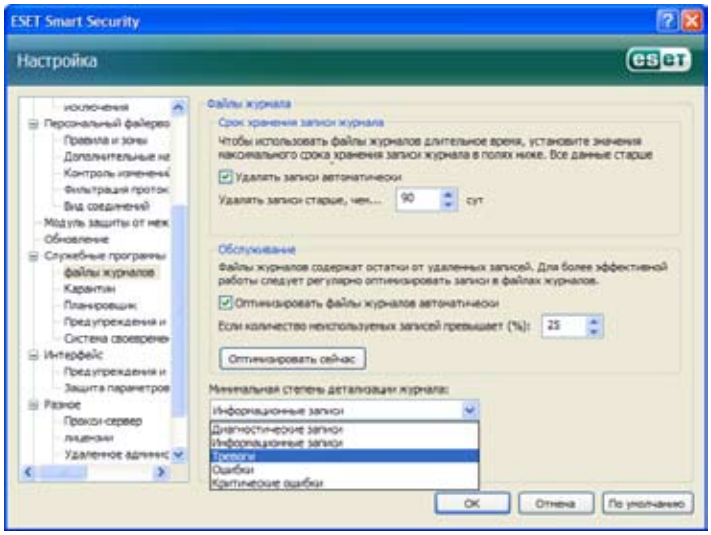
- **Обнаруженные угрозы** (Detected threats): в этих журналах содержатся все сведения о событиях, связанных с обнаружением вирусных проникновений;
- **События** (Events): этот пункт позволяет системным администраторам и пользователям находить решения проблем. В журналы событий записываются все значительные действия, выполняемые программой ESET NOD32 Smart Security;
- **Сканирование компьютера по требованию** (On-demand computer scan): в этом окне отображаются результаты всех завершенных операций сканирования. Дважды щелкнув любую запись, можно просмотреть соответствующие подробные результаты сканирования по запросу;
- **Журнал персонального файервола ESET** (ESET Personal firewall log): содержит записи о всех фактах обнаружения угроз персональным файерволом или связанных с ним. Анализ журнала файервола позволяет вовремя обнаружить попытки проникновения в систему и предотвратить несанкционированный доступ к ней.

В каждом разделе отображенные сведения можно напрямую скопировать в буфер обмена, выбрав запись и нажав кнопку **Копировать** (Copy). Чтобы выбрать несколько записей, удерживайте нажатыми клавиши CTRL или SHIFT.

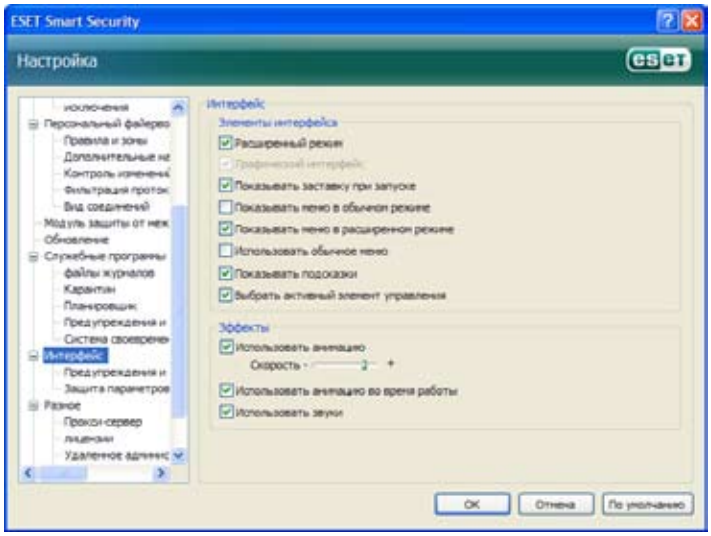
4.7.1 Ведение журнала

Доступ к конфигурации ведения журналов в ESET NOD32 Smart Security можно получить в главном окне программы. Выберите команды **Настроить** > **Открыть полное дерево расширенной настройки**... > **Инструменты** > **Файлы журналов** (Setup > Enter entire advanced setup tree... > Tools > Log files). Для файлов журналов можно настроить следующие параметры:

- **удалять записи автоматически** (Delete records automatically): автоматически удаляются записи журналов, возраст которых превысил указанное количество дней;
- **оптимизировать файлы журналов автоматически** (Optimize log files automatically): позволяет выполнить автоматическую дефрагментацию файлов журналов при превышении определенной процентной доли неиспользуемых записей;
- **Минимальная степень детализации журнала** (Minimum logging verbosity): определяет уровень словесного наполнения журнала. Доступные варианты:
  - **Критические ошибки** (Critical errors): в журнал включаются только опасные ошибки (ошибка запуска защиты против вирусов, персонального файервола и т. д.);
  - **Ошибки** (Errors): записываются только сообщения «Ошибка загрузки файла» (Error downloading file) и сообщения об опасных ошибках;
  - **Тревоги** (Warnings): записываются сообщения об опасных ошибках и предупреждениях;
  - **Информационные записи** (Informative records): записываются информационные сообщения, включая сообщения об успешном обновлении и все перечисленные выше;
  - **Диагностические записи** (Diagnostic records): в журнал включаются сведения, необходимые для настройки программы, и все перечисленные выше сообщения.



4.8 Пользовательский интерфейс



Параметры конфигурации пользовательского интерфейса в ESET NOD32 Smart Security можно изменить таким образом, чтобы настроить рабочую среду в соответствии с потребностями пользователя. Эти параметры конфигурации доступны в разделе **Интерфейс** (User interface) дерева расширенной настройки (ESET NOD32 Smart Security).

В разделе **Элементы пользовательского интерфейса** (User interface elements) пользователям предоставляется возможность включать и отключать расширенный режим по своему усмотрению. В расширенном режиме доступны более широкие возможности настройки и дополнительные функции управления программой ESET NOD32 Smart Security.

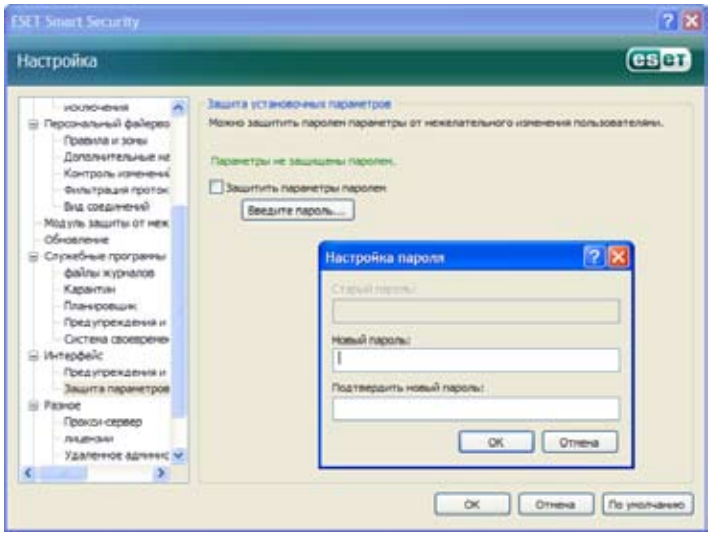
Флажок **Графический интерфейс пользователя** (Graphical user interface) необходимо снять, если графические элементы снижают производительность компьютера или приводят к возникновению проблем. Необходимость отключения графического интерфейса может возникнуть

у пользователей с нарушениями зрения, поскольку элементы этого интерфейса могут создать конфликт со специальными приложениями, используемыми для считывания текста с экрана.

Чтобы отключить появление заставки ESET NOD32 Smart Security при запуске программы, снимите флажок **Показывать заставку при запуске** (Show splash-screen at startup).

В верхней части основного окна программы ESET NOD32 Smart Security расположено стандартное меню, которое можно активировать или отключить с помощью флажка **Использовать обычное меню** (Use standard menu).

Если установлен флажок **Показывать подсказки** (Show tooltips), то при наведении курсора на какой-либо параметр будет отображаться его краткое описание. При установленном флажке **Выбрать активный элемент управления** (Select active control element) система выделяет элемент, находящийся в данный момент в области действия курсора мыши. После нажатия кнопки мыши выделенный элемент активируется.



Чтобы уменьшить или увеличить скорость отображения анимированных эффектов, установите флажок **Использовать анимацию** (Use animated controls) и передвиньте ползунок **Скорость** (Speed) соответственно влево или вправо.

Чтобы включить использование анимированных пиктограмм для представления хода выполнения различных операций, установите флаг **Использовать анимацию во время работы** (Use animated icons...) Если программа должна выдавать звуковое предупреждение о важном событии, установите флаг **Использовать звуки** (Use sound signal).

