ESET NOD32 Антивирус

Интегрированные компоненты:
Антивирус ESET NOD32
Приложение для антишпионской защиты ESET NOD32

Руководство пользователя

we protect your digital world

Содержание

ESET NOD32 Антивирус

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. Антивирус ESET NOD32

Антивирусное приложение ESET NOD32 – это преемник популярной антивирусной системы ESET NOD32. Быстродействие антивируса ESET NOD32 обусловлено применением последней версии ядра сканирования ThreatSense®.

Реализованные расширенные методы гарантируют проактивное предотвращение проникновения вирусов, шпионских и троянских программ, червей, рекламного ПО и руткитов без снижения производительности системы или нарушения работы компьютера.

1.1 Новые возможности

В результате длительной работы наших экспертов разработана совершенно новая архитектура программы ESET NOD32, которая гарантирует максимальный уровень обнаружения угроз при минимальных требованиях к системе.

– Защита от вирусов и шпионских программ

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

Характеристика	Описание
Улучшенная очистка	Теперь «интеллектуальная» антивирусная система способна без вмешательства пользователя очищать файлы и удалять большинство из обнаруженных вирусов, проникших в систему.
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.

1.2 Системные требования

Для бесперебойной работы антивирусного приложения ESET NOD32 система должна удовлетворять следующим программным и аппаратным требованиям.

- **Антивирус ESET NOD32:**

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)

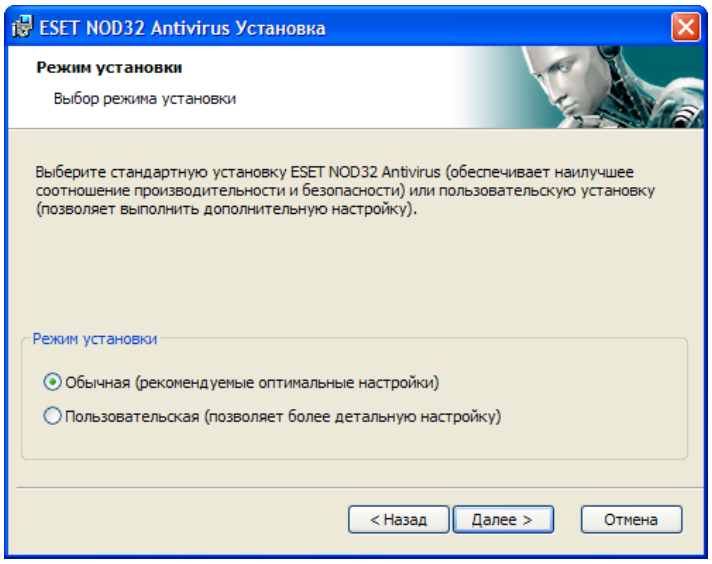
- **Антивирус ESET NOD32, версия для корпоративных клиентов:**

Windows 2000, XP	400 МГц 32-разрядный / 64-разрядный (x86 / x64) процессор 128 МБ оперативной памяти 35 МБ свободного пространства Super VGA (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)

2. Установка

После приобретения лицензии программу установки антивируса ESET NOD32 можно загрузить в виде MSI-пакета с веб-сайта компании ESET. Запустите программу установки и задайте основные настройки, следуя указаниям мастера установки. Доступны два типа установки, различающиеся уровнем детализации настройки:

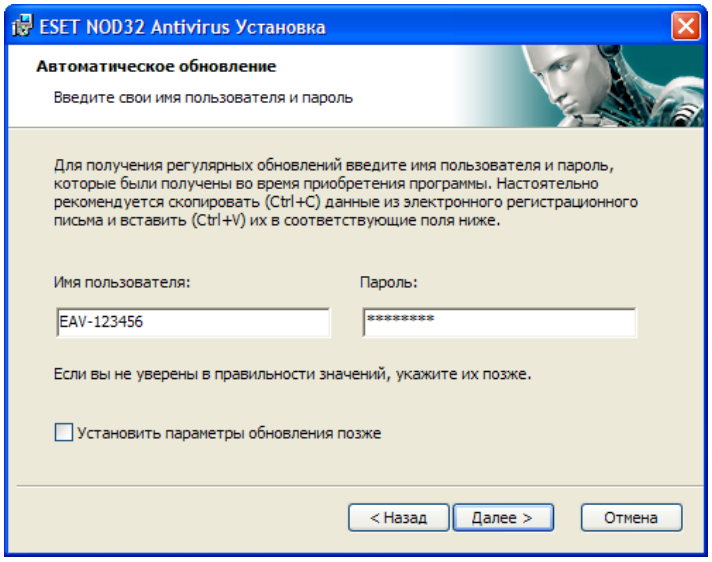
- обычная установка,
- выборочная установка.



2.1 Обычная установка

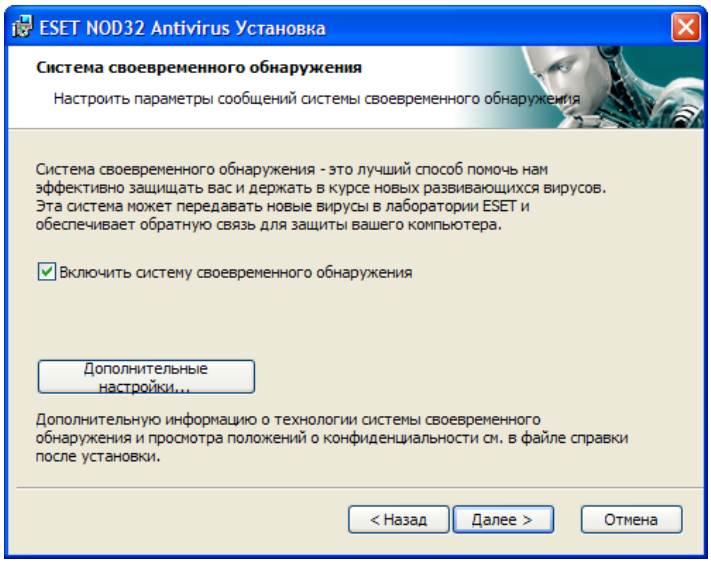
Обычная установка рекомендована для пользователей, желающих установить ESET NOD32 Антивирус с настройками по умолчанию. Этот вариант обеспечивает максимальный уровень защиты и удобства

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.



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

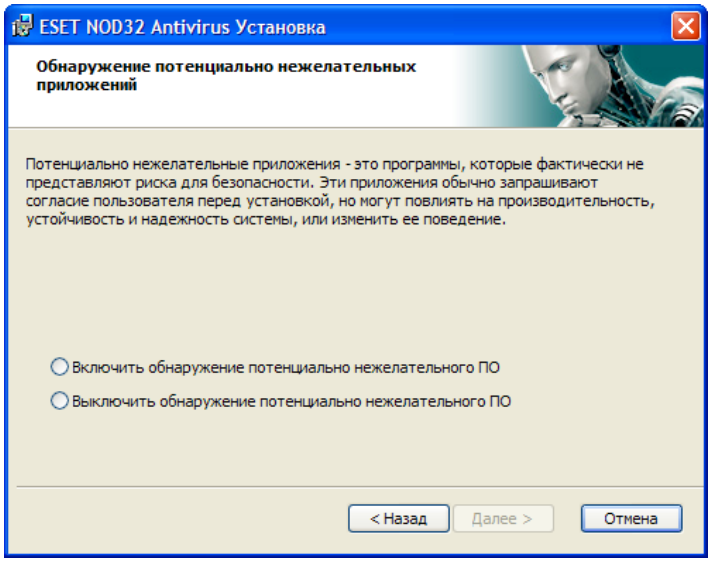
Следующий шаг установки – настройка системы раннего оповещения ThreatSense.NET. Система раннего оповещения ThreatSense.NET помогает обеспечивать незамедлительное и регулярное оповещение компании ESET о новых угрозах, что дает возможность своевременно защищать пользователей. Система позволяет передавать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



По умолчанию флажок **Включить систему раннего 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.

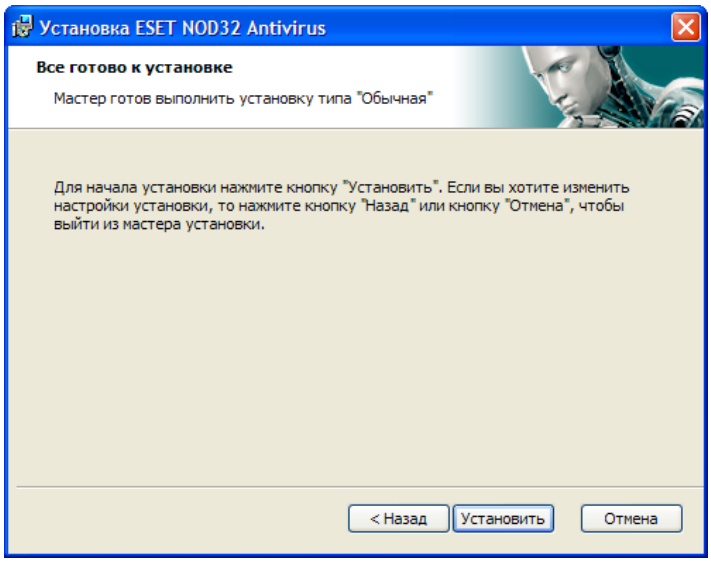
Следующий шаг установки – определение настроек для функции **Обнаружение потенциально нежелательных приложений** (Detection of potentially unwanted applications). Потенциально нежелательные приложения не всегда преднамеренно вредоносны, но могут негативно влиять на поведение системы.

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.



Отмеченный пункт **Включить обнаружение потенциально нежелательных приложений** (Enable detection of potentially unwanted applications) позволяет программе ESET NOD32 Антивирус выявлять угрозы данного типа (рекомендовано).

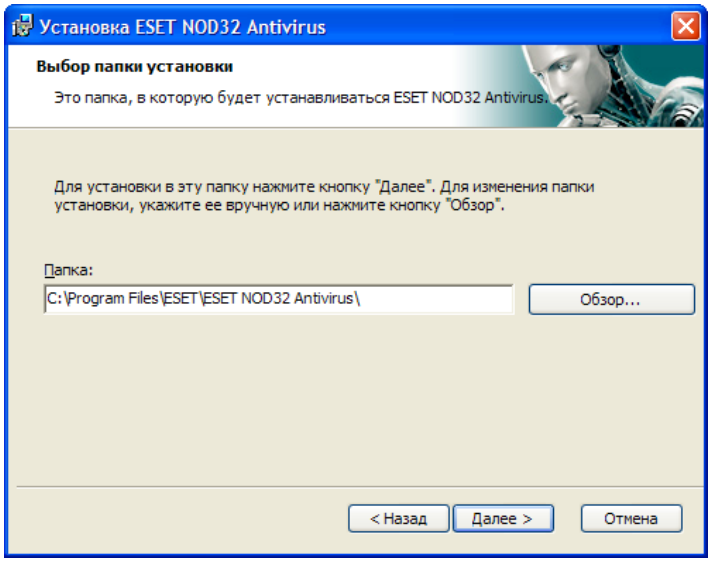
Последний шаг установки в обычном режиме – подтверждение установки нажатием кнопки **Установить** (Install).



2.2 Выборочная установка

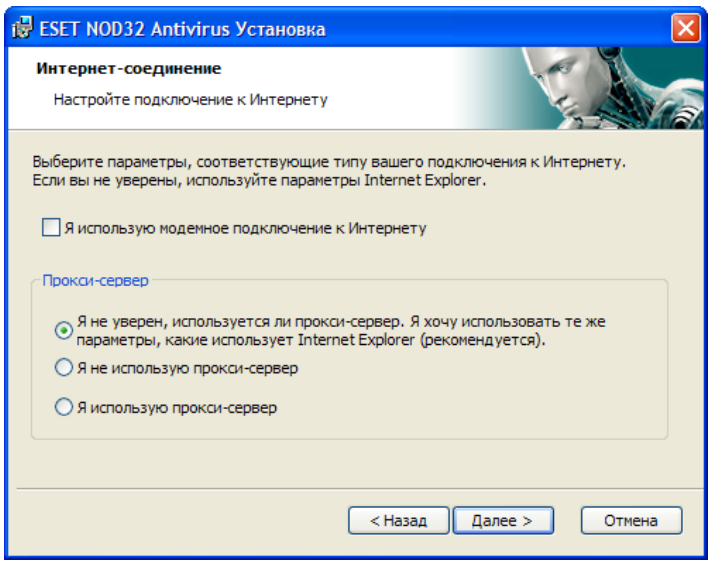
Выборочная установка разработана для пользователей, имеющих опыт в тонкой настройке программ и желающих вносить изменения в расширенные настройки в ходе установки.

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

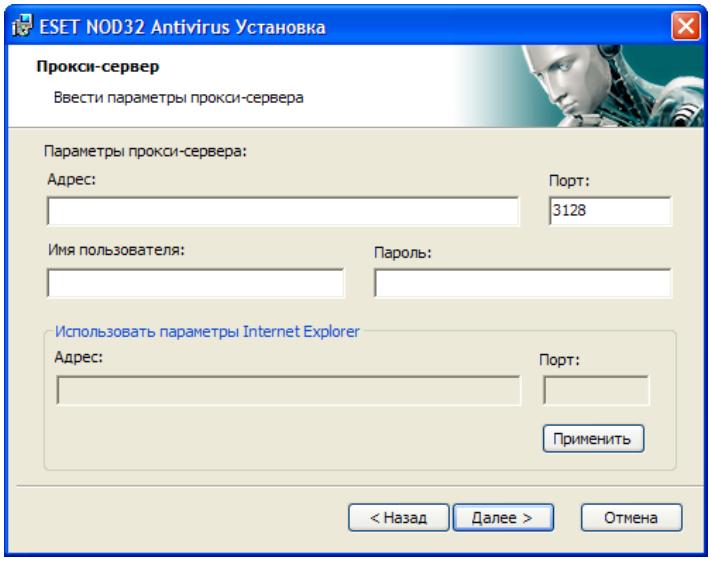


Затем потребуется ввести имя пользователя и пароль. Этот шаг аналогичен действиям при обычной установке (см. страницу 5).

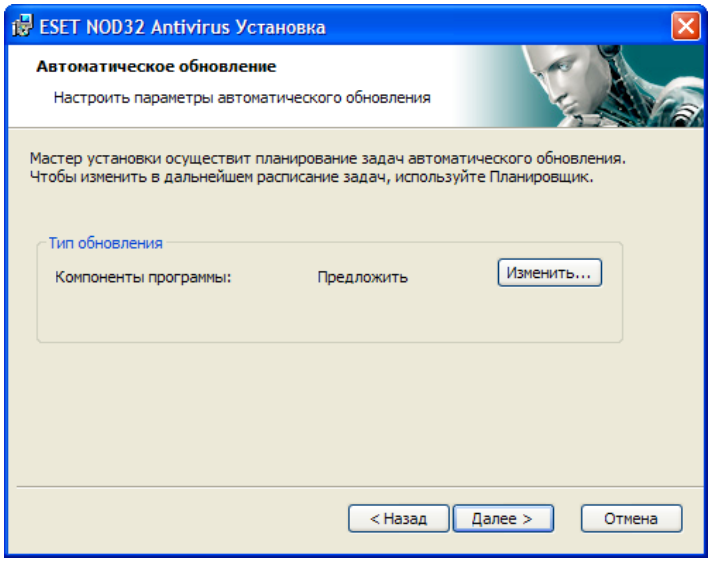
После ввода имени пользователя и пароля нажмите кнопку **Далее** (Next), чтобы перейти к окну **Настройка подключения к Интернету** (Configure your Internet connection).