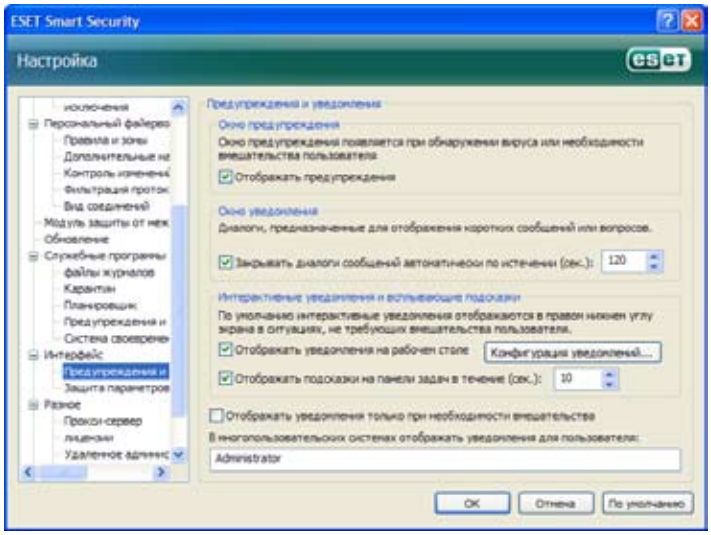
Интерфейс (User interface) включает также возможность защиты параметров настройки ESET NOD32 Smart Security паролем. Эта функция доступна в подменю **Защита параметров** (Settings protection) раздела **Интерфейс** (User interface). Правильная настройка системы очень важна для обеспечения ее максимальной безопасности. Несанкционированные изменения могут привести к утере важных данных. Чтобы установить пароль для защиты параметров настройки, нажмите кнопку **Ввести пароль**... (Enter password...).

4.8.1 Предупреждения и уведомления

Область **Предупреждений и уведомлений** (Alerts and notifications setup) в разделе **Интерфейс** (User interface) позволяет настроить, каким образом сообщения предупреждений об угрозах и системные уведомления обрабатываются в ESET NOD32 Smart Security.

Первый элемент – **Отображать предупреждения** (Display alerts). Снятие этого флажка отменяет все окна предупреждений и применимо только для ограниченного числа особых ситуаций. Для большинства пользователей рекомендуется оставить настройку по умолчанию (установленный флажок).

Чтобы всплывающие окна автоматически закрывались по истечении определенного времени, установите флажок **Закрывать диалоги сообщений автоматически по истечении (сек.)** (Close messageboxes automatically after (sec.)). Если окна предупреждений не закрыты пользователем вручную, они автоматически закрываются по истечении указанного периода времени.



Уведомления на рабочем столе и всплывающие подсказки носят только информативный характер и не требуют взаимодействия с пользователем. Они отображаются в области уведомлений в нижнем правом углу экрана. Чтобы включить отображение уведомлений на рабочем столе, установите флажок **Отображать уведомления на рабочем столе** (Display notifications on desktop). Более подробные параметры (время отображения уведомления и степень прозрачности окна) можно изменить, нажав кнопку **Настроить уведомления**... (Configure notifications...). Кнопка **Предварительный просмотр** (Preview) выводит на экран предварительный просмотр поведения уведомлений. Продолжительность отображения всплывающих подсказок задается параметром **Отображать подсказки в панели задач в течение (сек.)** (Display balloon tips in taskbar (for sec.)).

В нижней части экрана **Предупреждения и уведомления** (Alerts and notifications) расположен параметр **Отображать уведомления только при необходимости вмешательства** (Display only notifications requiring user intervention). Установка и снятие этого флажка позволяют соответ-

ственно включить или выключить отображение предупреждений и уведомлений, не требующих реакции пользователя. Последний элемент в этом разделе задает адреса уведомлений в многопользовательской среде.

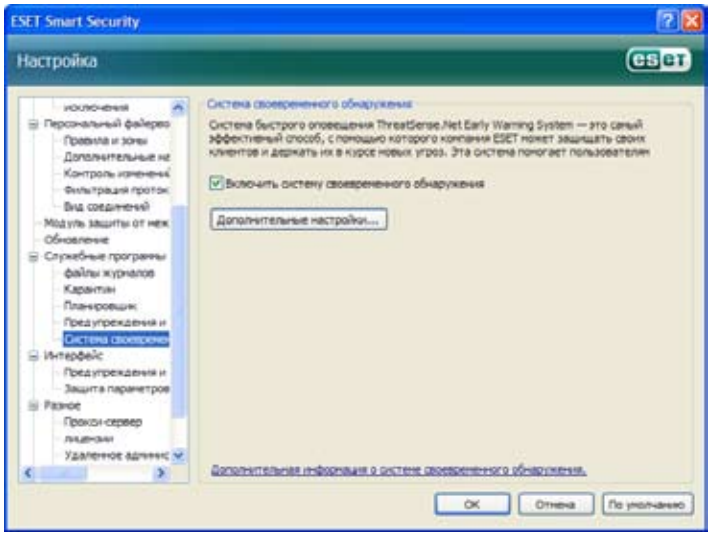
Поле **В многопользовательских системах отображать уведомления для пользователя:** (On multi-user systems, display notifications on the screen of the user:) позволяет определить адресатов для получения важных уведомлений программы ESET NOD32 Smart Security. Как правило, здесь указан системный администратор или администратор сети. Этот параметр особенно полезен при работе с терминальным сервером, позволяя указать отправку всех системных уведомлений администратору.

4.9 ThreatSense.Net

Система предупреждения ThreatSense.Net Система раннего оповещения – это инструмент, поддерживающий немедленное и постоянное информирование ESET о новых проникновениях.

У двунаправленной системы предупреждений ThreatSense.Net Early Warning System одно назначение – совершенствовать предлагаемую защиту. Оптимальный метод обнаружения новых угроз по мере их возникновения заключается в установлении связи с максимально большим числом наших клиентов и использовании их в качестве «разведчиков угроз». Существует два варианта:

- Вы можете отключить систему раннего оповещения ThreatSense.Net Early Warning System. При этом вы не проигрываете в функциональности программного обеспечения и продолжаете получать наилучшую защиту, какую мы только можем предложить.
- Вы можете настроить систему предупреждений Early Warning System на объединение анонимных сведений о новых угрозах и местах обнаружения нового вредоносного программного кода в один файл. Этот файл может быть отправлен в ESET для подробного изучения. Исследование данных угроз позволит компании ESET сделать продукты еще лучше. В системе предупреждений ThreatSense.Net Early Warning System производится сбор данных о компьютере, имеющих отношение к новым обнаруженным угрозам. Среди этих данных могут быть образец или копия файла, в котором была обнаружена угроза, путь к этому файлу, имя файла, дата и время, процесс, в результате которого угроза проникла на компьютер, и сведения об операционной среде компьютера. Некоторые из данных могут включать личные сведения о пользователе компьютера, например имена пользователей в пути к каталогу и т. д.



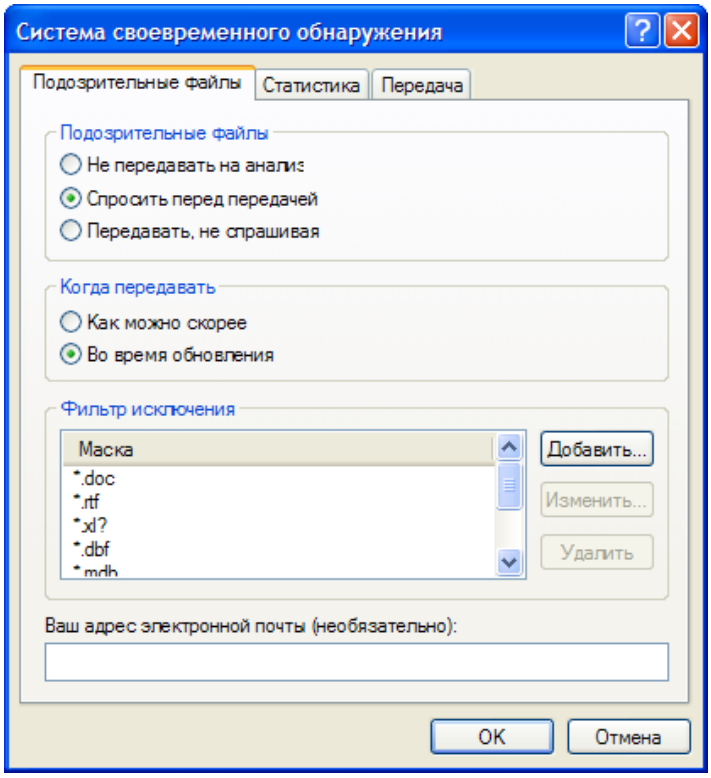
Несмотря на то, что в вирусной лаборатории ESET может быть раскрыта информация о пользователях или компьютерах, эти сведения используются исключительно в целях немедленного реагирования на новые угрозы и НЕ предназначена для других целей.