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 парамеры, какие использует Internet Explorer (рекомендуется)** (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.

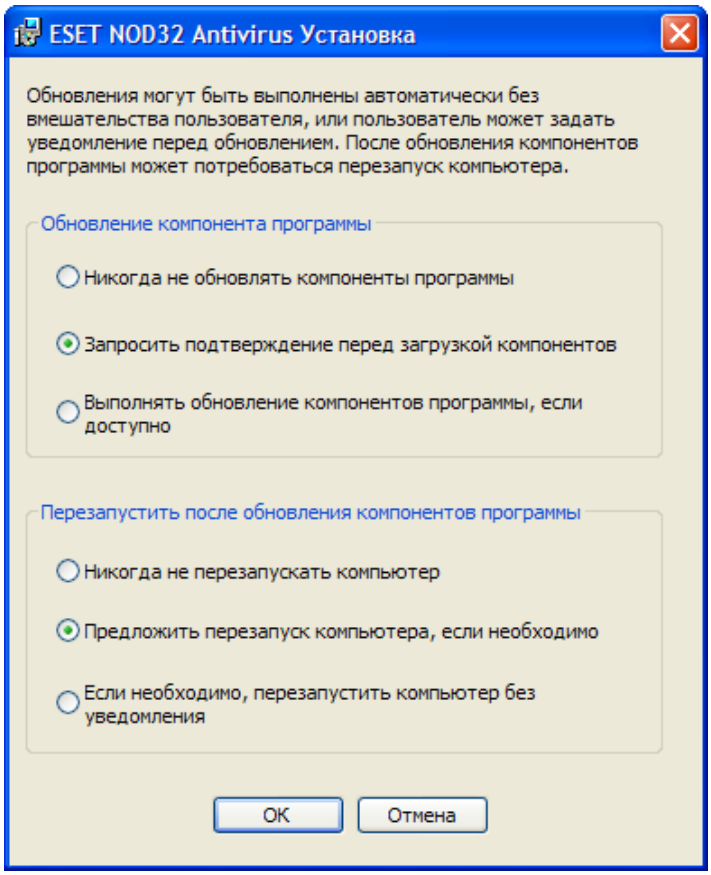


Для настройки установок своего прокси-сервера выберите пункт **Я использую прокси-сервер** (I use a proxy server) и нажмите кнопку **Далее** (Next). Введите IP- или URL-адрес вашего прокси-сервера в поле **Адрес** (Address:). В поле **Порт** (Port) укажите порт подключения к прокси-серверу (по умолчанию 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.



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

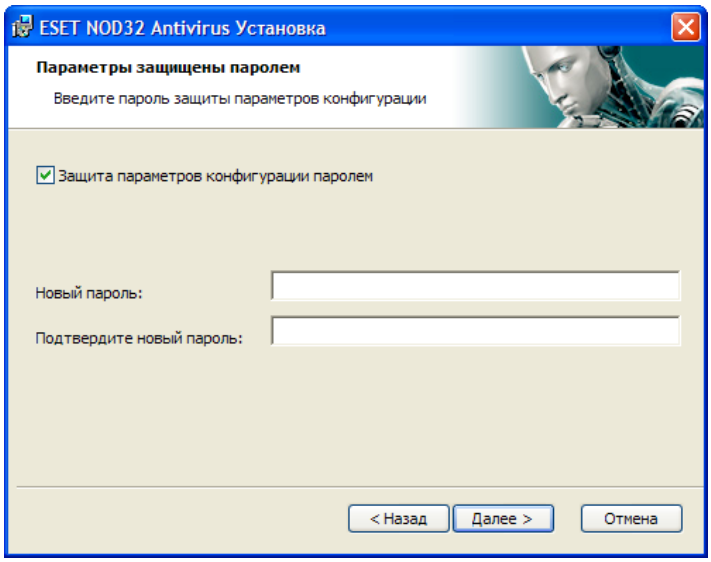
Чтобы отказаться от обновления компонентов программы, выберите пункт **Никогда не обновлять компоненты программы** (Never update program components). Если включена опция **Запросить подтверждение перед загрузкой компонентов** (Ask before downloading program components), перед загрузкой компонентов программ будет выводиться окно подтверждения. Для автоматической загрузки обновления компонентов программ 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.

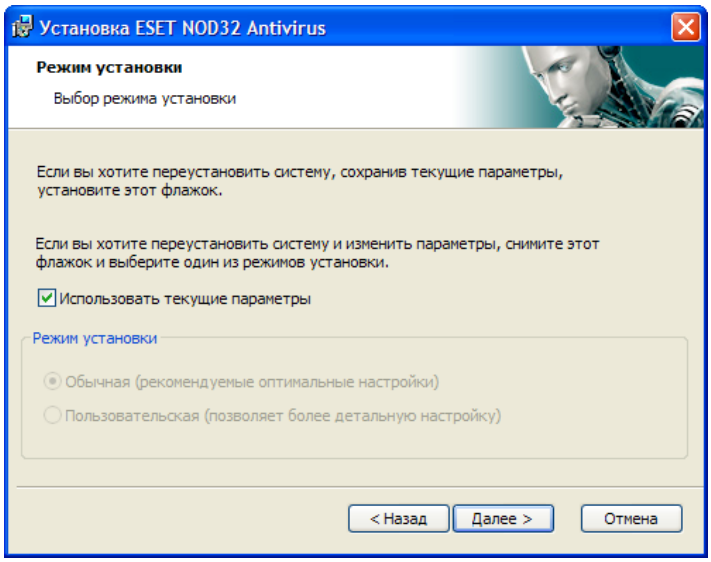
Шаги **Настройка системы раннего оповещения ThreatSense.NET** (Configuration of the ThreatSense.Net Early Warning System) и **Обнаружение потенциально нежелательных приложений** (Detection of potentially unwanted applications) выполняется так же, как и при обычной установке (см. страницу 5).



На последнем шаге выводится окно с запросом подтверждения установки программы.

2.3 Использование текущих настроек

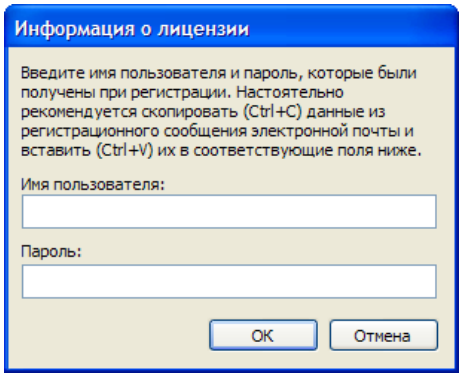
При переустановке ESET NOD32 Антивируса предлагается **Использовать текущие настройки** (Use current settings). Выберите эту опцию для переноса параметров настройки из предыдущей установки.



2.4 Ввод имени пользователя и пароля

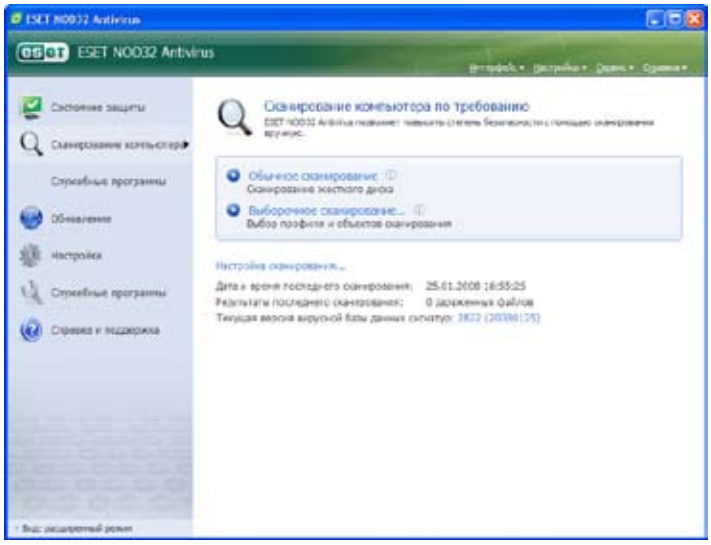
Для оптимальной работы важно, чтобы компоненты программы периодически обновлялись. Это возможно, только если в настройках обновления указаны действующие имя пользователя и пароль.

Если имя пользователя и пароль не были введены при установке, это можно сделать во время работы. В главном окне программы нажмите кнопку **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 запросу

После установки ESET NOD32 Антивируса необходимо провести сканирование компьютера на наличие вредоносного программного кода. Для быстрого запуска сканирования выберите в основном меню команду **Сканирование компьютера** (Computer scan), а затем, в основном окне программы, – команду **Обычное сканирование** (Standard scan). Дополнительные сведения о сканировании компьютера см. в главе «Сканирование компьютера» (Computer scan).



3. Руководство для начинающих

Эта глава содержит описание ESET NOD32 Антивирус и базовые настройки.

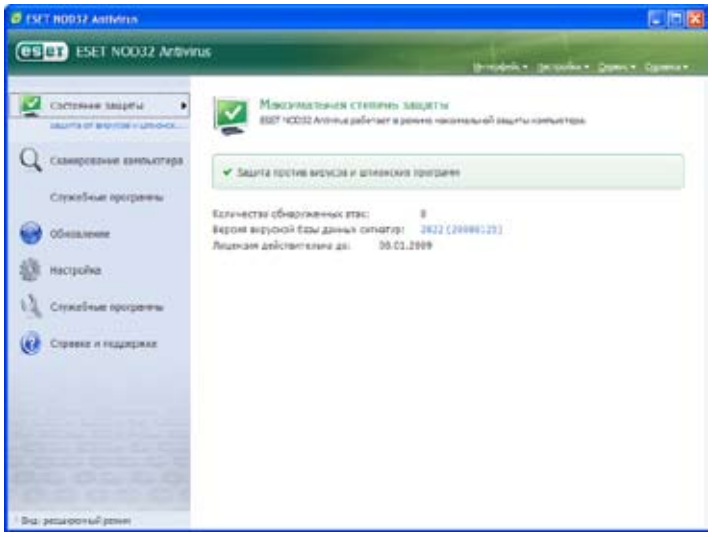
3.1 Описание пользовательского интерфейса – режимы

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

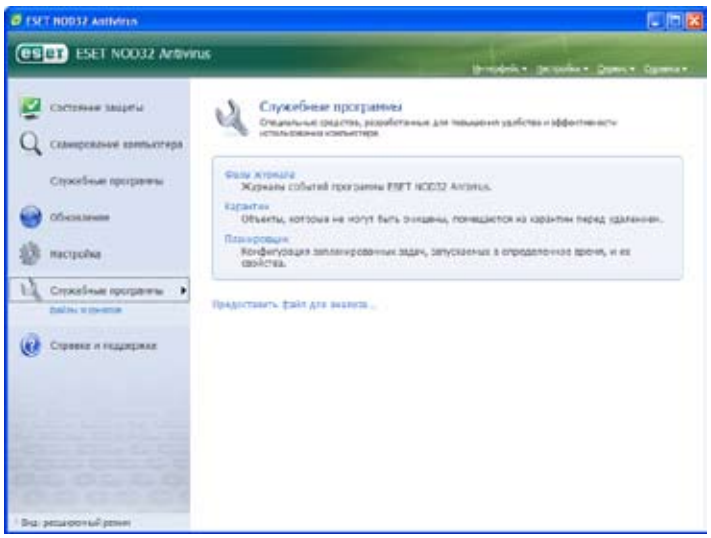
Ниже описаны кнопки основного меню:

- **Состояние защиты** (Protection status) – информация о состоянии защиты ESET 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.
- **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 помощью этого раздела вы можете просматривать справочные файлы, базу данных и веб-страницу ESET, а также отправлять запросы в техническую поддержку.

Пользовательский интерфейс ESET NOD32 Антивирус позволяет переключаться между стандартным и расширенным режимами. Для того чтобы выбрать необходимый режим, щелкните по индикатору режима отображения в нижнем левом углу основного окна ESET NOD32 Антивирус.



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

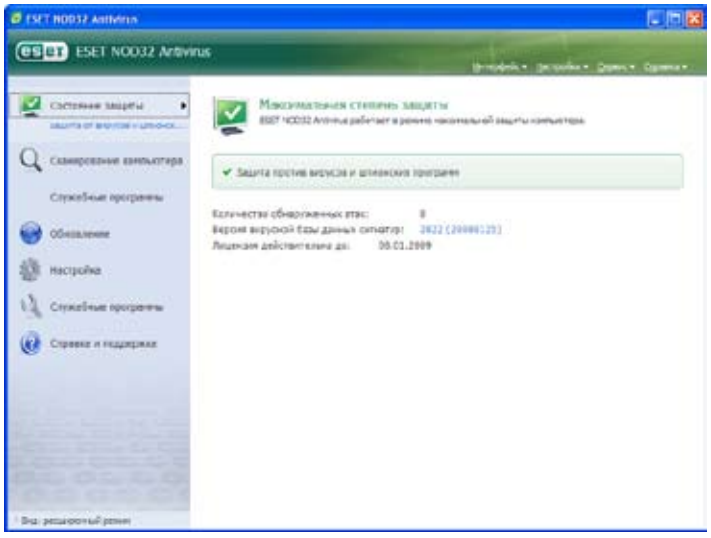


При переключении в расширенный режим в основном меню появляется опция **Инструменты** (Tools). Благодаря ей пользователь получает доступ к опциям планировщика, к области карантина и файлам журнала ESET NOD32 Антивируса.

Примечание. Остальные инструкции настоящего руководства относятся к расширенному режиму.

3.1.1 Проверка работы системы

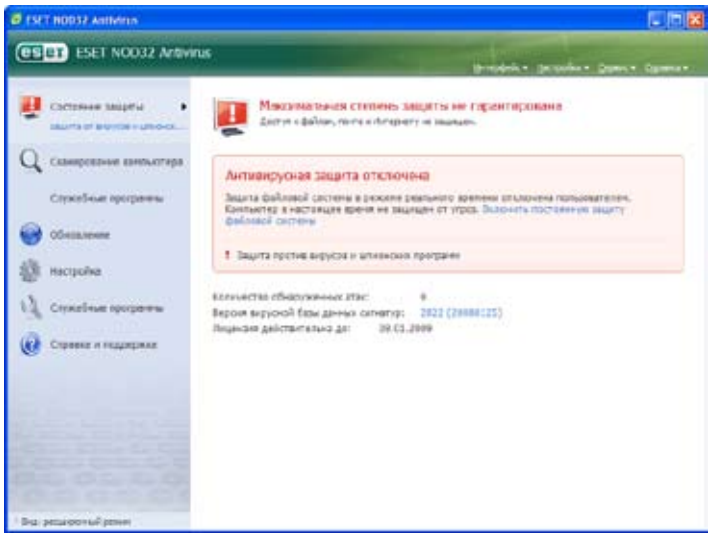
Чтобы просмотреть **Состояние защиты** (Protection status), щелкните по этой опции в верхней части основного меню. Непосредственно под этим пунктом появится подменю З**ащита против вирусов и шпионских программ** (Antivirus and antispyware), а в основном программном окне будут отображены краткие сведения о статусе работы ESET NOD32 Антивируса. Щелкнув пункт меню **Защита против вирусов и шпионских программ** 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. Чтобы изменить статус отдельных модулей, выберите в основном меню команду **Настройка** (Setup), щелкните по модулю, который необходимо изменить.

3.1.2 Что делать, если программа работает неправильно

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

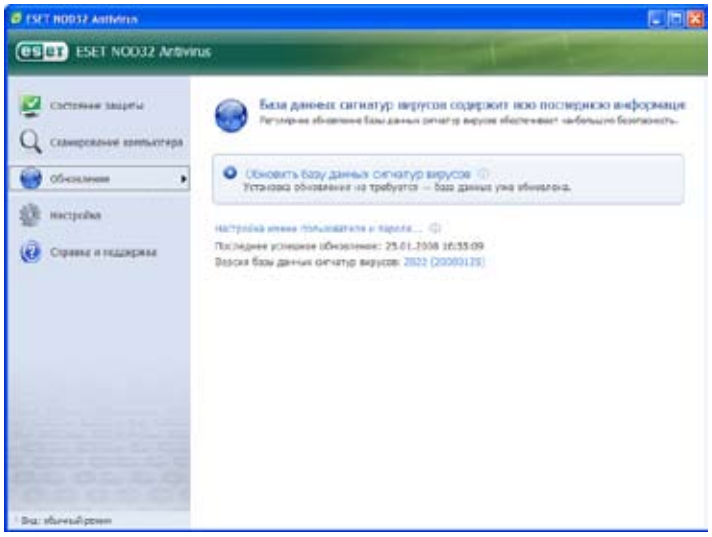


Если в представленном списке известных проблем и способов их решения нет вашей, выберите опцию **Справка и поддержка** (Help and support) для поиска информации в справочных файлах и базе данных. Если найти решение все равно не получается, вы можете отправить запрос в службу технической поддержки ESET.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

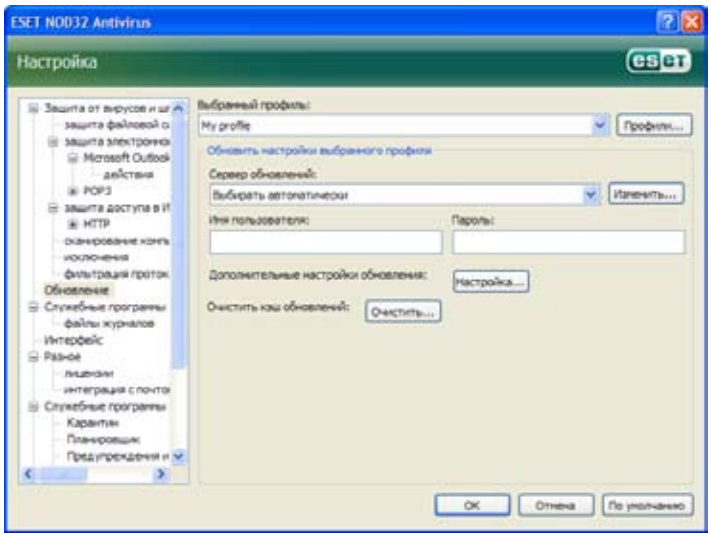
3.2 Настройка обновлений

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 Антивируса, то на данном этапе этого делать не требуется.

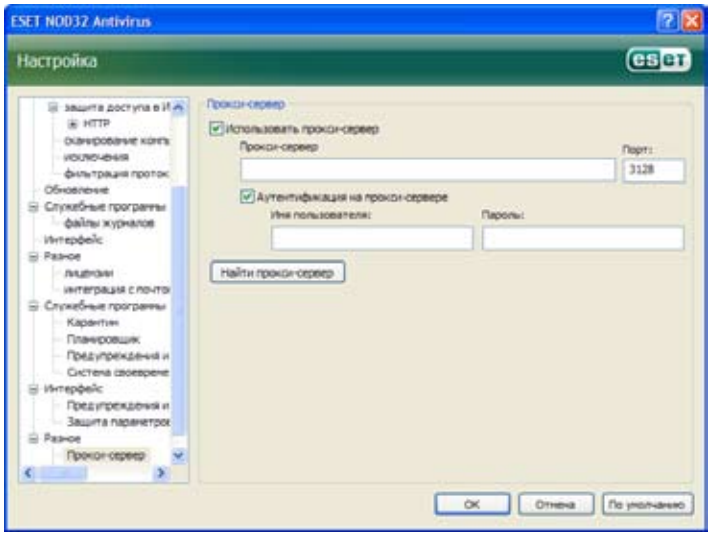


В окне **Расширенная настройка** (Advanced Setup) (для доступа к нему нажмите клавишу F5) представлены другие опции обновлений. В раскрывающемся меню **Обновление** (Update server) должна быть выбрана команда **Выбрать автоматически** (Choose automatically). Для настройки расширенных опций обновления: обновления режима, доступа к прокси-серверу, подключения к обновлениям на локальном сервере и создания копий вирусных сигнатур (ESET NOD32 Business Edition), нажмите кнопку **Настройка** (Setup).



3.3 Настройка прокси-сервера

Если вы используете прокси-сервер для выхода в Интернет в системе, использующей ESET NOD32 Антивирус, он должен быть обозначен в **Расширенных настройках** (F5). Чтобы в соответствующем окне конфигурации настроить **Прокси-сервер** (Proxy server), из дерева расширенной настройки выберите команды **Разное** – **Прокси-сервер** (Miscellaneous – Proxy server). Установите флаг **Использовать прокси-сервер** (Use proxy server), затем введите IP адрес, номер порта прокси-сервера и аутентификационные данные для него.



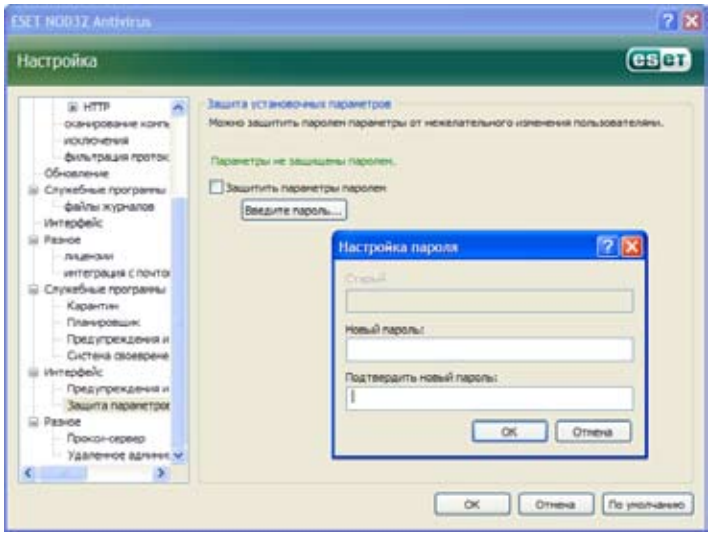
При отсутствии данной информации нажмите кнопку **Найти прокси-сервер** (Detect proxy server), чтобы автоматически определить настройки прокси-сервера для ESET NOD32 Антивирус.

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

3.4 Защита настроек

Настройки антивируса ESET NOD32 Антивирус очень важны с точки зрения политики безопасности вашей организации. Несанкционированное изменение настроек может представлять угрозу для стабильности и безопасности вашей системы. Чтобы защитить параметры настроек паролем, выберите команды **Настройка** – **Дополнительные настройки**... – **Интерфейс** – **Защита параметров** (Setup – Enter entire advanced setup tree... – User interface – Settings protection) и нажмите кнопку **Введите пароль**... (Enter password).

Введите пароль, подтвердите его повторным вводом и нажмите кнопку **OK** (OK). В дальнейшем для изменения настроек ESET NOD32 Антивирус нужно будет ввести данный пароль.



4. Работа с антивирусом ESET NOD32

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 запускается при различных событиях. При контроле используются методы обнаружения 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

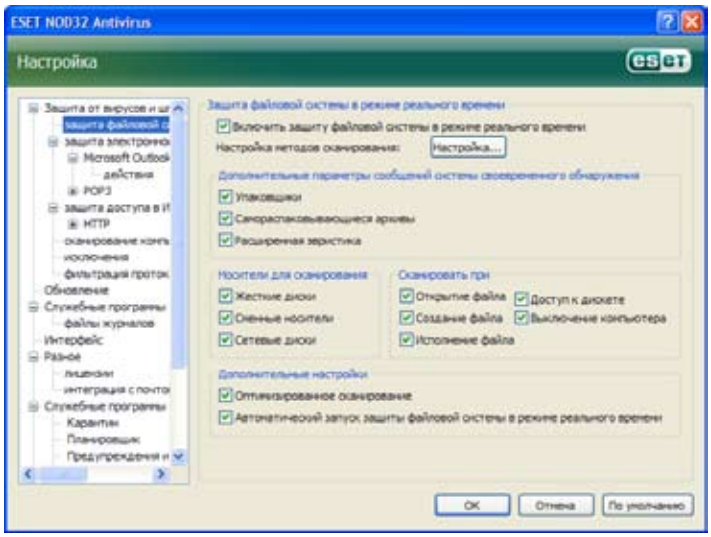
По умолчанию сканируются все носители, которые могут содержать потенциальную угрозу.

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 изменять их только в определенных случаях. Так, например, при сканировании отдельных носителей значительно замедляется передача данных.



4.1.1.1.2 Сканирование по событию

По умолчанию все файлы сканируются при открытии, создании и исполнении. Рекомендуется сохранить настройки «по умолчанию», чтобы обеспечить, таким образом, 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 загрузочными секторами жесткого диска 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 таких файлов программой используются дополнительные параметры сканирования. Помимо основных методов, основанных на вирусных сигнатурах,применяются расширенные эвристики, что позволяет значительно увеличить эффективность обнаружения. Кроме новых созданных файлов сканированию подвергаются самораскрывающиеся архивы (SFX) и вызывающие упаковщики (внутренне сжатым исполняемым файлам).

4.1.1.1.4 Расширенная настройка

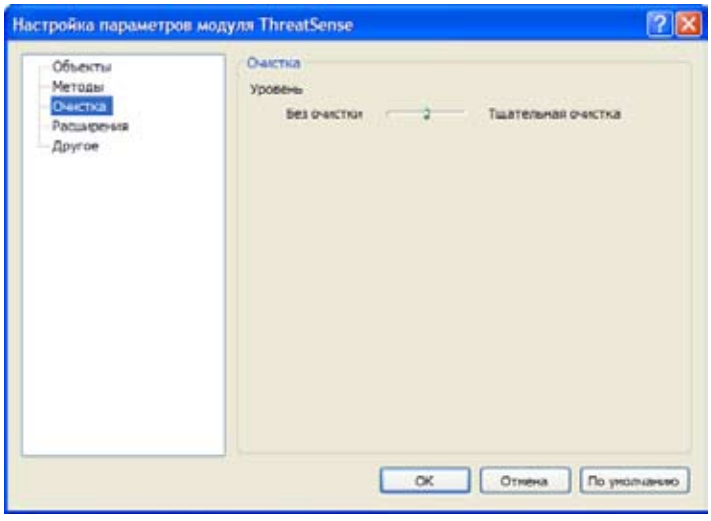
Для минимального использования системных ресурсов во время защиты в реальном времени прошедшие сканирование файлы будут сканироваться повторно только в том случае, если они изменятся. Сканирование всех файлов происходит каждый раз после обновления базы данных вирусных сигнатур. Данная функция может быть изменена с помощью опции **Оптимизированное сканирование** (Optimized scanning). Если она отключена, то сканирование будет происходить при каждой операции доступа к файлу.

По умолчанию защита в реальном времени запускается при загрузке оперативной 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

Для защиты в реальном времени предусмотрено три уровня очистки (для получения доступа к ним в разделе **Защита в режиме реального времени** (Real-time file system protection) выберите команду **Настройка**... (Setup...) и щелкните ветвь **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, понимающих меры, необходимые для каждого типа проникновений.
- На среднем уровне происходит автоматический выбор и выполнение предопределенного действия (в зависимости от типа проникновения). Сведения об обнаружении и удалении зараженных файлов предоставляются в информационном сообщении, расположенном в нижнем правом углу экрана. Однако автоматическое действие не выполняется, если проникновение находится в архиве, где содержатся чистые файлы, или если для какого-то объекта не существует предопределенного действия.
- Третий уровень самый «жесткий» – на нем 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 Антивирус настройки устанавливаются оптимальным образом для обеспечения максимального уровня системной безопасности. Для восстановления настроек «по умолчанию» в нижнем правом углу окна **3Защита в режиме реального времени** (Real-time file system protection) нажмите кнопку **По умолчанию** (Default) (**Расширенная настройка** – **Защита от вирусов и шпионских программ** – **Защита 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.

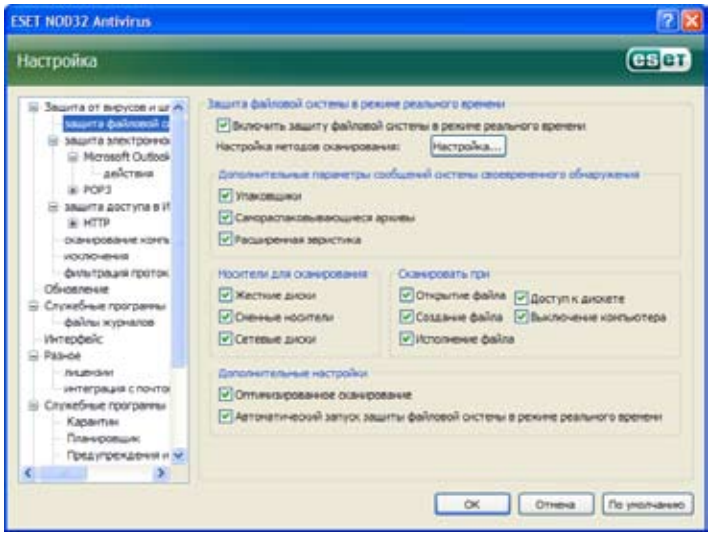
4.1.1.5 Что делать, если защита в режиме реального времени не работает

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

Защита в режиме реального времени отключена

Если защита в режиме реального времени была случайно отключена, необходимо вновь запустить ее. Для этого выберите команды **Настройка** – **Защита от вирусов и шпионских программ** (Setup – Antivirus and antispyware), затем в разделе **Защита в режиме реального времен**и (Real-time file system protection), нажмите кнопку **Включить** (Enable).

Если защита в режиме реального времени не запускается при запуске системы, возможно, отключена опция **Автоматический запуск защиты в режиме реального времени** (Automatic real-time file system protection startup). Чтобы включить эту опцию, перейдите к расширенной настройке (вызываемой клавишей F5) и выберите в этом дереве опцию **3защита в режиме реального времени** (Real-time file system protection). 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, не установлена ли на вашем компьютере другая антивирусная программа. 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, полученную через протокол POP3. Используя подключаемый модуль для Microsoft Outlook, ESET NOD32 Антивирус контролирует весь обмен данными с почтовыми клиентами, осуществляемый по протоколам POP3, MAPI, IMAP, HTTP. Во время проверки входящих сообщений программа применяет все расширенные методы сканирования, предоставленные сканирующим механизмом ThreatSense.