По умолчанию в программе ESET NOD32 Smart Security настроен запрос подтверждения перед отправкой подозрительных файлов для подробного изучения в вирусной лаборатории ESET. Необходимо отметить, что файлы с определенными расширениями (DOC, XLS) всегда исключаются из отправки, даже если в них обнаружены угрозы. Чтобы избежать нежелательной отправки файлов других определенных типов, сюда можно добавить и другие расширения.

Настройка ThreatSense.Net доступна в дереве расширенной настройки в разделе **Инструменты** > **ThreatSense.Net** (Tools > ThreatSense.Net). Установите флажок **Включить систему раннего оповещения ThreatSense.Net Early Warning System** (Enable ThreatSense.Net Early Warning System). Это позволит активировать и нажать кнопку **Расширенная настройка**... (Advanced Setup...).

4.9.1 Подозрительные файлы

На вкладке **Подозрительные файлы** (Suspicious files) вы можете настроить способ отправки обнаруженных угроз для изучения в лабораторию ESET.



При обнаружении подозрительного файла его можно отправить в вирусные лаборатории на изучение. Если эта угроза окажется вредоносным приложением, его код будет добавлено в следующие обновления вирусных сигнатур.

Предусмотрена возможность автоматической отправки файлов, без подтверждения пользователя. Если этот флажок установлен, отправка подозрительных файлов осуществляется в фоновом режиме. Чтобы отслеживать файлы, отправляемые на изучение, и подтверждать отправку, установите флаг **Спросить перед передачей** (Ask before submitting).

Если вы хотите запретить отправку любых файлов, установите флаг **Не передавать на анализ** (Do not submit for analysis). Обратите внимание, что отключение отправки файлов на анализ не оказывает влияния на отправку в ESET статистических данных. Для статистических данных предусмотрен отдельный раздел настройки, описание которого приводится в следующей главе.

Время отправки

Подозрительные файлы будут отправлены на изучение в лаборатории ESET. Этот параметр рекомендуется при наличии постоянного интернет-подключения и возможности незамедлительной отправки подозрительных файлов. Другая возможность заключается в отправке подозрительных файлов **Во время обновления** (During update). Если выбран этот параметр, подозрительные файлы будут сгруппированы и выгружены на сервер системы предупреждений Early Warning System во время обновления.

Исключающий фильтр

Не все файлы требуется отправлять на изучение. Исключающий фильтр позволяет исключить из отправки определенные файлы или папки. Так, например, может оказаться целесообразным исключить файлы, в которых могут содержаться потенциально конфиденциальные сведения (например, документы или электронные таблицы). Наиболее распространенные типы файлов исключены по умолчанию (Microsoft Office, OpenOffice). Список исключенных файлов при необходимости может быть расширен.

Контактный адрес электронной почты

Вместе с подозрительными файлами в ESET отправляется контактный адрес электронной почты, по которому с вами можно будет связаться при необходимости получения дополнительных сведений об отправленных файлах. Обратите внимание на тот факт, что ответ от ESET не будет вам отправлен, пока не потребуется дополнительная информация.

4.9.2 Статистические данные

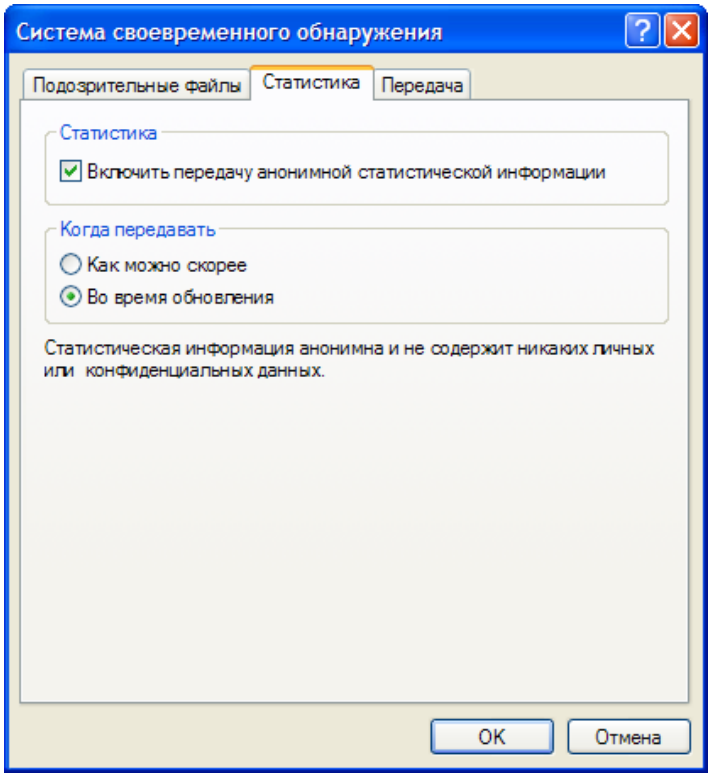
В системе раннего оповещения ThreatSense.Net Early Warning System производится сбор анонимных данных о компьютере, имеющих отношение к новым обнаруженным угрозам. Эти сведения могут содержать имя проникнувшего вируса, дату и время его обнаружения, версию программы ESET NOD32 Smart Security, версию операционной системы компьютера и настройки расположения. Обычно отправка статистических данных на серверы ESET осуществляется один или два раза в день.

Пример отправленного пакета статистических данных:

```
# 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\ rdgFR1463[1].exe
```

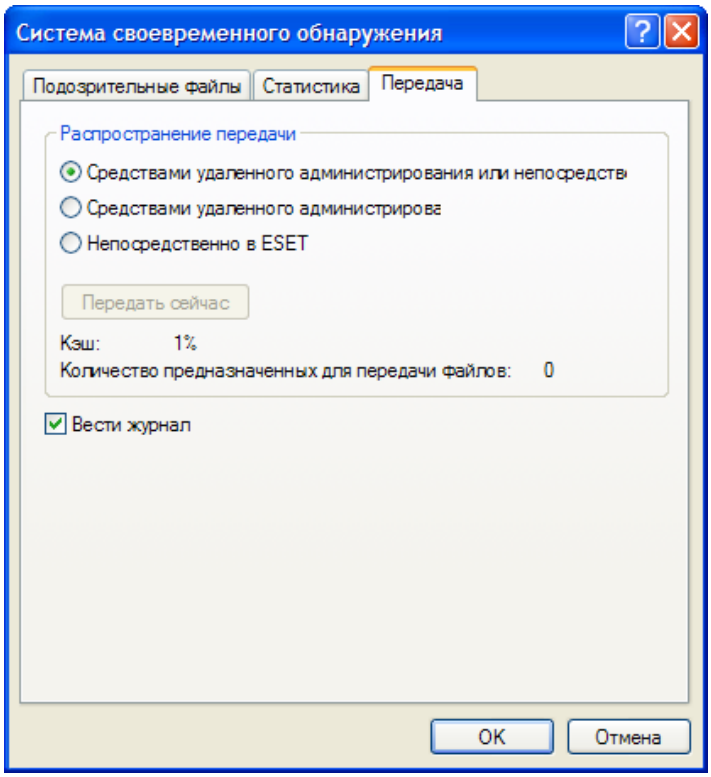
Время отправки

В разделе **Время отправки** (When to submit) вы можете задать момент отправки статистических данных. Если выбран параметр **Как можно скорее** (As soon as possible), статистические данные отправляются сразу после их создания. Эта настройка применима при наличии постоянного интернет-подключения. Если выбран параметр **Во время обновления** (During update), статистические данные сохраняются и отправляются одновременно во время следующей операции обновления.



4.9.3 Отправка

В данном разделе можно выбрать, должны ли файлы и статистические данные отправляться при помощи ESET Remote Administrator или непосредственно в ESET. Чтобы убедиться в доставке подозрительных файлов и статистических данных в ESET, выберите параметр **Средствами удаленного администрирования или непосредственно в ESET** (By means of Remote Administrator or directly to ESET). Если этот флажок установлен, файлы и статистические данные отправляются всеми доступными средствами. При отправке подозрительных файлов **Средствами удаленного администрирования** файлы и статистические данные отправляются на удаленный сервер администрирования, гарантирующий их последующую доставку в вирусные лаборатории ESET. Если выбран параметр **Непосредственно в ESET** (Directly to ESET), все подозрительные файлы и статистические данные отправляются в вирусные лаборатории ESET непосредственно из программы.