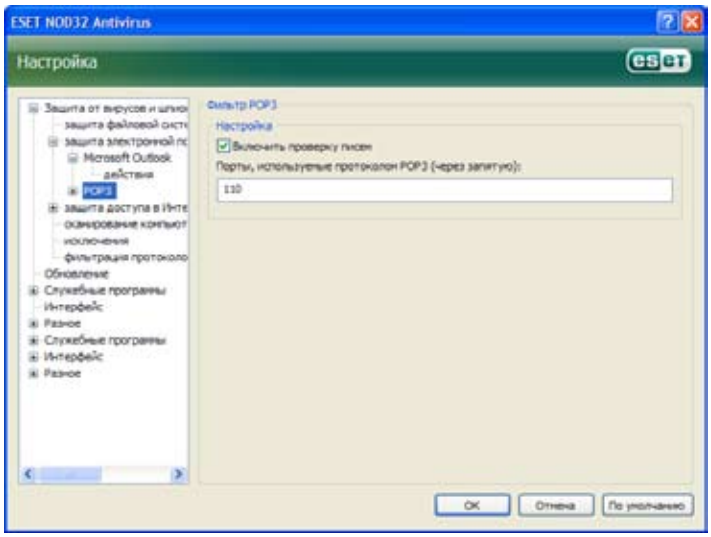
Это означает, что обнаружение вредоносных программ происходит даже раньше, чем их сопоставление с базой данных вирусных сигнатур. На сканирование данных, передаваемых через протокол POP3, не влияет тип используемого клиента электронной почты.

4.1.2.1 Проверка POP3

Протокол POP3 – самый распространенный протокол для получения сообщений по электронной почте в клиентском приложении. Антивирус ESET NOD32 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 очистительного процесса. Чтобы изменить уровень контроля фильтрации POP3, выберите команду Защита от вирусов и шпионских программ – **Защита электронной почты** – **POP3** – **Совместимость** (Antivirus and antispyware – Email protection – POP3 – Compatibility).

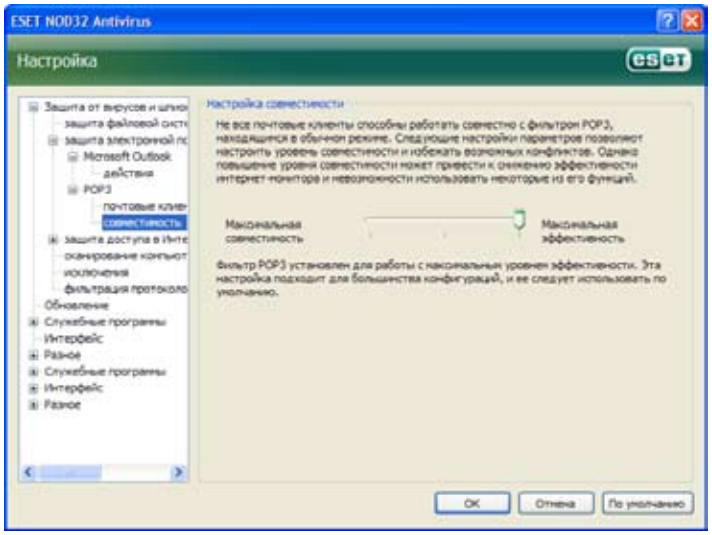
Если включена **Максимальная эффективность** (Maximum efficiency), то вирусы удаляются из зараженных сообщений, а информация о них выносится перед исходной темой сообщения (должны быть включены опции **Удалить** (Delete) или **Очистить** (Clean), уровень очистки должен быть **Строгий** (Strict) или **По умолчанию** (Default)).

Средняя совместимость (Medium compatibility) приводит к изменению способа 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 совместимост**ь (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.

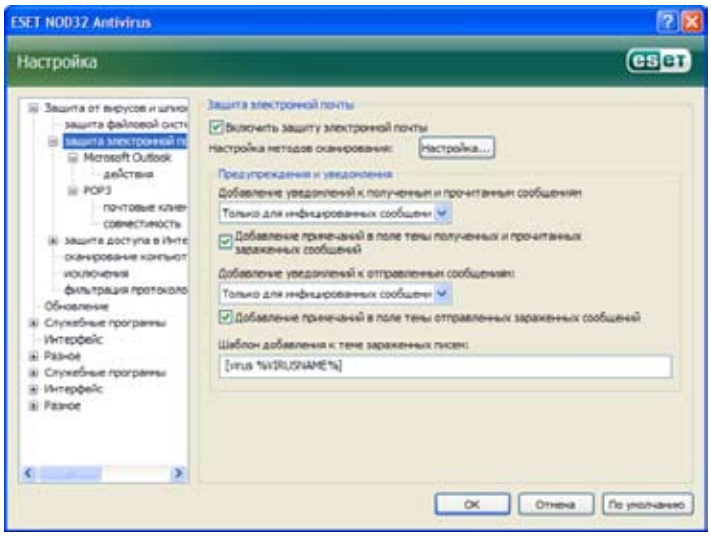


4.1.2.2 Интеграция с Microsoft Outlook, Outlook Express и Windows Mail

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

Если Антивирус ESET NOD32 поддерживает ваш клиент электронной почты, то можно произвести интеграцию. Тогда панель инструментов приложения ESET NOD32 Антивирус будет интегрирована с интерфейсом клиента электронной почты, что повышает эффективность защиты электронной почты. Для настройки интеграции выберите команду **Настройка** – **Открыть полное дерево расширенной 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.

Защита электронной почты запускается установкой 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)).



4.1.2.2.1 Добавление теговых сообщений к тексту письма

Каждое письмо, контролируемое ESET NOD32 Антивирусом можно отметить, 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 функцию 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 Антивирусе 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).

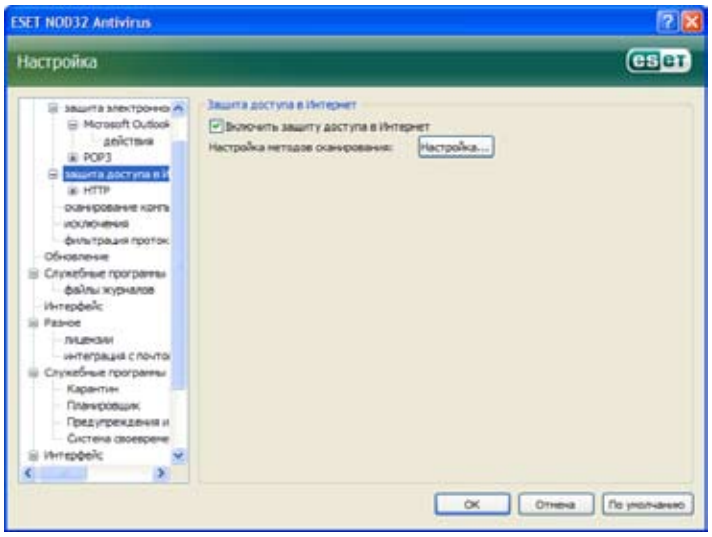
Содержание уведомлений можно изменять в поле образца, присоединенного к зараженному сообщению. Перечисленные выше настройки помогут автоматизировать процесс фильтрации зараженных сообщений, так как письма с определенной темой перемещаются в отдельную папку (при условии, что данная функция поддерживается 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), предназначенные для применения к зараженным объектам. В большинстве случаев рекомендуется выбрать команду **Очистить** (Clean) либо **Удалить** (Delete). В особых случаях, если зараженный файл необходимо принять, выберите команду **Оставить** (Leave). Если включена функция **Строгой очистки** (Strict cleaning), то появится информационное окно, в котором все операции с зараженными объектами отключены.

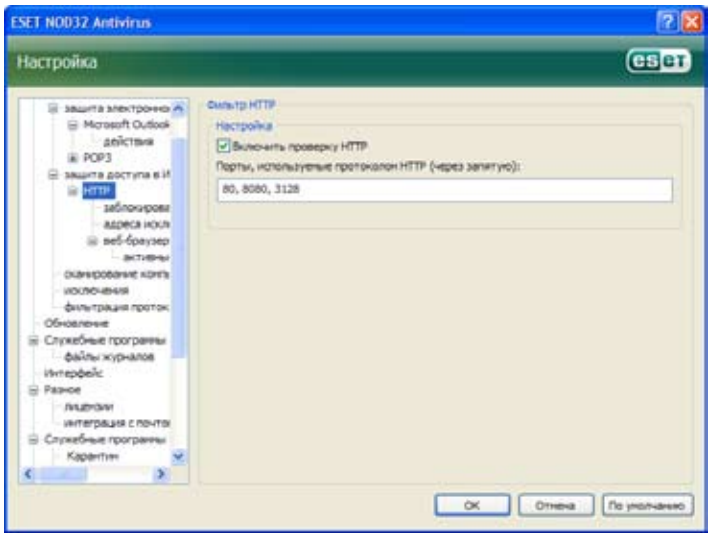
4.1.3 Защита веб-доступа

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

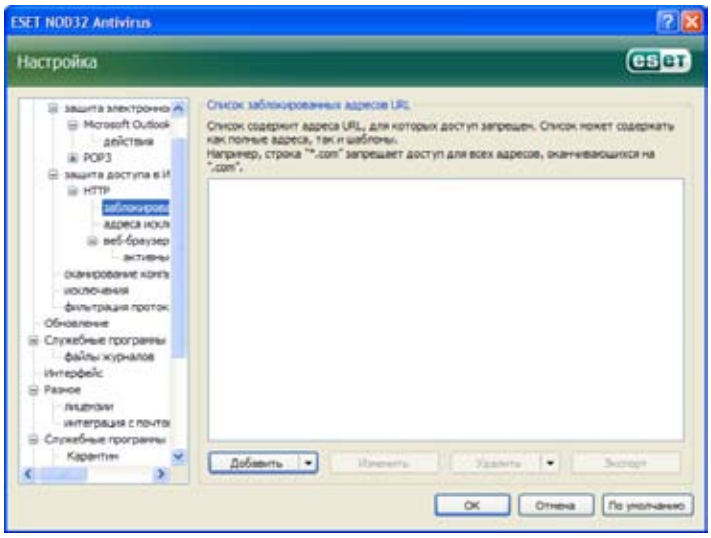
Основной функцией защиты доступа в Интернет является мониторинг соединений между интернет-браузерами и удаленными серверами в соответствии с правилами протокола HTTP (Hypertext Transfer Protocol, протокол передачи гипертекста). По умолчанию ESET NOD32 Антивирус использует HTTP-стандарты большинства интернет-браузеров. 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 особые списки URL-адресов (унифицированных указателей информационных ресурсов): **Заблокированные адреса** (Blocked addresses) или **Адреса исключений** (Excluded addresses).

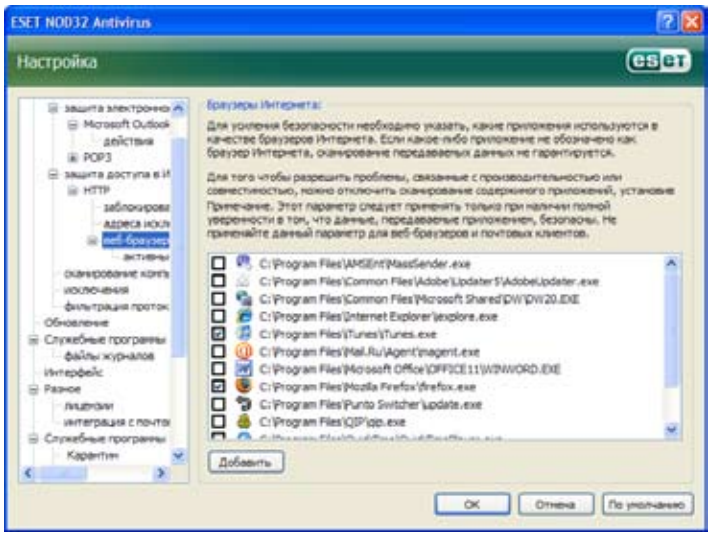
Оба диалоговых окна содержат кнопки **Добавить** (Add), **Изменить** (Edit), **Удалить** (Remove) и **Экспорт** (Export), позволяющие управлять списками указанных адресов. Если запрашиваемый пользователем адрес включен в список заблокированных, доступ к соответствующему ресурсу будет невозможен. Если 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

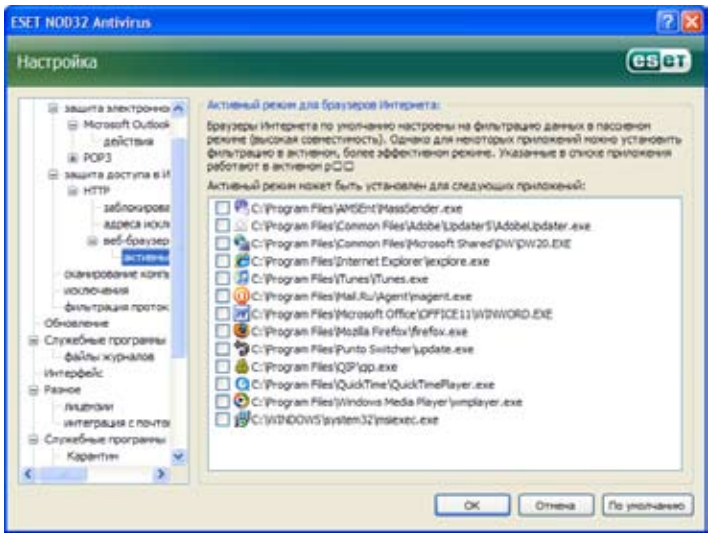
ESET NOD32 Антивирус также содержит функцию Веб-браузеры (Web browsers), позволяющую пользователю указывать приложения, являющиеся браузерами. Если приложение отмечается как браузер, все его соединения отслеживаются вне зависимости от номеров портов, участвующих в соединении.

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 в нем 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

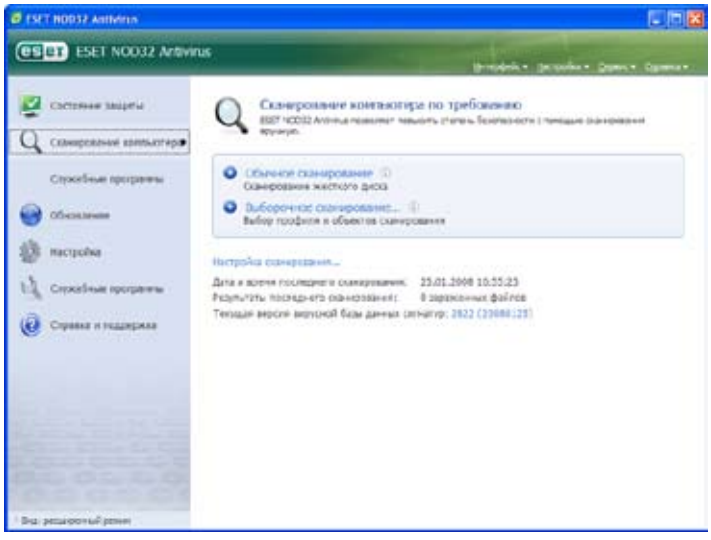
Если есть подозрение, что компьютер заражен (то есть его поведение необычно), выполните его сканирование по требованию, чтобы обнаружить возможные угрозы. С точки зрения безопасности, важно выполнять сканирование компьютера не только при подозрении на заражение, но и в качестве рутинной меры. Регулярное сканирование обеспечивает обнаружение угроз, которые не были обнаружены при сканировании в реальном времени.

Такое может 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 один или два раза 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 предопределенных профилей сканирования, 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 без 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 повторного 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

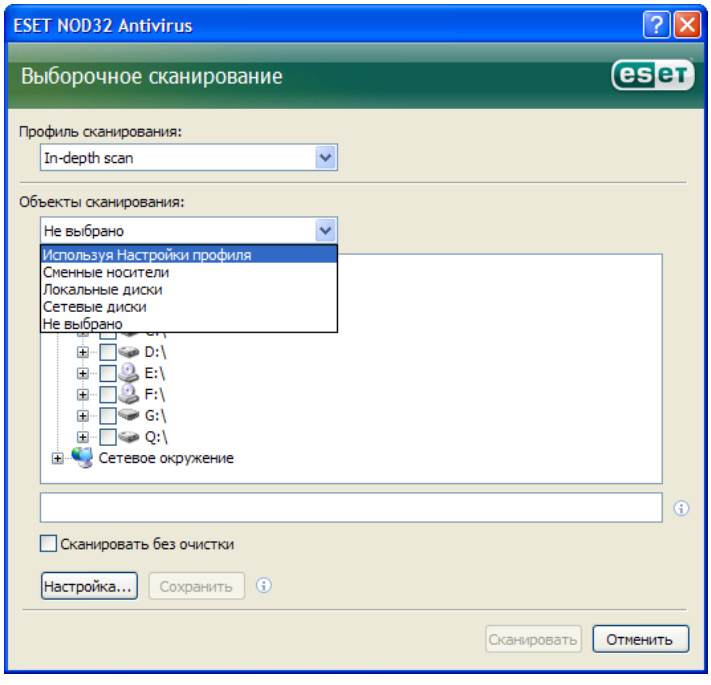
Раскрывающееся меню **Объекты сканирования** (Scan targets) позволяет выбирать файлы, папки и устройства (диски) для антивирусного сканирования.

С помощью пунктов меню можно выбрать следующие объекты сканирования:

Локальные диски (Local drives) – все жесткие диски в системе;

Съемные носители (Removable media) – дискеты, запоминающие устройства USB, компакт-диски и DVD-диски;

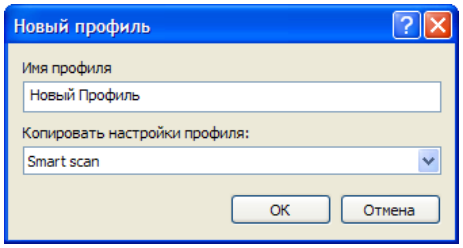
Сетевые диски (Network drives) – все отображенные диски.



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» (ThreatSense engine parameters setup), будут подробно описаны все параметры настройки сканирования. Это поможет создать необходимые профили сканирования.

Пример:

Предположим, необходимо создать собственный профиль сканирования, и настройки профиля «Интеллектуальное сканирование» частично совпадают с требуемыми. Только вот сканирование архивов, вызываемых во время выполнения, или потенциально опасных приложений не нужно и, кроме того, хотелось бы применять параметр **Строгая очистка** (Strict cleaning).

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, обеспечивающая защиту даже в первые часы распространения новой угрозы. В ней используется комбинация нескольких методов (анализ кода, эмуляция кода, общие сигнатуры, вирусные сигнатуры), сочетание которых значительно повышает безопасность системы. Ядро сканирования способно контролировать несколько потоков данных одновременно, максимально увеличивая эффективность и уровень обнаружения. Кроме того, технология ThreatSense успешно детектирует руткиты.

Опции настройки технологии ThreatSense позволяют пользователю задавать различные параметры сканирования:

- Типы и расширения файлов, для которых требуется выполнить сканирование
- 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 режиме реального времени
- Проверка файлов при запуске системы.
- Защита электронной почты
- Защита веб-доступа
- Сканирование компьютера по запросу

Параметры ThreatSense для каждого модуля имеют высокую степень оптимизации, поэтому их изменение может существенно повлиять на производительность системы. Например, если задать параметр сканирования упаковщиков, 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 наличие проникновений:

Оперативная память (Operating memory) – сканирование на наличие угроз, нацеленных на оперативную память системы;

Загрузочные секторы (Boot sectors) – сканирование загрузочных секторов на наличие вирусов в основной загрузочной записи;

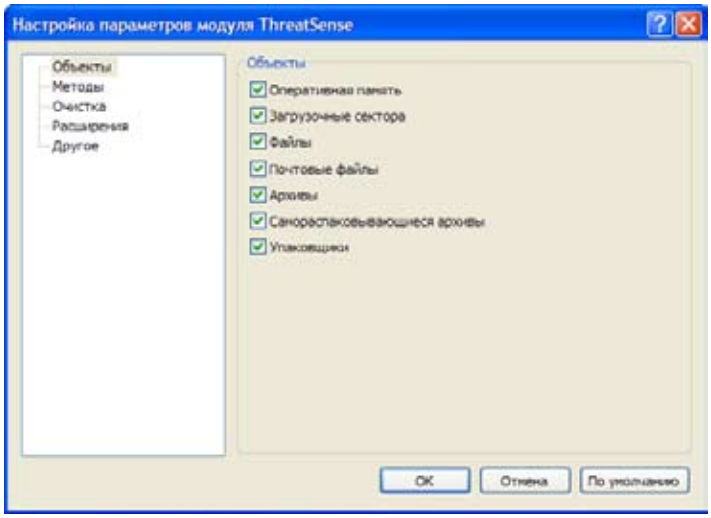
Файлы (Files) – сканирование всех обычных типов файлов (программы, изображения, звуковые файлы, видеофайлы, файлы баз данных и т.д.);

Почтовые файлы (Email files) – сканирование специальных файлов, в которых хранятся сообщения электронной почты;

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

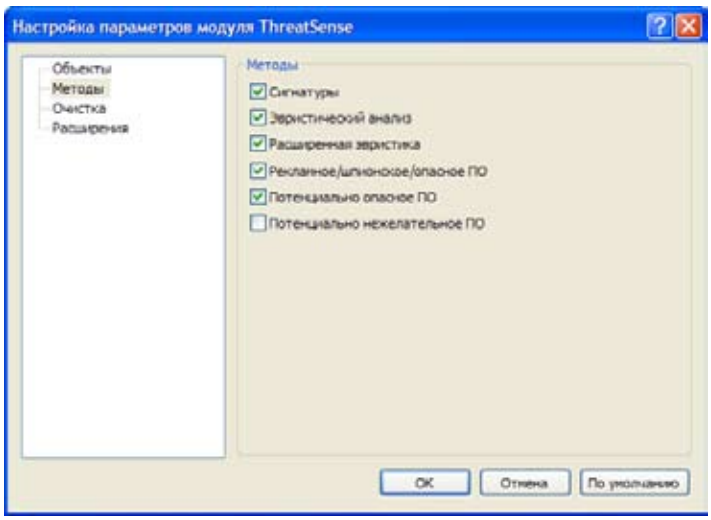
Самораскрывающиеся архивы (Self-extracting archives) – сканирование файлов, содержащих самораскрывающиеся архивы, но обычно имеющих расширение EXE;

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 наличие проникновений. Доступны следующие варианты:



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

эвристический анализ (Heuristics) – применение аналитических алгоритмов к функционированию 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. 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 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.

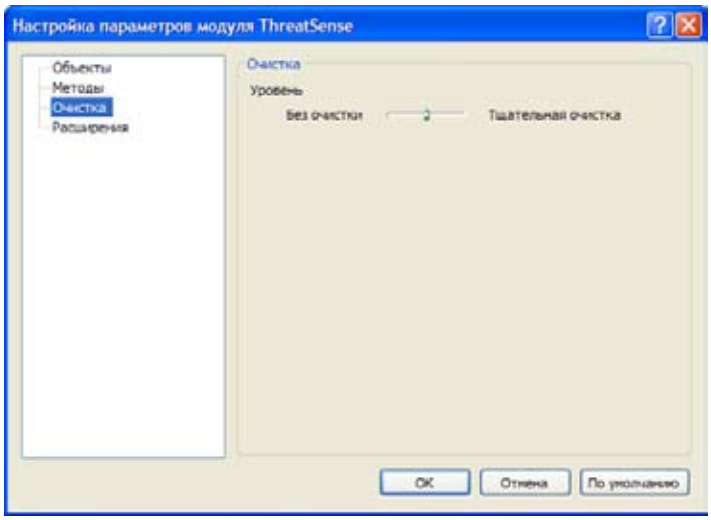
4.1.5.3 Очистка

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. Действия на выбор также предлагаются, если предопределенное действие не может быть выполнено.
- **строгая 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 архивный файл удаляется целиком, только если инфицированы все находящиеся в нем файлы. Если в него входят и нормальные файлы, он не удаляется. Если же зараженный архивный файл обнаруживается в режиме полной очистки, он удаляется целиком, даже если содержит и чистые файлы.



4.1.5.4 Расширения

Расширение – это часть имени файла, отделенная точкой.

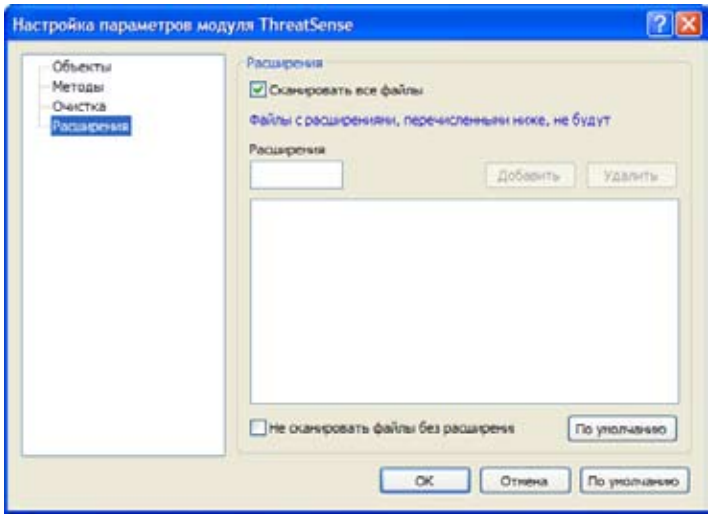
Расширение определяет тип и содержимое файла. Данный раздел параметров настройки ThreatSense позволяет определять, какие типы файлов следует сканировать.

По умолчанию сканируются все файлы независимо от расширений.

При этом в список файлов, исключаемых из сканирования, можно добавить любые расширения. Если флаг **Сканировать все файлы** (Scan all files) не установлен, то в списке отображаются 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

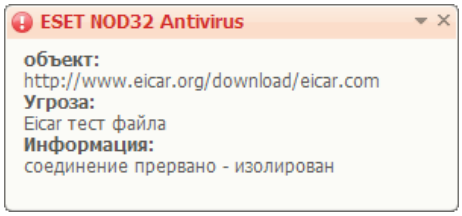
Угрозы могут проникать в систему разными путями: с веб-страниц, из совместно используемых папок, по электронной почте или через съемные носители, такие как USB-устройства, внешние диски, компакт-диски, DVD-диски, дискеты и т.д.

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

- откройте приложение ESET NOD32 Антивирус и щелкните пункт меню Сканирование компьютера (Computer scan).
- выберите опцию **Стандартное сканирование** (Standard scan) (дополнительные сведения см. в разделе «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 Антивирус 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 (Leave) 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 только 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.

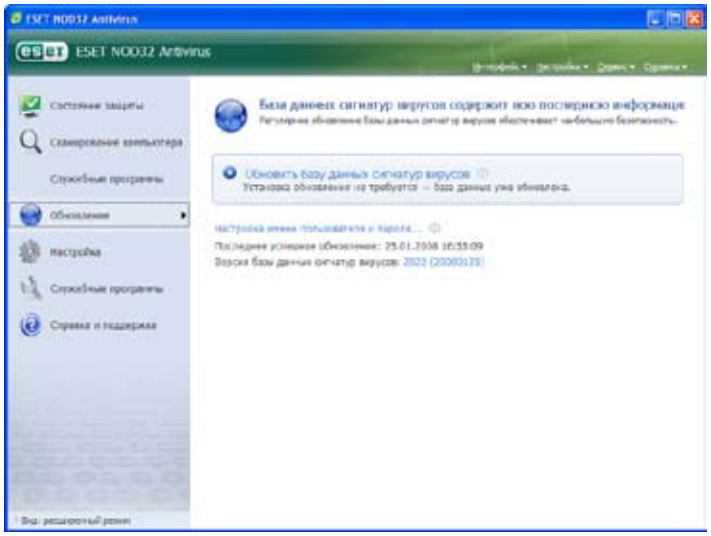
4.2 Обновление версии программы

Регулярное обновление системы – это основное условие достижения максимального уровня защиты, обеспечиваемой ESET NOD32 Антивирус.

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 опции настройки обновления, такие как имя пользователя и пароль для доступа к серверам обновлений ESET.

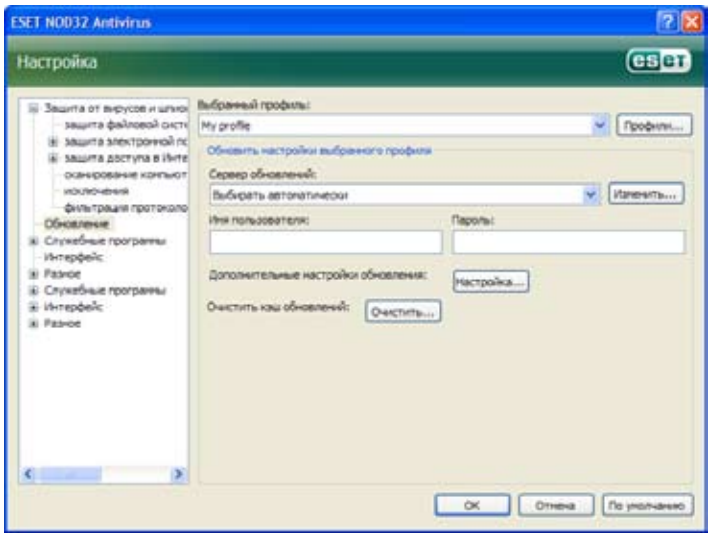
В информационном окне содержатся сведения о дате и времени последнего успешного обновления, номер базы данных вирусных сигнатур. Цифровое обозначение представляет собой действующую ссылку на веб-сайт ESET с перечислением всех сигнатур, добавленных в рамках данного обновления.



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

4.2.1 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. Опции настройки обновлений находятся в разделе **Обновления** (Update) дерева расширенной настройки, вызываемого клавишей F5.