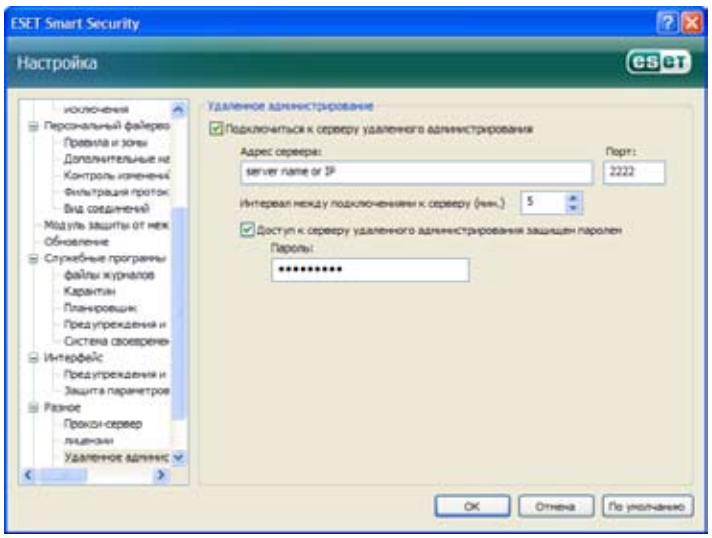
При наличии файлов с отложенной отправкой в этом окне настройки активирована кнопка **Отправить сейчас** (Submit now). Нажмите эту кнопку, чтобы отправить файлы и статистические данные немедленно.

Установленный флажок **Вести журнал** (Enable logging) позволяет включить запись отправки файлов и статистических данных. После каждой отправки подозрительного файла или порции статистических данных в журнале событий создается запись.

4.10 Удаленное администрирование

Удаленное администрирование представляет собой мощный инструмент для поддержания политики безопасности и управления безопасностью в рамках сети. Это особенно полезно в отношении крупных сетей. Удаленное администрирование не только увеличивает уровень защиты, но и предоставляет простую в использовании возможность администрирования ESET NOD32 Smart Security на клиентских рабочих станциях.

Параметры настройки удаленного администрирования доступны из главного окна программы ESET NOD32 Smart Security. Выберите пункты меню **Настройка** > **Полностью раскрыть дерево расширенной настройки**... > **Разное** > **Удаленное администрирование** (Setup > Enter the entire advanced setup tree... > Miscellaneous > Remote administration).



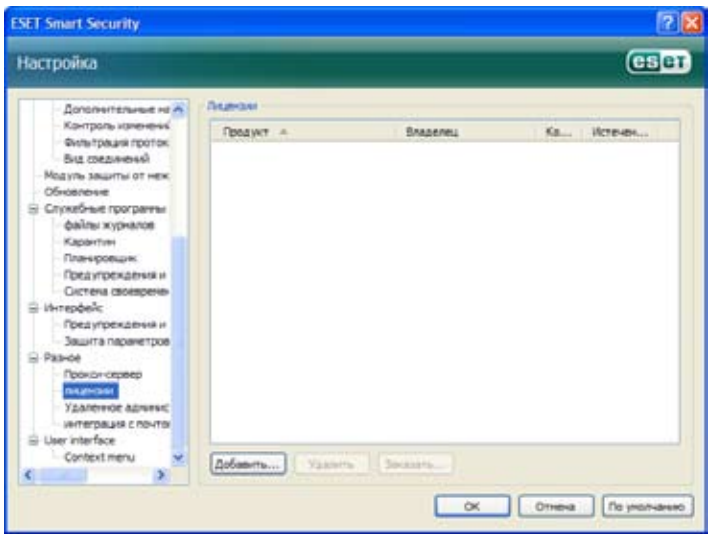
В окне настройки вы можете включить режим удаленного администрирования, установив флаг **Подключиться к серверу удаленного администрирования** (Connect to Remote Administration server check). После этого доступны следующие параметры:

- **Адрес сервер**а (Server address): сетевой адрес сервера, на котором установлен сервер удаленного администрирования;
- **Порт** (Port): в этом поле содержится номер предопределенного порта сервера, используемого для подключения. Рекомендуется оставить предопределенную настройку порта (2222).
- **Интервал между подключениями к серверу (мин.)** (Interval between connections to server (min.)): обозначает частоту подключения программы ESET NOD32 Smart Security к серверу ERA для отправки данных. Другими словами, сведения отправляются с указанными здесь интервалами времени. Если этому параметру присвоено значение 0, отправка данных осуществляется каждые 5 секунд.
- **Для Remote Administrator требуется проверка подлинности** (Remote Administrator requires authentication): установленный флаг позволяет при необходимости ввести пароль для подключения к серверу Remote Administrator.

Нажмите кнопку OK (OK), чтобы подтвердить изменения и применить эти настройки. Используя эти настройки, программа ESET NOD32 Smart Security подключается к удаленному серверу.

4.11 Лицензия

В разделе **Лицензии** (License) реализовано управление ключами лицензий для программы ESET NOD32 Smart Security и других продуктов ESET, например ESET Remote Administrator, ESET NOD32 for Microsoft Exchange и др. После приобретения продукта ключи лицензии поставляются вместе с именем пользователя и пароля. Чтобы **Добавить/Удалить** (Add/Remove) ключ лицензии, нажмите соответствующую кнопку в окне диспетчера лицензий. Чтобы открыть диспетчер лицензий из дерева расширенной настройки, выберите узлы **Разное** > **Лицензии** (Miscellaneous > Licenses).



Ключ лицензии представляет собой текстовый файл, в котором содержатся сведения о приобретенном продукте: владелец продукта, количество лицензий и срок действия лицензии.

Окно диспетчера лицензий позволяет пользователю выгрузить и просмотреть содержимое ключа лицензии, нажав кнопку **Добавить**... (Add...): содержимое лицензии будет отображено в окне диспетчера. Чтобы удалить файлы лицензий из списка, нажмите кнопку **Удалить** (Remove).

Если срок действия ключа истек, и вы заинтересованы в приобретении продления лицензии, нажмите кнопку **Заказать**... (Order...), и вы будете перенаправлены в онлайн-магазин.

5. Опытный пользователь

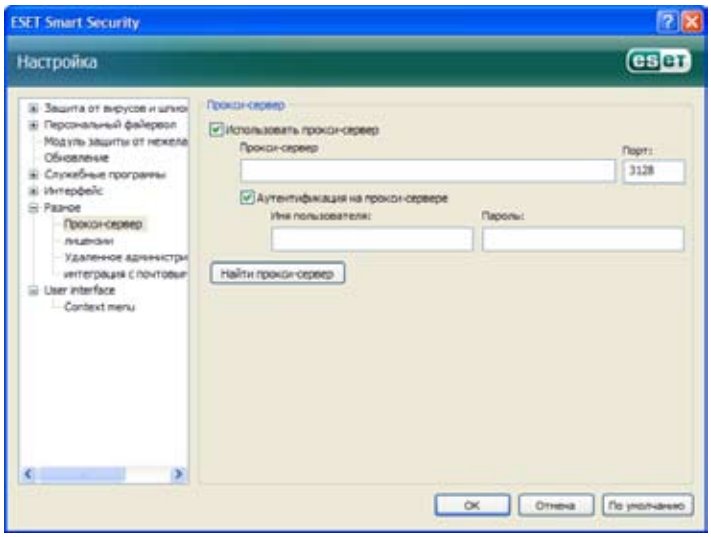
В данной главе описаны функциональные возможности ESET NOD32 Smart Security, которые могут оказаться полезными для опытных пользователей. Параметры настройки этих функций доступны только в расширенном режиме. Чтобы переключиться в расширенный режим, щелкните запись **Переключатель расширенного режима** (Toggle Advanced mode) в нижнем левом углу главного окна программы или нажмите клавиши CTRL+M.

5.1 Настройка прокси-сервера

В программе ESET NOD32 Smart Security настройка прокси-сервера может быть выполнена в двух различных разделах древовидной структуры расширенной настройки.

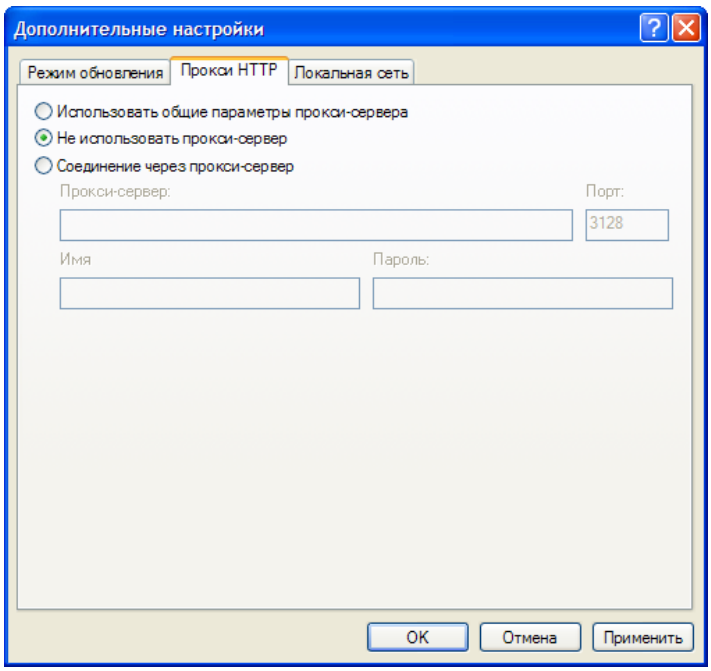
Настройки прокси-сервера можно сконфигурировать в разделе **Разное** > **Прокси-сервер** (Miscellaneous > Proxy server). Определение прокси-сервера на этом уровне задает глобальные настройки прокси-сервера для всей программы ESET NOD32 Smart Security. Указанные здесь параметры будут использованы во всех модулях, требующих интернет-подключения.