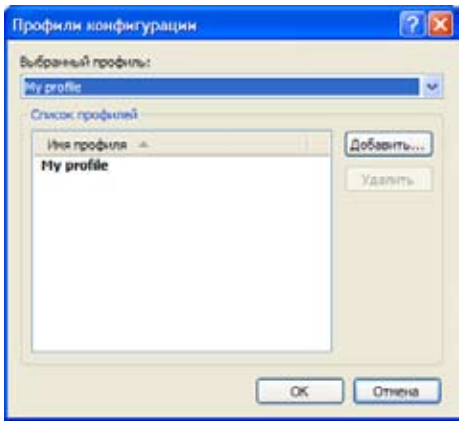


4.2.1.1 Профили обновления

Для различных настроек 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).

4.2.1.2 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).

4.2.1.2.1 Режим обновлений

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

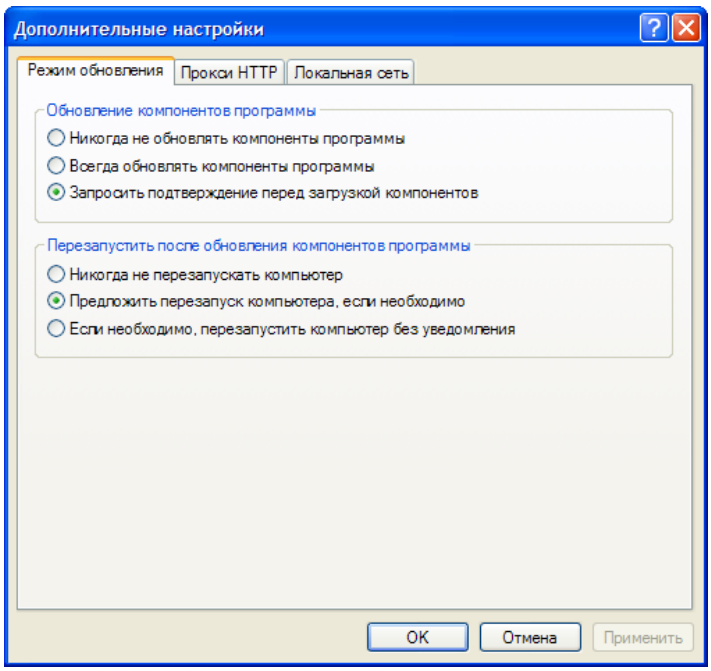
Раздел **Обновления программных компонентов** (Program component update) содержит три опции:

- **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 выбрана опция **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. Опция **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 третьей опции, **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 установлена опция **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 программных компонентов** (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, перезапускать компьютер без уведомления** (If necessary, restart computer without notifying)

По умолчанию для перезагрузки компьютера установлена опция **Предложить перезапуск компьютера, если необходимо** (Offer computer restart if necessary). Выбор наиболее подходящих опций 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.

4.2.1.2.2 Прокси-сервер

Чтобы получить доступ к опциям 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 одну из следующих трех опций:

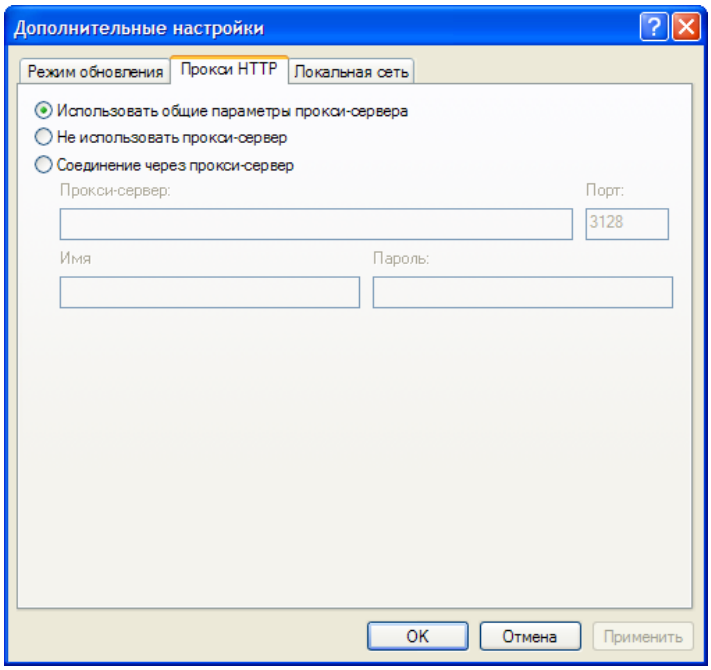
- **Использовать общие параметры прокси-сервера** (Use global proxy server settings)
- **Не использовать прокси-сервер** (Do not use proxy server)
- **Соединение через прокси-сервер** (Connection through a proxy server, подключение определяется свойствами подключения)

Выбор опции **Использовать общие параметры прокси-сервера** (Use global proxy server settings) приводит к использованию опций настроек прокси-сервера, установленных в дереве расширенной настройки в разделе **Разное** – **Прокси-сервер** (Miscellaneous – Proxy server).

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

Опция **Соединение через прокси-сервер** (Connection through a proxy server) следует выбрать, если для обновления ESET NOD32 Антивирус необходимо использовать прокси-сервер, отличный от указанного в общих параметрах (**Разное** – **Прокси-сервер** (Miscellaneous – Proxy server)). В этом случае нужно будет указать следующие настройки: **Прокси-сервера**

(Proxy server), **Порт связи** (Port), а также, при необходимости, **Имя пользователя** (User name) и **Пароль** (Password) для доступа к прокси-серверу.



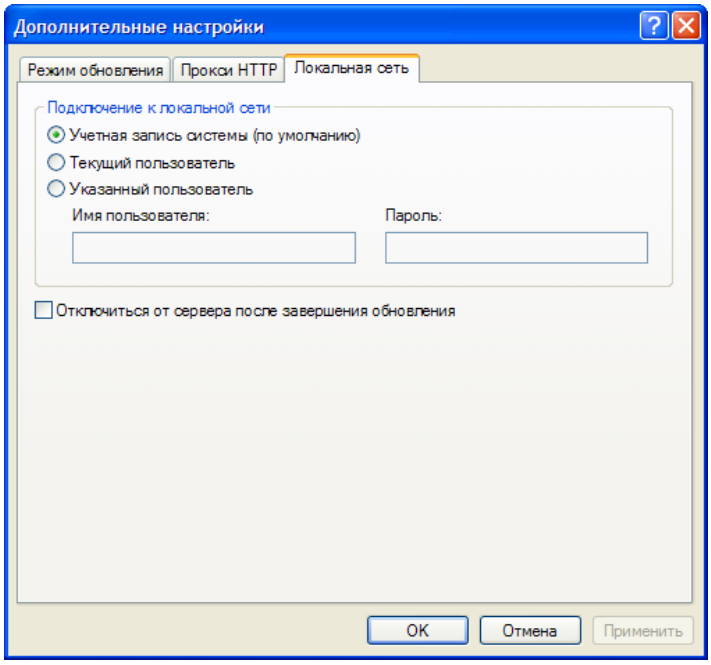
Эту опцию следует выбрать и в том случае, если настройки прокси-сервера не были заданы глобально, но система ESET NOD32 Антивирус подключается к прокси-серверу для загрузки обновлений.

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

4.2.1.2.3 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 в разделе настройки обновлений следует ввести имя пользователя и пароль или 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 **Подключиться к локальной сети как** (Connect to LAN as) предлагаются варианты **Учетная запись системы (по умолчанию)** (System account (default)), **Текущий пользователь** (Current user) и **Указанный пользователь** (Specified user).



Чтобы для проверки подлинности использовать системную учетную запись, выберите опцию **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 выбрана опция **Учетная запись системы** (System account).

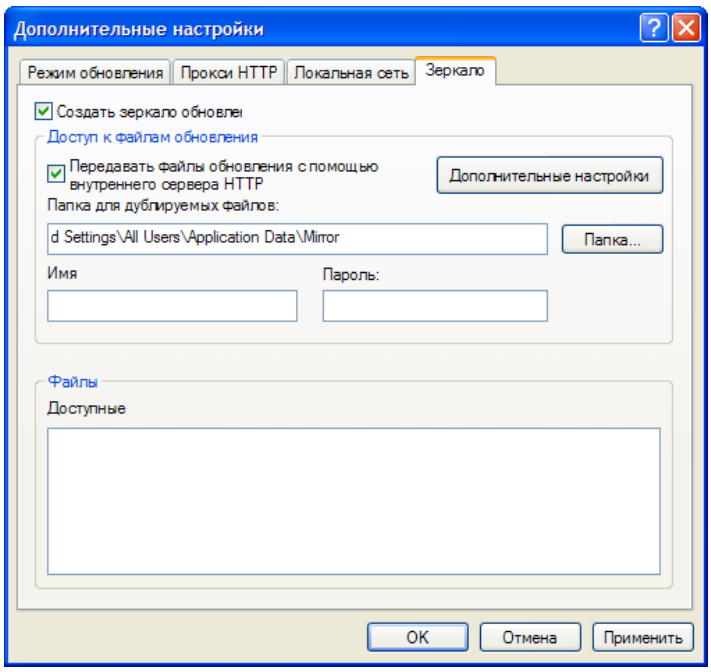
Внимание!

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.

4.2.1.2.4 Создание копий обновлений – зеркало

Версия ESET NOD32 Антивирус 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.

Опции настройки локального сервера-зеркала доступны в разделе **Расширенная настройка обновлений** (Advanced update setup; вызывается клавишей F5, после чего в дереве расширенной настройки необходимо выбрать раздел **Обновления** (Update), нажать кнопку **Настроить**... (Setup...) рядом с командой **Расширенная настройка обновлений:** (Advanced update setup:) и перейти на вкладку **Зеркало** (Mirror)).



Первым шагом в настройке зеркала является установка флажка **Создать зеркало обновлений** (Create update mirror). Выбор этой команды активирует другие опции настройки (например, способ доступа к файлам обновления и путь обновления 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 хранения зеркальных отображений 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:).

4.2.1.2.4.1 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 внутреннего HTTP-сервера

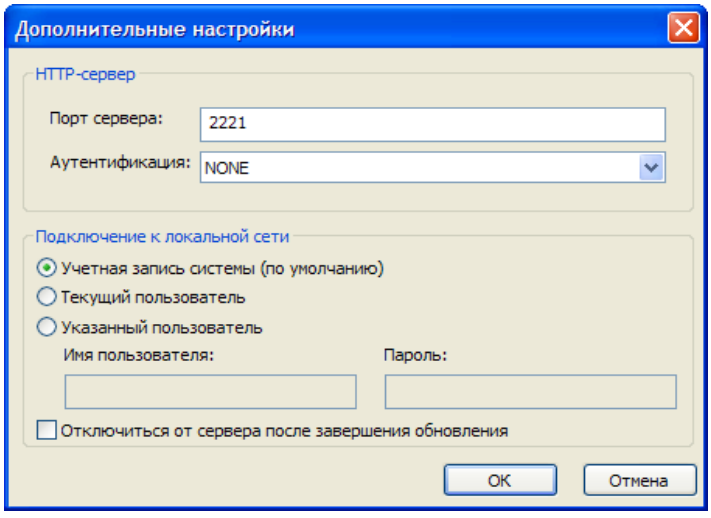
Эта настройка задается по умолчанию и указана в предопределенной конфигурации программы. Чтобы получить доступ к зеркалу при помощи HTTP-сервера, в разделе **Расширенная настройка обновлений** (Advance update setup) перейдите на вкладку **Зеркало** (Mirror) и установите флаг **Создать зеркало обновлений**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

В разделе **Расширенная настройка** (Advanced setup) вкладки Зеркало (Mirror) можно указать прослушиваемый HTTP-сервером **Порт сервера** (Server Port) и в поле **Проверка пользователя** (Authentication) задать необходимый для этого HTTP-сервера тип проверки. По умолчанию указан порт сервера 2221. Параметр **Проверка подлинности** (Authentication) определяет метод проверки, используемый для доступа к файлам обновлений. Доступны следующие варианты: **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 Антивирус.



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 Антивирус** (ESET NOD32 Antivirus Advanced Setup) и перейдите в раздел **Обновления** (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 Антивирус 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 Антивирус (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 \\UNC\PATH в качестве сервера обновлений. Для осуществления этой операции выполните следующие действия:

- Откройте раздел «Расширенная настройка ESET NOD32 Антивируса » (ESET NOD32 Antivirus Advanced Setup) и выберите раздел Обновления (Update).
- Рядом с полем для задания сервера обновлений нажмите кнопку **Изменить**... (Edit...) и добавьте новый сервер в формате \\UNC\PATH;
- 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.

4.2.1.2.4.2 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 Антивирус сообщает об ошибке подключения к северу зеркала** (ESET NOD32 Антивирус 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 **ОК** (OK). Это должно привести к отображению содержимого папки;
- **Программе ESET NOD32 Антивирус необходимы имя пользователя и пароль** (ESET NOD32 Антивирус 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. В группу «Everyone» не входят неуполномоченные пользователи, папка доступна только для всех пользователей домена. Таким образом, даже если папка доступна группе пользователей «Everyone», в разделе настройки обновлений должны быть указаны имя пользователя и пароль;

- **ESET NOD32 Антивирус сообщает об ошибке подключения к серверу зеркала** (ESET NOD32 Антивирус reports an error connecting to the Mirror server): блокирована передача данных через порт, указанный для доступа к HTTP-версии зеркала.

4.2.2 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.

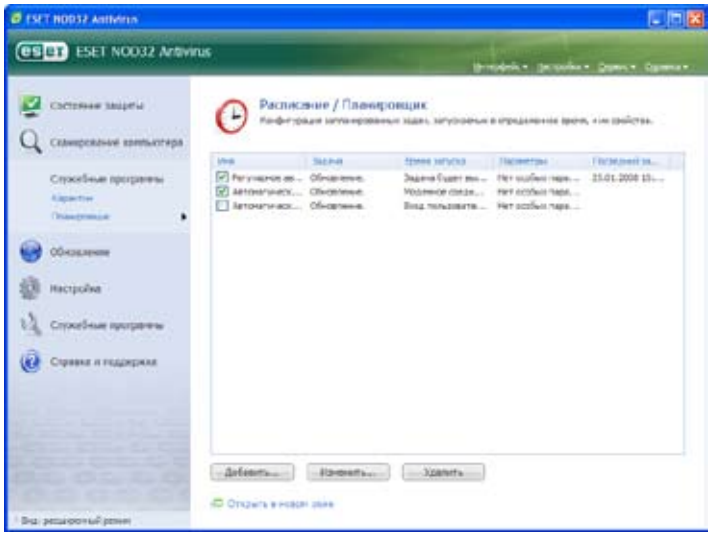
Кроме того, загрузка обновлений может быть запущена как запланированная задача. Чтобы настроить запланированную задачу, выберите команды пункты меню **Инструменты** – **Планировщик** (Tools – Scheduler). По умолчанию в программе ESET NOD32 Антивирус активированы следующие задачи:

- **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 настройкой. Более подробные сведения о создании и настройке задач обновления см. в главе «Планировщик» (Scheduler).

4.3 Планировщик

Планировщик доступен в ESET NOD32 Антивирус при включенном расширенном режиме. Планировщик (Scheduler) находится в разделе Инструменты (Tools) главного меню ESET NOD32 Антивирус. Планировщик содержит сводный список всех запланированных задач и свойства их конфигурации (например, предопределенную 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 настройки 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...).

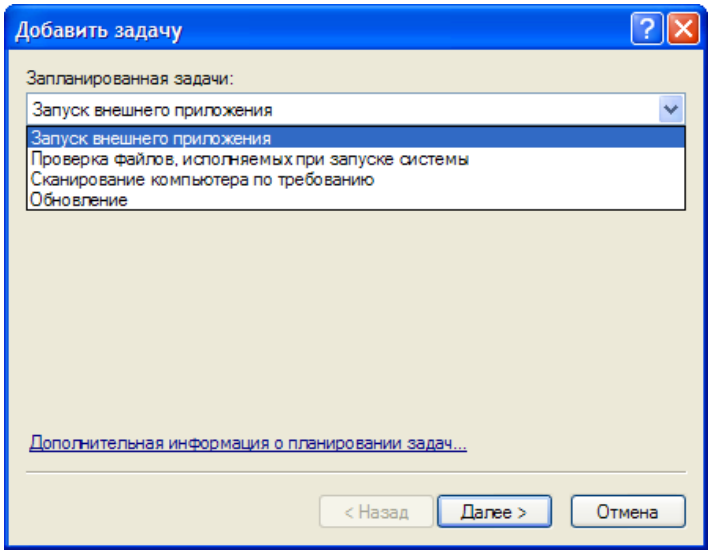
4.3.1 Цель планирования задач

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.

4.3.2 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)
- **Системная проверка файла запуска** (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 ука-**

занными параметрами (Run task with specific parameters) должен быть установлен автоматически. Нажмите кнопку **Готово** (Finish).

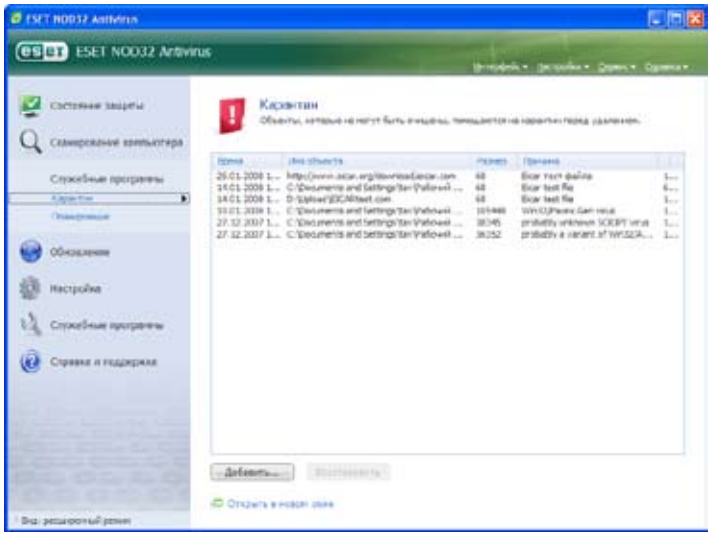
Появится диалоговое окно, позволяющее выбрать профили, используемые для данной запланированной задачи. Кроме основного, здесь можно указать альтернативный профиль, который должен применяться при невозможности выполнения задачи с использованием основного профиля. Подтвердите выбор, нажав кнопку **OK**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

4.4 Карантин

Основная задача карантина – безопасное сохранение 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 Антивирус.

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

Файлы, сохраненные в папке карантина, можно просмотреть в таблице, в которой 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).



4.4.1 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 файл из исходного расположения не удаляется. Для этих целей можно воспользоваться контекстным меню: щелкнуть окно карантина правой кнопкой мыши и выбрать команду **Добавить** (Add...)

4.4.2 Восстановление из карантина

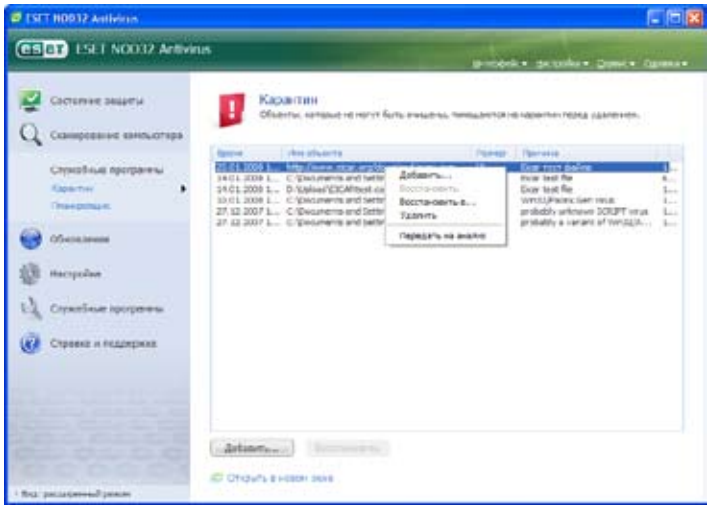
Помещенные в карантин файлы можно восстановить в их исходное местоположение. Для этого воспользуйтесь командой **Восстановить** (Restore) из контекстного меню файла (чтобы открыть его, щелкните файл в окне карантина правой кнопкой мыши). Кроме этого, контекстное меню содержит команду **Восстановить в**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

4.4.3 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 отправить на рассмотрение файл, помещенный в карантин, щелкните его правой кнопкой мыши и выберите в контекстном меню команду Отправить на анализ (Submit for analysis).

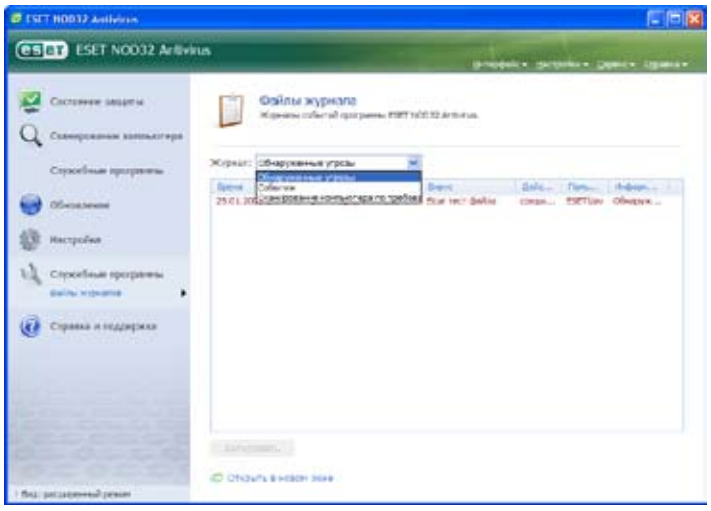


4.5 Файлы журналов

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 просматривать и архивировать непосредственно в среде ESET NOD32 Антивирус.

Доступ к файлам журналов можно получить, выбрав в основном окне ESET NOD32 Антивирус 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 Антивирус;
- **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;

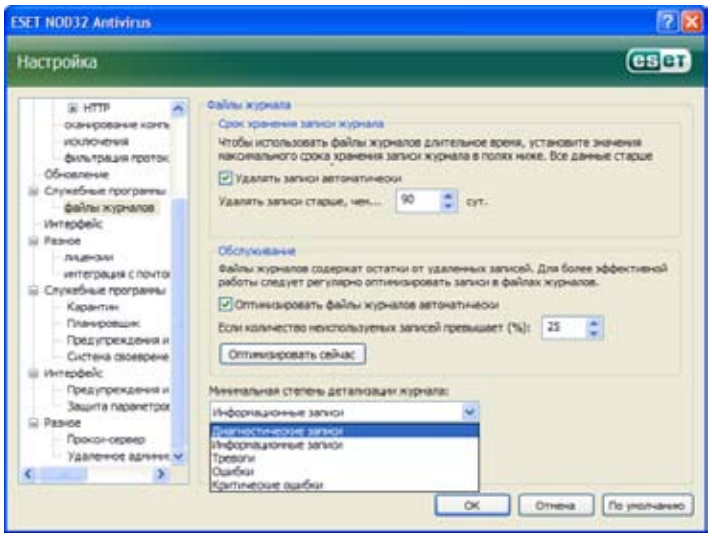


В каждом разделе отображенные сведения можно напрямую скопировать в буфер обмена, выбрав запись и нажав кнопку **Копировать** (Copy). Чтобы выбрать несколько записей, удерживайте нажатыми клавиши CTRL или SHIFT.

4.5.1 Ведение журнала

Доступ к конфигурации ведения журналов в ESET NOD32 Антивирус можно получить в главном окне программы. Выберите команды **Настроить** – **Открыть полное дерево расширенной настройки**... – **Служебные программы** – **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;
- **Минимальное стапень детализации журнала** (Minimum logging verbosity): определяет уровень словесного наполнения журнала. Доступные опции:
  - **Опасные 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.



4.6 Пользовательский интерфейс

Опции настройки пользовательского интерфейса в ESET NOD32 Антивирус можно изменить таким образом, чтобы настроить рабочую среду в соответствии с потребностями пользователя. Эти опции настройки доступны в разделе **Интерфейс** (User interface) дерева расширенной настройки ESET NOD32 Антивирус.

В разделе **Элементы 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 Антивирус.

Флажок **Графический интерфейс** (Graphical user interface) необходимо снять, если графические элементы снижают производительность компьютера или приводят к возникновению проблем. Отключение графического интерфейса может потребоваться и для пользователей с нарушениями зрения, поскольку элементы этого интерфейса могут привести к конфликту со специальными приложениями, используемыми для считывания текста с экрана.

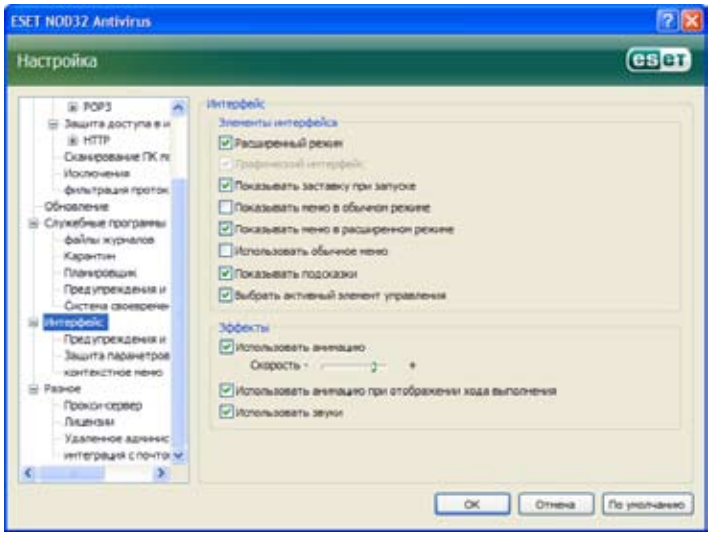
Чтобы отключить появление заставки ESET NOD32 Антивирус при запуске программы, снимите флажок **Показывать заставку при запуске** (Show splash-screen at startup).

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

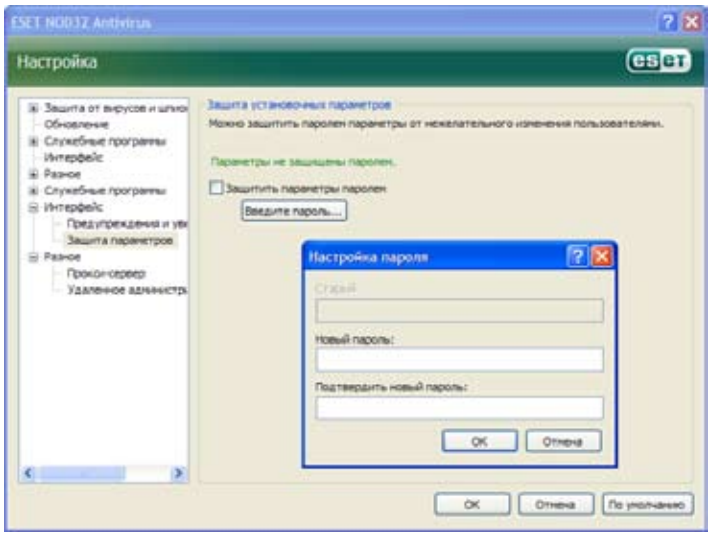
Если установлен флажок **Показывать подсказки** (Show tooltips), то при наведении курсора на какой-либо параметр будет отображаться его краткое описание. При установленном флажке **Выбрать активный элемент управления** (Select active control element) система выделяет элемент, находящийся в данный момент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

Чтобы уменьшить или увеличить скорость отображения анимированных эффектов, установите флажок **Использовать анимацию при отображении хода действия** (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 анимированные пиктограммы** (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 Антивирус 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...).



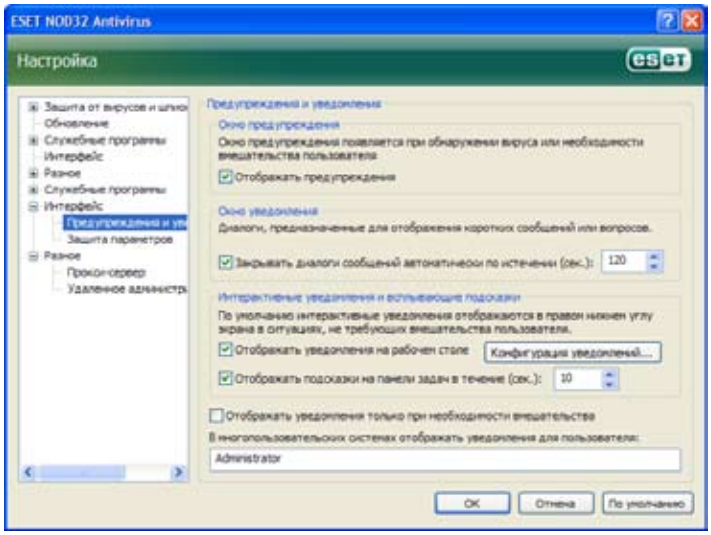
4.6.1 Предупреждения и уведомления

Область **Предупреждения и уведомления** (Alerts and notifications setup) в разделе **Пользовательский интерфейс** (User interface) позволяет настроить, каким образом сообщения предупреждений об угрозах и системные уведомления обрабатываются в ESET NOD32 Антивирусе.

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 **Конфигурация уведомления**... (Configure notifications...). Кнопка **Предварительный просмотр** (Preview) выводит на экран предварительный просмотр поведения уведомлений. Продолжительность отображения всплывающих подсказок задается параметром **Отображать подсказки на панели задач в течении (сек.)** (Display balloon tips in taskbar (for sec.)).