Чтобы установить настройки прокси-сервера для этого уровня, установите флажок **Использовать прокси-сервер** (Use proxy server), в поле **Прокси-сервер:** (Proxy server:) укажите адрес прокси-сервера, а в поле **Порт** (Port) – номер порта прокси-сервера.



Если для обмена данными с прокси-сервером требуется проверка подлинности, установите флаг **Аутентификация на прокси-сервере** (Proxy server requires authentication) и в соответствующие поля введите **Имя пользователя** (User name) и **Пароль** (Password). Нажмите кнопку **Найти прокси-сервер** (Detect proxy server), чтобы автоматически определить и вставить настройки прокси-сервера. При этом будут скопированы параметры, настроенные в приложении Internet Explorer. Обратите внимание, что эта функция не извлекает учетные данные (имя пользователя и пароль) – пользователь должен предоставить их самостоятельно.

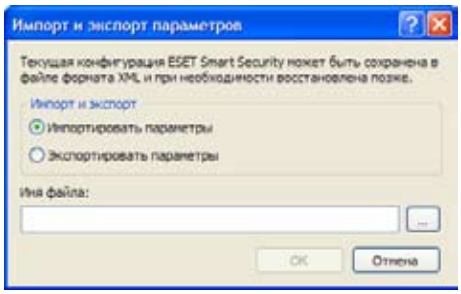
Кроме того, параметры прокси-сервера можно настроить в блоке **Дополнительные настройки обновлений** (Advanced update setup) (в разделе **Обновления** (Update) дерева расширенной настройки). Эти настройки применяются к конкретному профилю обновлений и рекомендованы для переносных компьютеров, поскольку на них обновления вирусных сигнатур часто запрашиваются из разных расположений. Дополнительные сведения об этом параметре см. в разделе 4.4 «Обновление системы» (Updating the system).



5.2 Экспорт / импорт настроек

Экспорт и импорт текущей конфигурации программы ESET NOD32 Smart Security можно запустить в расширенном режиме из раздела **Настройка** (Setup).

Как экспорт, так и импорт осуществляются при помощи файлов XML-типа. Экспорт и импорт полезны при необходимости резервного копирования текущей конфигурации системы ESET NOD32 Smart Security с целью использования ее в дальнейшем (по каким бы то ни было причинам). Возможность настройки экспорта может быть использована и пользователями, желающими работать со своей, ранее созданной конфигурацией ESET NOD32 Smart Security в нескольких системах: им требуется только импортировать XML-файл.



5.2.1 Экспорт настроек

Экспортировать конфигурацию очень просто. Чтобы сохранить текущую конфигурацию программы ESET NOD32 Smart Security, выберите команды **Настройка** > **Импорт и экспорт настроек**... (Setup > Import and export settings...). Выберите команду **Экспортировать настройки** (Export settings) и введите имя для файла конфигурации. При помощи обозревателя вы можете выбрать папку на своем компьютере, в которой должен быть сохранен этот файл.

5.2.2 Импорт настроек

Действия по импорту конфигурации схожи с действиями по ее экспорту. Выберите раздел **Импорт и экспорт настроек** (Import and export settings) и команду **Импортировать настройки** (Import settings). Нажмите кнопку «...» и выберите файл конфигурации, который необходимо импортировать.

5.3 Командная строка

Модуль защиты от вирусов ESET NOD32 Smart Security можно запустить из командной строки: вручную (при помощи команды «ecls») или при помощи командного файла («BAT»).

При запуске сканирования по запросу из командной строки можно использовать описанные далее параметры и переключатели.

■ **Общие параметры:**

– help — Отобразить справку и выйти
– version — Отобразить сведения о версии и выйти
– base-dir = ИМЯ_ПАПКИ — Загрузить модули из каталога ИМЯ_ПАПКИ
– quar-dir = ИМЯ_ПАПКИ — Поместить каталог ИМЯ_ПАПКИ в карантин
– aind — Отобразить индикатор активности

■ **Объекты назначения:**

– 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 = ПРЕДЕЛ — Сканировать архивы не дольше указанных в значении ПРЕДЕЛ секунд.. Если время сканирования достигает этого предела, сканирование архива останавливается и продолжается со следующего файла.
– max-arch-size=РАЗМЕР — Сканировать только указанное в значении РАЗМЕР количество первых байтов архивов (по умолчанию: 0 = без ограничений)
– mail — Сканировать файлы электронной почты
– no-mail — Не сканировать файлы электронной почты
– sfx — Сканировать самораспаковывающиеся архивы
– no-sfx — Не сканировать самораспаковывающиеся архивы
– rtp — Сканировать runtime-пакеты
– no-rtp — Не сканировать runtime-пакеты
– exclude = ИМЯ_ПАПКИ — Исключить каталог ИМЯ_ПАПКИ из сканирования
– subdir — Сканировать вложенные каталоги (по умолчанию)
– no-subdir — Не сканировать вложенные каталоги
– max-subdir-level = УРОВЕНЬ — Максимальный УРОВЕНЬ вложенности каталогов (по умолчанию: 0 = без ограничений)
– symlink — Следовать по символическим ссылкам (по умолчанию) (?)
– no-symlink — Пропустить символические ссылки
– ext-remove = РАСШИРЕНИЯ
– ext-exclude = РАСШИРЕНИЯ — Исключить из сканирования РАСШИРЕНИЯ, перечисленные через двоеточие

■ **Методы:**

– adware — Сканировать на наличие рекламного ПО / шпионских программ / потенциально опасных приложений
– No-adware — Не сканировать на наличие рекламного ПО / шпионских программ / потенциально опасных приложений
– 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 эвристики
– No-heur — Отключить эвристики
– Adv-heur — Включить расширенные эвристики
– No-adv-heur — Отключить расширенные эвристики

■ **Очистка:**

– action = ДЕЙСТВИЕ — Выполнить ДЕЙСТВИЕ в отношении зараженных объектов. Возможные действия: нет, очистка, запрос (none, clean, prompt)
– quarantine — Скопировать зараженные файлы в папку Quarantine (дополнение к ДЕЙСТВИЮ)
– no-quarantine — Не копировать зараженные файлы в папку Quarantine

■ **Журналы:**

– log-file=ФАЙЛ — Вывод журнала в ФАЙЛ
– log-rewrite — Перезаписать файл вывода (по умолчанию: добавить)
– log-all — Включать в журнал в том числе чистые файлы
– no-log-all — Не включать в журнал чистые файлы (по умолчанию)

■ **Возможные коды завершения сканирования:**

0 – Угрозы не обнаружены
1 – Угроза обнаружена, но не ликвидирована
10 – Осталось несколько зараженных файлов
101 – Ошибка архивирования
102 – Ошибка доступа
103 – Внутренняя ошибка

ПРИМЕЧАНИЕ.

Коды завершения, превышающие 100, означают, что файл не был включен в сканирование и, таким образом, может быть зараженным.

6. Глоссарий

6.1 Типы проникновений

Проникновение – экземпляр вредоносного программного обеспечения, проникающий и/или повреждающий компьютер пользователя.

6.1.1 Вирусы

Компьютерный вирус представляет собой проникновение, повреждающее существующие на компьютере файлы. Вирусы названы по аналогии с биологическими вирусами, поскольку для распространения с одного компьютера на другой они используют похожие методы.

Объектами атак компьютерных вирусов являются, как правило, исполняемые файлы и документы. В целях репликации (размножения) вирус добавляет свое «тело» в целевой файл. Вкратце действие компьютерного вируса можно описать следующим образом: после выполнения зараженного файла вирус самоактивируется (до того, как это сделает исходное приложение) и осуществляет свою предопределенную задачу. Только после этого очередность выполнения передается исходному приложению. Вирус не может инфицировать компьютер до тех пор, пока пользователь (случайно или преднамеренно) не запустит или не откроет вредоносную программу.

Существует множество компьютерных вирусов, различающихся по способу заражения и серьезности. Некоторые из них особенно опасны, поскольку реализуют возможность целенаправленного удаления файлов с жесткого диска. С другой стороны, некоторые вирусы не приносят фактического ущерба, ставя своей целью раздражение пользователя и демонстрацию возможностей своих создателей.

Важно помнить, что вирусы (в отличие от троянского или шпионского ПО) постепенно теряют свою популярность, поскольку не приносят коммерческой выгоды создателям вредоносного ПО. Кроме того, под термином «вирус» часто ошибочно понимают все типы проникновений. В настоящее время эта тенденция уходит в прошлое и замещается более точным термином «вредоносное ПО» (malware).

Если компьютер заражен вирусом, необходимо восстановить исходное состояние зараженных файлов, то есть очистить их при помощи антивирусной программы.

Примеры вирусов: OneHalf, Tenga и Yankee Doodle.

6.1.2 Черви

Компьютерный червь – программа, содержащая вредоносный программный код, совершающая атаки на хост-компьютеры и распространяющаяся по сети. Основное различие между вирусом и червем заключается в том, что в червях реализована возможность саморепликации и самостоятельного перемещения. Они не зависят от основного файла (или загрузочных секторов).

Распространение червей осуществляется по электронной почте или в виде сетевых пакетов. В соответствии с этим червей можно классифицировать по двум категориям:

- **Электронная почта** (Email): самостоятельно рассылающие себя по адресам электронной почты, найденным в списке контактов пользователя, и
- **Сетевые** (Network): эксплуатирующие уязвимость системы безопасности в различных приложениях.

Таким образом, жизнеспособность червей по сравнению с компьютерными вирусами выше. Благодаря широкой доступности интернета они распространяются по всему миру за считанные часы с момента выпуска, а в некоторых случаях и в пределах нескольких минут. Возможность независимого и быстрого размножения повышает их опасность по сравнению с другими типами вредоносного ПО (например, вирусами).

Червь, активированный в системе, может вызвать ряд неудобств: он может удалять файлы, способствовать снижению производительности системы и даже деактивировать некоторые программы. Природа компьютерных червей позволяет отнести их в разряд «транспортных средств» для других типов проникновения.

Если компьютер инфицирован компьютерным червем, рекомендуется удалить зараженные файлы, поскольку в них вероятно присутствие вредоносного кода.

Примеры хорошо известных червей: Lovsan/Blaster, Stration/Warezov, Bagle и Netsky.

6.1.3 Троянские программы

Раньше компьютерные троянские программы считались классом проникновений с попытками выдать себя за полезные программы и таким обманным путем заставить пользователя запустить их. Важно помнить, что это определение троянских программ справедливо в отношении прошлого; в настоящее время они редко самомаскируются . Основная цель таких программ заключается в максимально простом проникновении и дальнейшем достижении целей. «Троянский конь» – обобщающий термин, обозначающий любые проникновения, которые не попадают под определения других классов.

Вследствие общности этой категории в ней часто выделяют подкатегории, наиболее известными среди которых являются:

- менеджер закачек (downloader): вредоносная программа с возможностью загрузки других проникновений через интернет;
- инсталляторы прочих программ (dropper): троянские программы этого типа устанавливают на инфицированные компьютеры вредоносное ПО других типов;
- «бэкдор» (backdoor): приложение для обмена данными с удаленными взломщиками, позволяющее им получить доступ к системе и перенять управление ей;
- перехватчик клавиатуры (keylogger, keystroke logger): программа для записи каждого нажатия клавиши пользователем и отправки этих данных удаленным взломщикам;
- «дозвонщик» (dialer): в таких программах реализовано подключение к номерам с повышенными тарифами на соединение. Создание нового подключения практически незаметно для пользователя. Программы-дозвонщики могут стать проблемой для пользователей, использующих модемы с наборным вызовом, но такие модемы постепенно выходят из обращения.

Как правило, троянские программы принимают форму исполняемых файлов с расширением EXE. Если на компьютере обнаружено троянское ПО, его рекомендуется удалить.

Примеры хорошо известных троянских программ: NetBus, Trojandownloader, Small.ZL и Slapper.

6.1.4 Руткиты

Руткиты (rootkits) – вредоносные программы, предоставляющие интернет-злоумышленникам несанкционированный доступ к системе, скрывая при этом их присутствие. Получив доступ к системе (как правило, посредством использования уязвимости в системе безопасности), руткиты при помощи функций операционной системы предотвращают их обнаружение антивирусным ПО: они маскируются под процессами, файлами и данными реестра Windows. По этим причинам обнаружить их при помощи обычных методов тестирования практически невозможно.

Чтобы предотвратить активность руткитов, следует помнить о двух уровнях обнаружения:

- во время их попыток получить доступ к системе: программы еще не присутствуют в системе, а потому неактивны. Возможность ликвидировать руткиты на этом уровне реализована в большинстве антивирусных систем (при условии, что они считают такие файлы зараженными);
- во время их укрытия от обычной проверки: Пользователям антивирусной системы ESET предоставляется преимущество технологии Anti-Stealth, позволяющей выявить и ликвидировать активные руткиты.

6.1.5 Рекламное программное обеспечение

Adware – сокращение от английского выражения «advertising supported software» (программное обеспечение с поддержкой рекламы). В эту категорию попадают программы, при выполнении которых пользователю показываются рекламные материалы. Приложения рекламного ПО автоматически открывают новые всплывающие окна веб-браузера, содержащие рекламу, или изменяют домашнюю страницу браузера. Часто рекламное ПО входит в комплекты свободно распространяемых программ, таким образом позволяя их создателям покрыть расходы на разработку своих (часто полезных) приложений.

За исключением показов рекламы, рекламное ПО не несет в себе угрозы. Опасность заключается в возможности осуществления такими программами отслеживающих действий (аналогично шпионскому ПО).

При использовании свободно распространяемых программ следует обратить особое внимание на программу установки. Программа-установщик, скорее всего, выдаст уведомление об установке дополнительных рекламных компонентов. Часто предоставляется возможность отменить это действие и установить программу без рекламного ПО.

С другой стороны, некоторые программы не допускают установки без рекламных компонентов либо предлагают ограниченную функциональность. Это означает, что рекламному ПО предоставляется «официальный» доступ к системе, поскольку это осуществляется с согласия пользователя. В данном случае лучше придерживаться правил безопасности, чем сожалеть в будущем о своих действиях.

Если на компьютере некоторые файлы определены как рекламное ПО, их рекомендуется удалить, поскольку они могут содержать вредоносный код.

6.1.6 Шпионские программы

В эту категорию попадают все приложения, отправляющие личные данные без ведома или согласия пользователя. Используя отслеживающие функции, эти программы отправляют различные статистические данные, например список посещенных веб-сайтов, адреса электронной почты из списка контактов пользователя или список записанных нажатий клавиш.

Создатели шпионских программ утверждают, что эти методы предназначены для выявления пользовательских потребностей и интересов с целью проведения более направленной рекламы. Проблема заключается в отсутствии четкой разницы между полезными и вредоносными приложениями, и никто не может гарантировать отказ от злоупотребления полученными данными. Среди данных, собранных шпионскими приложениями, могут оказаться коды безопасности, личные идентификационные номера (PIN-коды), номера банковских счетов и т. д. Часто шпионские программы включаются их создателями в бесплатные версии программ, позволяя получить прибыль или мотивировать пользователя на приобретение ПО. Как правило, во время установки программы пользователям выдается предупреждение о наличии шпионского ПО, побуждая их приобрести версию, не содержащую подобные компоненты.

Примерами хорошо известных бесплатных продуктов, сопровождаемых шпионскими приложениями, являются клиентские приложения одноранговых (P2P) сетей. Spyfalcon, Spy Sheriff и многие другие программы принадлежат к особой подкатегории шпионских программ – они представляются как программы защиты от шпионского ПО, хотя сами являются таковым.

Если на компьютере некоторые файлы определены как шпионские программы, их рекомендуется удалить, поскольку они могут содержать вредоносный код.

6.1.7 Потенциально опасные приложения

Существует множество законных программ, упрощающих администрирование компьютеров, объединенных в сеть. Тем не менее, злоумышленники могут использовать их во вредоносных целях. Именно поэтому в системах ESET создана эта отдельная категория. Клиентам ESET предоставляется возможность указать системе защиты от вирусов на необходимость (или отсутствие таковой) обнаружения таких угроз.

«Потенциально опасные приложения» – термин, используемый для коммерческого, законно распространяемого ПО. К этой категории относятся такие программы, как средства удаленного доступа, приложения для взлома паролей и перехватчики клавиатур (программы, записывающие каждое нажатие клавиш пользователем).

Обнаружив присутствие и выполнение потенциально опасного приложения на своем компьютере (при условии, что вы не сами его установили), обратитесь к администратору сети или удалите приложение.

6.1.8 Потенциально нежелательные приложения

Потенциально нежелательные приложения необязательно являются вредоносными, но могут отрицательно воздействовать на производительность системы. Как правило, для установки таких программ требуется согласие пользователя. Наличие таких программ на компьютере изменяет поведение системы (по сравнению с ее состоянием до установки этих программ). Наиболее существенные изменения заключаются в следующем:

- открываются новые окна, которых не было видно раньше;
- активируются и запускаются скрытые процессы;
- увеличивается использование системных ресурсов;
- изменяются результаты поиска;
- приложения обмениваются данными с удаленными серверами.

6.2 Типы удаленных атак

Существует множество специальных методов, позволяющих злоумышленникам подвергнуть риску удаленные системы. Среди этих методов можно выделить несколько категорий.

6.2.1 DoS-атаки

DoS (Denial of Service, отказ в обслуживании) – попытка создать условия, при которых компьютер или сеть становятся недоступными для легитимных пользователей. Обмен данными между пораженными пользователями затрудняется, его дальнейшая функциональность невозможна. Чтобы восстановить работоспособность, подвергнутым DoS-атакам компьютерам требуется перезагрузка.

В большинстве случаев объектами таких атак являются веб-сервера, а цель заключается в прекращении их доступности для пользователей на определенный период времени.

6.2.2 DNS Poisoning

Метод «отравления DNS» (Domain Name Server, система доменных имен) позволяет злоумышленникам ввести DNS-сервер любого компьютера в заблуждение и заставить его принять поддельные данные за подлинные. Поддельные сведения кэшируются в течение определенного срока, позволяя злоумышленникам перезаписывать DNS-ответы IP-адресов. В итоге пользователи, пытающиеся получить доступ к веб-сайтам в интернете, вместо исходного содержимого скачивают компьютерные вирусы и черви.

6.2.3 Атаки червей

Компьютерный червь – программа, содержащая вредоносный программный код, совершающая атаки на хост-компьютеры и распространяющаяся по сети. Сетевые черви эксплуатируют уязвимость системы безопасности в различных приложениях. Благодаря широкой доступности интернета они распространяются по всему миру за считанные часы с момента выпуска, а в некоторых случаях и в пределах нескольких минут.

Атак большинства червей (Sasser, SqlSlammer) можно избежать, используя стандартные настройки безопасности файервола или блокируя незащищенные и неиспользуемые порты. Кроме того, важную роль играет обновление системы и установка новых «заплат» безопасности.

6.2.4 Сканирование портов

Сканирование портов отслеживает наличие открытых компьютерных портов на хост-компьютере сети. Сканер портов представляет собой ПО, в котором реализован поиск таких портов.

Компьютерный порт – виртуальная точка, в которой происходит обработка входящих и исходящих данных, – представляет собой ключевой элемент с точки зрения безопасности. В крупных сетях сведения, собранные сканерами портов, позволяют определить потенциальные уязвимые места. Такое использование является легитимным.

Однако злоумышленники часто используют сканирование портов с целью подвергнуть безопасность системы риску. Свои действия они начинают с отправки пакетов на каждый порт. В зависимости от типа ответа можно определить порты, находящиеся в эксплуатации. Само по себе сканирование не представляет опасности, но позволяет обнаружить потенциально уязвимые места и предоставляет злоумышленникам возможность перенять управление удаленными компьютерами.

Администраторам сети рекомендуется блокировать неиспользуемые порты и обеспечить защиту используемых портов от несанкционированного доступа.

6.2.5 Десинхронизация TCP-соединения

Десинхронизация TCP-соединения – метод, используемый для «захвата» TCP-соединения.

Действие запускается процессом, в котором номер последовательности во входящих пакетах отличается от ожидаемого. Пакеты с непредвиденным номером последовательности отклоняются (или сохраняются в буферной памяти, если они находятся в текущем окне обмена данными).

В состоянии десинхронизации обе сообщающиеся конечные точки

отклоняют полученные пакеты. Именно в этот момент удаленные злоумышленники могут осуществить проникновение и предоставить пакеты с верным номером последовательности. Злоумышленники могут даже повлиять на обмен данными с помощью своих команд или изменить его каким-либо другим образом.

Атаки на «захват» TCP-соединения нацелены на обрыв сообщения между клиентом и сервером или между одноранговыми узлами. Применение проверки подлинности к каждому TCP-сегменту позволяет избежать многих атак. Целесообразно также придерживаться рекомендованных настроек сетевых устройств.

6.2.6 Утилиты SMB Relay

SMBRelay и SMBRelay2 – специальные программы с возможностью применения атаки к удаленным компьютерам. Программы используют сетевой файловый протокол SMB (Server Message Block, блок сообщений сервера), дополняющий протокол нижнего уровня NetBIOS. Если пользователь открывает свои папки для общего доступа в локальной сети, то при этом, скорее всего, используется именно данный сетевой файловый протокол.

При передаче данных в локальной сети происходит обмен хэшами паролей.

Утилита SMBRelay получает подключение на UDP-порт 139 и 445, удерживает пакеты, пересылаемые между клиентом и сервером, и изменяет их. После подключения и проверки подлинности клиент отключается. Утилита SMBRelay создает новый виртуальный IP-адрес. Доступ к новому \ адресу возможен при помощи команды «net use \\192.168.1.1». Этот адрес затем может быть использован любой сетевой функцией Windows. Утилита SMBRelay перехватывает передачу данных по SMB-протоколу, исключая этапы согласования и проверки подлинности. После этого удаленные злоумышленники могут использовать полученный IP-адрес до тех пор, пока компьютер-клиент не будет отключен.

Принцип действия программы SMBRelay2 аналогичен программе SMBRelay. Отличие заключается в использовании не IP-адресов, а имен NetBIOS. Обе программы могут реализовывать так называемые «атаки посредника» (man-in-the-middle). Эти атаки позволяют удаленным злоумышленникам незаметно считывать, вставлять и изменять сообщения, пересылаемые между двумя сообщающимися конечными точками. Компьютеры, подвергнутые таким атакам, часто перестают реагировать или производят непредвиденную перезагрузку.

Во избежание атак рекомендуется использовать пароли или ключи для проверки подлинности.

6.2.7 ICMP-атаки

ICMP (Internet Control Message Protocol, межсетевой протокол управляющих сообщений) – популярный и широко используемый интернет-протокол. Данный протокол используется в основном компьютерами, объединенными в сеть, для отправки различных сообщений об ошибках.

Удаленные злоумышленники предпринимают попытку использовать недостатки ICMP-протокола. ICMP-протокол предназначен для односторонней передачи данных и не требует проверки подлинности. Это позволяет удаленным злоумышленникам инициировать так называемые DoS-атаки (отказ в обслуживании) или атаки, предоставляющие несанкционированный доступ к входящим и исходящим пакетам.

Типичными примерами ICMP-атак являются ping-флуд, флуд ICMP_ECHO и smurf-атаки. Компьютеры, подвергнутые ICMP-атакам, отличаются снижением производительности (это относится ко всем приложениям, использующим интернет) и затруднениями при подключении к интернету.

6.3 Электронная почта

Электронная почта представляет собой современный способ обмена данными, обладающий определенными преимуществами. Это средство обеспечивает гибкую, быструю и прямую передачу данных. В начале 1990-х гг. электронная почта играла решающую роль в распространении интернета.

К сожалению, вследствие высокого уровня анонимности электронная почта и интернет открывают возможности для нелегальных действий, например отправки незатребованных сообщений. В общей классификации в спаме выделяют незатребованную рекламу, письма-мистификации и распространение вредоносного ПО. Неудобство и опасность для пользователя увеличиваются в связи с практическим отсутствием затрат на отправку таких сообщений и наличием у создателей спама различных инструментов и источников получения новых адресов электронной почты. Кроме того, объемы и разнообразие спама затрудняют контроль над ним. Чем дольше используется

адрес электронной почты, тем выше вероятность попадания в базы данных спам-машин. Следующие советы позволяют предотвратить этот риск:

- по возможности избегать публикации адреса электронной почты в интернете;
- сообщать свой адрес электронной почты только доверенным лицам;
- по возможности не использовать распространенные псевдонимы: чем сложнее псевдоним, тем ниже вероятность его отслеживания;
- не отвечать на спам-сообщения, уже находящиеся в папке входящих сообщений;
- соблюдать осторожность при заполнении интернет-формуляров: особенно внимательно нужно относиться к установке флагов типа «Да, я хочу получать информацию о...» (Yes, I want to receive information about... in my inbox);
- использовать «специализированные» адреса электронной почты для рабочей переписки, связи с друзьями и т. п.;
- время от времени изменять адрес электронной почты;
- использовать решения по защите от спама.

6.3.1 Рекламные материалы

интернет-реклама представляет собой одну из наиболее быстро растущих форм предоставления рекламы. Для рекламы по электронной почте в качестве средства связи используется электронная почта. Основные преимущества таких маркетинговых действий заключается в минимальных затратах, высоком уровне направленности и эффективности; кроме того, доставка сообщений происходит практически мгновенно. Многие компании используют средства для проведения маркетинговых кампаний по электронной почте в качестве эффективного средства связи с имеющимися и потенциальными клиентами.

Этот метод рекламы законен, поскольку пользователь может быть заинтересован в получении коммерческих сведений о тех или иных продуктах.

В действительности многие компании рассылают незатребованные массовые сообщения коммерческого характера. В таких случаях реклама по электронной почте попадает в категорию спама.

Количество спама растет, что становится настоящей проблемой. Авторы незатребованных сообщений электронной почты, конечно, стараются замаскировать спам под видом легитимных сообщений. С другой стороны, даже законная реклама в больших количествах может вызвать отрицательную реакцию.

6.3.2 Мистификации

Мистификация (hoax) – сообщение, распространяемое в интернете. Обычно оно отправляется по электронной почте, но иногда привлекаются и коммуникационные инструменты типа ICQ и Skype. Само по себе сообщение часто является шуткой или выдумкой.

Компьютерные вирусы этой категории нацелены на пробуждение у получателей чувства страха, неопределенности и сомнений, убеждение их в наличии «неопределяемого вируса», удаляющего файлы и перехватывающего пароли, либо применение других вредоносных действий в отношении системы.

Целью некоторых сообщений-мистификаций является вызов эмоционального замешательства. Получателей просят переслать сообщение по всем имеющимся контактам, что продлевает жизненный цикл данной мистификации. Существуют также мистификации, передаваемые посредством мобильных телефонов, просьбы о помощи, предложение

денежных сумм из-за границы и т. д. В большинстве случаев отследить намерения авторов таких сообщений невозможно.

В принципе, сообщение, предлагающее пересылку по всем возможным контактам, с большой долей вероятности является мистификацией. В интернете существует множество специализированных сайтов, позволяющих проверить легитимность сообщения электронной почты. Перед пересылкой сообщения, которое кажется вам мистификацией, выполните по нему поиск в интернете.

6.3.3 Фишинг

Термин «фишинг» определяет преступную деятельность с применением методов социотехники (манипулирование пользователями с целью получения конфиденциальных сведений). Целью этих действий является получение доступа к важным данным: номерам банковских счетов, ПИН-кодам и т. п.

Для достижения этой цели пользователю отправляется электронное письмо от лица, выдающего себя за доверенное лицо или бизнес-партнера (финансовый институт, страховую компанию). Электронное сообщение при этом выглядит неподдельным и содержит графические элементы и содержимое, которые могли быть получены от источника, за который выдает себя отправитель сообщения. Под различными предлогами (проверка данных, финансовые операции) пользователя просят ввести некоторые личные данные: номера банковских счетов, имя пользователя, пароли. Такие данные, в случае их предоставления, могут быть перехвачены и использованы не по назначению.

Следует отметить, что банки, страховые компании и другие законные компании никогда не запрашивают имена пользователей и пароли в незатребованных сообщениях электронной почты.

6.3.4 Определение мошенничества с использованием спама

В принципе, определить спам (незатребованные письма) в папке входящих сообщений можно по нескольким признакам. Если сообщение соответствует хотя бы некоторым критериям из перечисленных далее, оно с большой долей уверенности является спамом:

- адрес отправителя не принадлежит лицам из вашего списка контактов;
- вам предлагаются крупные денежные суммы при условии предварительной отправки вами небольшой суммы;
- под различными предлогами (проверка данных, финансовые операции) вас просят ввести некоторые личные данные: номера банковских счетов, имя пользователя, пароли и т. д.;
- сообщение составлено на иностранном языке;
- вам предлагается продукт, в котором вы не заинтересованы. Если вы все же решаете совершить покупку, убедитесь, что отправитель сообщения является надежным продавцом (проконсультируйтесь с производителем продукта);
- некоторые слова содержат орфографические ошибки с целью обхода спам-фильтра, например, «ваигра» вместо «виагра» и т. д.

6.3.4.1 Правила

В контексте решений защиты от спама и почтовых клиентов под «правилами» понимаются инструменты для управления операциями с электронными сообщениями. Правила состоят из двух логических частей:

1. Условие (например, входящее сообщение с определенного адреса);
2. Действие (например, удаление сообщения, перемещение его в определенную папку).

Количество и комбинация правил зависит от решения, обеспечивающего защиту от спама. Эти правила выполняют роль мер защиты от спама (незатребованных электронных сообщений). Типичные примеры:

1. Условие: входящее сообщение содержит некоторые слова, типичные для незатребованных сообщений.
2. Действие: удалить сообщение.

1. Условие: входящее сообщение содержит приложение с расширением EXE.
2. Действие: удалить приложение и доставить сообщение в папку входящих сообщений.

1. Условие: входящее сообщение, отправленное работодателем.
2. Действие: переместить сообщение в папку «Работа».

В программах, защищающих от незатребованных сообщений электронной почты, рекомендуется использовать комбинацию правил, что позволяет упростить администрирование и повысить производительность спам-фильтров.

6.3.4.1 Фильтр Бейеса

Фильтрация спама по методу Бейеса – эффективное средство фильтрации электронной почты, используемое почти во всех продуктах защиты от спама. Этот метод позволяет определять незатребованные сообщения электронной почты с высокой степенью точности. Фильтр Бейеса может быть настроен для отдельных пользователей.

Функциональность базируется на следующем принципе. На первом этапе осуществляется процесс обучения. Пользователь вручную отмечает достаточное количество сообщений как легитимные или как спам (обычно 200/200(?)). Фильтр анализирует обе категории и запоминает, например, что в незатребованных сообщениях часто содержатся слова «rolex» или «viagra», а легитимные сообщения отправляются членами семьи или с адресов, входящих в список контактов пользователя. При условии обработки еще большего количества сообщений фильтр Бейеса может присвоить каждому сообщению определенный «спам-индекс» и на его основе определить принадлежность сообщения к спаму.

Основное преимущества этого метода заключается в его гибкости. Так, например, для пользователя-биолога всем входящим сообщениям, имеющим отношение к биологии или родственным областям науки, будет присвоен невысокий индекс вероятности. Если сообщение содержит слова, которые при других условиях были бы рассчитаны как незатребованные, но было отправлено пользователем из списка контактов, оно будет отмечено как легитимное, поскольку отправители из списка контактов снижают общую вероятность спама.

6.3.4.2 «Белый список»

«Белый список» представляет собой список таких объектов или лиц, которые могут быть приняты или которым был предоставлен доступ. Термин «белый список электронной почты» определяет список контактов, сообщения от которых пользователь согласен получать. Такие «белые списки» основаны на поиске ключевых слов в адресах электронной почты, именах доменов и IP-адресах.

Если «белый список» настроен на «исключающий режим», то все письма, отправленные с других адресов, доменов или IP-адресов, получены не будут. С другой стороны, в неисключающем режиме такие сообщения не удаляются, а отфильтровываются другим способом.

Принцип работы «белого списка» противоположен «черному списку». По сравнению с «черными списками», «белые списки» более просты в управлении.

Чтобы обеспечить наиболее производительную фильтрацию спама, рекомендуется использовать как «белый», так и «черный» списки.

6.3.4.3 «Черный список»

В принципе, «черный список» представляет собой список недопустимых или запрещенных объектов или лиц. В виртуальном мире это метод, позволяющий принимать сообщения от всех пользователей, не входящих в такой список.

Существует два типа «черных списков». В программах по защите от спама пользователи могут создавать собственные «черные списки». Помимо этого, в интернете можно найти множество профессиональных, регулярно обновляемых «черных списков», созданных специализированными институтами.

Принцип составления «черного списка» противоположен составлению «белого списка». Использование «черных списков» является существенным компонентом в блокировании спама, но их поддержка затрудняется ежедневным появлением новых объектов, которые должны

быть заблокированы. Чтобы обеспечить наиболее производительную фильтрацию спама, рекомендуется использовать как «белый», так и «черный» списки.

6.3.4.5 Управление на стороне сервера

Управление на стороне сервера представляет собой метод определения массовых незатребованных сообщений на основе ряда полученных сообщений и реакции пользователей на них. В зависимости от содержимого, каждое сообщение оставляет на сервере уникальный цифровой «след». В действительности это уникальный идентификационный номер, который не содержит никаких сведений о содержимом сообщения. У двух идентичных сообщений будут идентичные «следы», тогда как «следы» различных сообщений будут отличаться.

Если сообщение помечается как спам, его след отправляется на сервер. Если сервер получает несколько идентичных следов (соответствующих определенному спам-сообщению), след сохраняется в базе данных следов спама. При сканировании входящих сообщений программа отправляет следы сообщений на сервер. Сервер возвращает сведения о том, какие следы соответствуют сообщениям, уже отмеченным пользователями как спам.