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

4.7 ThreatSense.Net

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

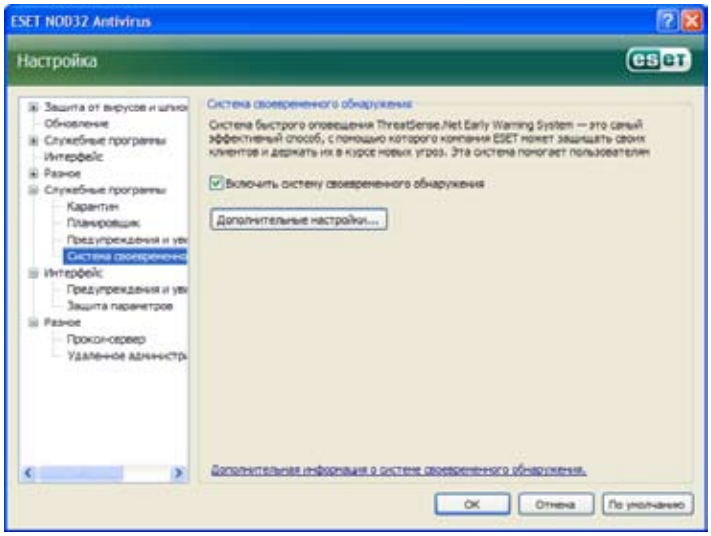
У двунаправленной системы предупреждений ThreatSense.Net одно назначение – совершенствовать предлагаемую защиту. Оптимальный метод обнаружения новых угроз по мере их возникновения заключается в установлении связи с максимально большим числом наших клиентов и использовании их в качестве «разведчиков угроз».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

- Вы можете отключить систему раннего оповещения ThreatSense.Net. При этом вы не проигрываете в функциональности программного обеспечения и продолжаете получать наилучшую защиту, какую мы только можем предложить.
- Вы можете настроить систему раннего оповещения 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. В системе быстрого оповещения ThreatSense.Net производится сбор данных о компьютере, имеющих отношение к новым обнаруженным угрозам. Данная информация может содержать образец или копию файла, в котором обнаружена угроза, путь к этому файлу, имя файла, сведения о дате и времени, процессе, через который угроза появилась в компьютере, а также сведения об установленной операционной системе. Некоторые сведения могут содержать личную информацию о пользователе компьютера, например, имена пользователей в пути каталога 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 предназначены для других целей.

По умолчанию в программе ESET NOD32 Антивирус 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 (Enable ThreatSense.Net Early Warning System). Это позволит активировать и нажать кнопку **Расширенная настройка**... (Advanced Setup...).

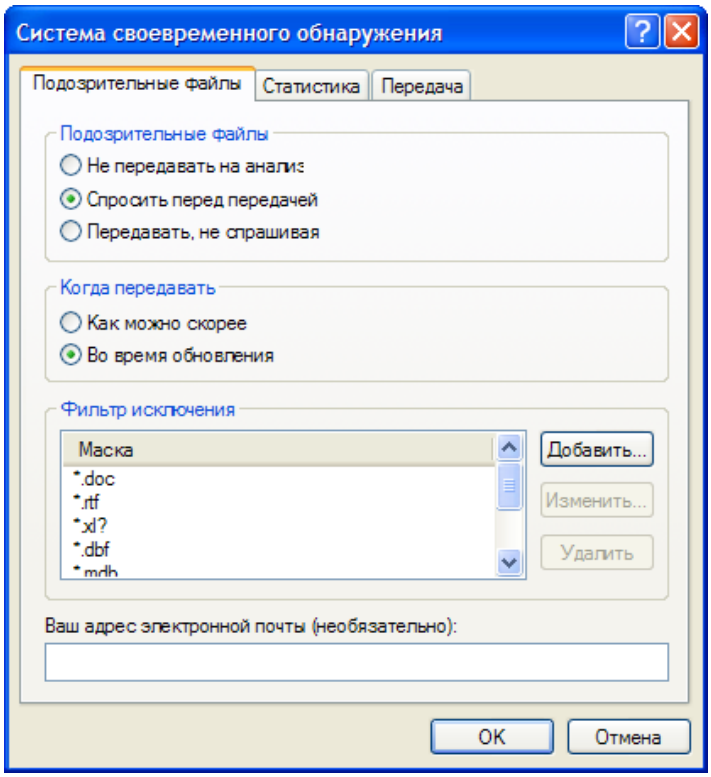


4.7.1 Подозрительные файлы

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 обнаружение 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 как можно быстрее. 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. 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.

4.7.2 Статистические данные

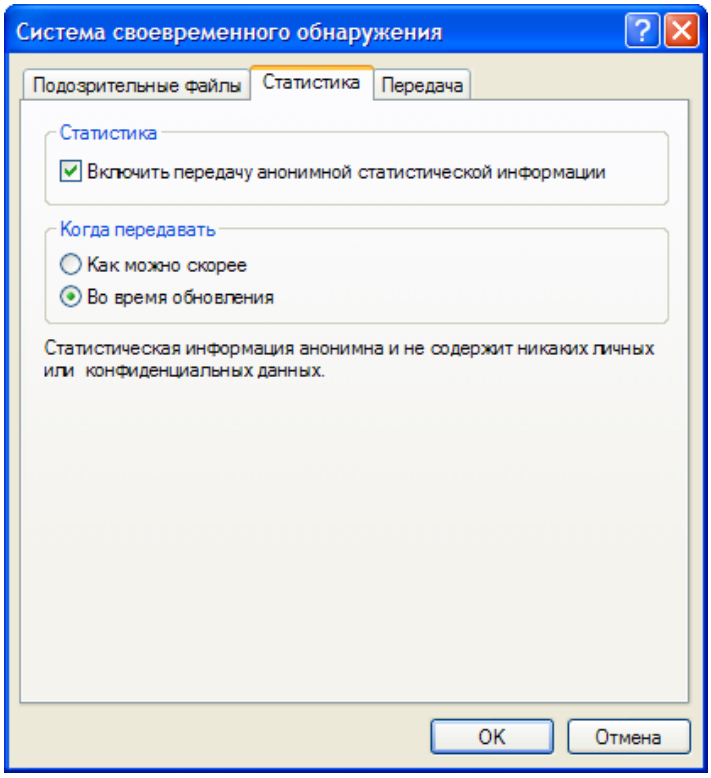
В системе своевременного оповещения ThreatSense.Net производится сбор анонимных данных о компьютере, имеющих отношение к новым обнаруженным угрозам. Эти сведения могут содержать имя проникнувшего вируса, дату и время его обнаружения, версию программы ESET NOD32 Антивирус, версию операционной системы 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
```

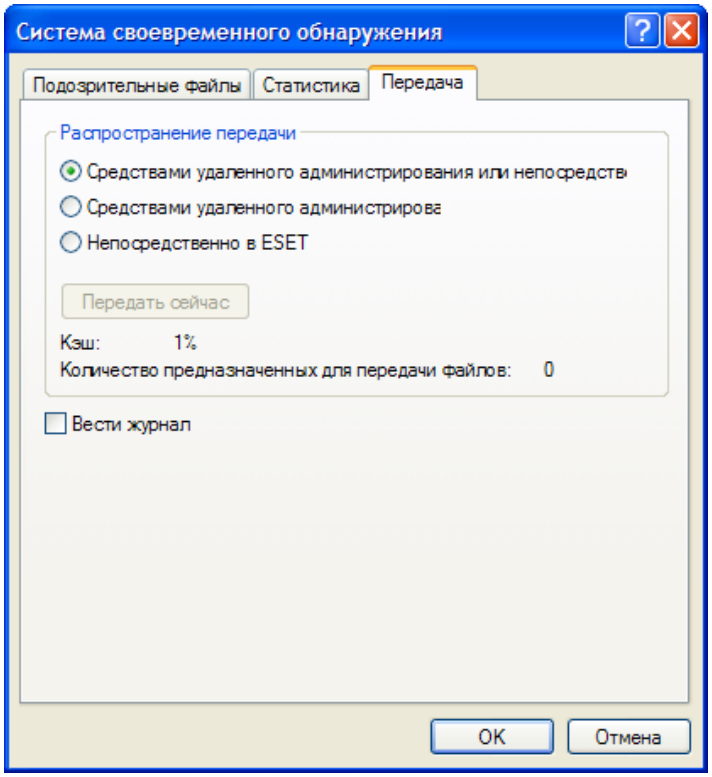
Время отправки

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.



4.7.3 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.



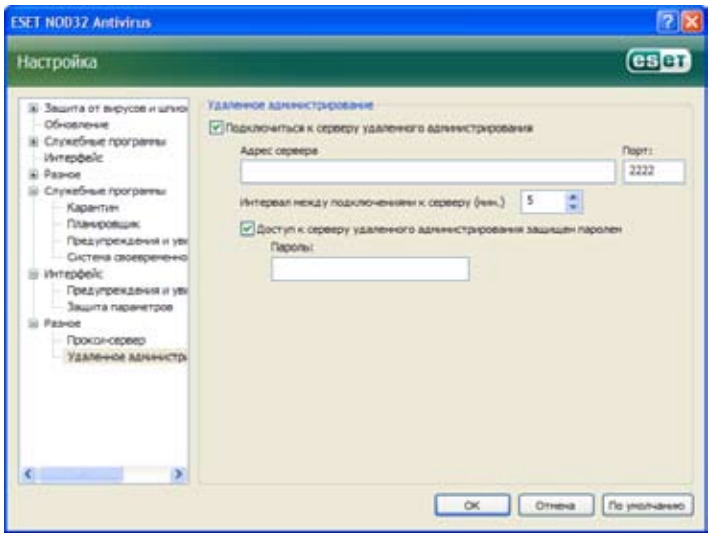
При наличии файлов с отложенной отправкой в этом окне настройки активирована кнопка Отправить сейчас (Submit now). Нажмите эту кнопку, чтобы отправить файлы и статистические данные немедленно.

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

4.8 Удаленное администрирование

Удаленное администрирование представляет собой мощный инструмент для поддержания политики безопасности и получения обзора общего 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 Антивирус на клиентских рабочих станциях.

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



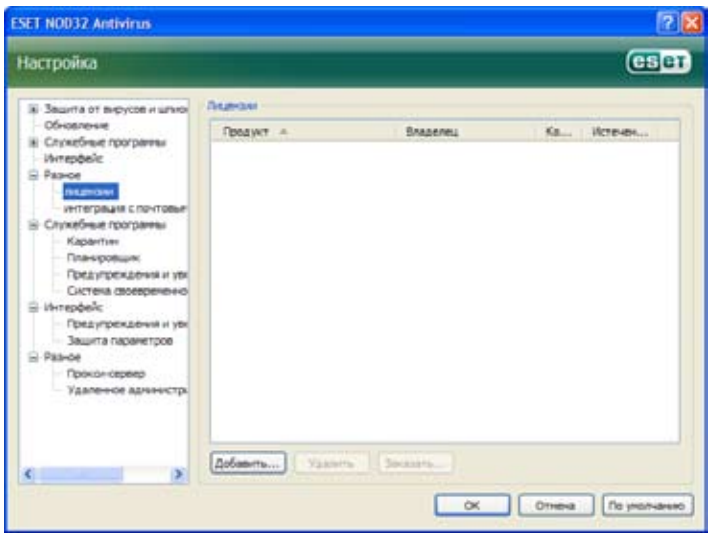
В окне настройки вы можете включить режим удаленного администрирования, установив флаг **Подключиться к серверу удаленного администрирования** (Connect to Remote Administration server check). После этого доступны следующие параметры:

- **Адрес сервера** (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 Антивирус 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.
- **Доступ к серверу удаленного администрирования защищен паролем** (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 Антивирус подключается к удаленному серверу.

4.9 Лицензия

В разделе **Лицензия** (License) реализовано управление ключами лицензий для программы ESET NOD32 Антивирус и других продуктов ESET. После приобретения продукта ключи лицензии поставляются вместе с именем пользователя и паролем. 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: владелце продукта, количестве и сроке 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 лицензии истек и вы заинтересованы в продлении лицензии, нажмите кнопку **Заказать**... (Order...), чтобы перейти в наш онлайн-магазин.

5. Опытный пользователь

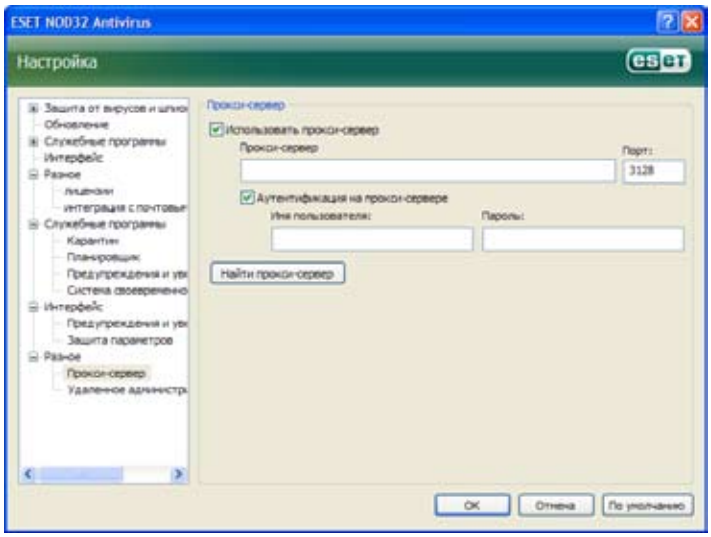
В данной главе описаны функциональные возможности ESET NOD32 Антивируса, которые могут оказаться практически полезными для опытных пользователей. Параметры настройки этих функций доступны только в расширенном режиме. Чтобы переключиться в расширенный режим, щелкните запись **Переключатель расширенного 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 Антивирус настройка прокси-сервера может быть выполнена в двух различных разделах древовидной структуры расширенной настройки.

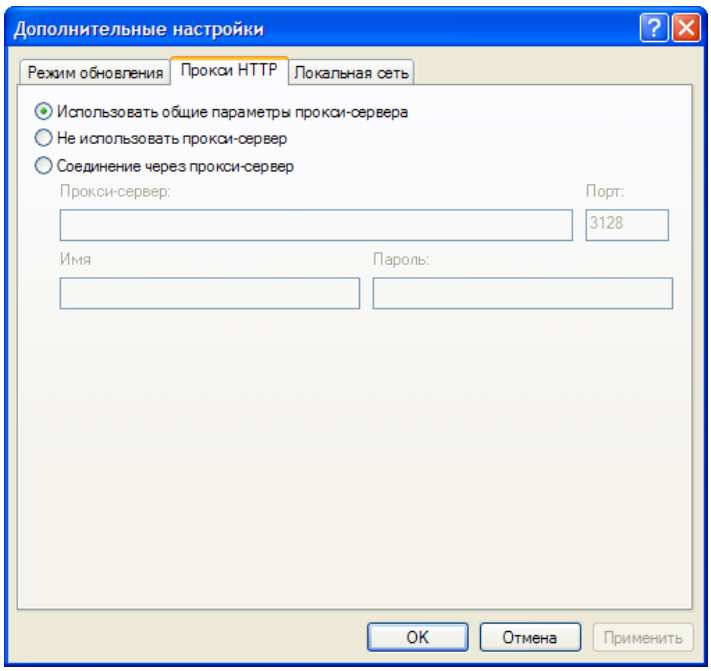
Настройки прокси-сервера можно сконфигурировать в разделе **Разное – Прокси-сервер** (Miscellaneous – Proxy server). Определение прокси-сервера на этом уровне задает глобальные настройки прокси-сервера для всей программы ESET ESET NOD32 Антивирус. Указанные здесь параметры будут использованы во всех 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 действительные **Имя пользовател**я (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.

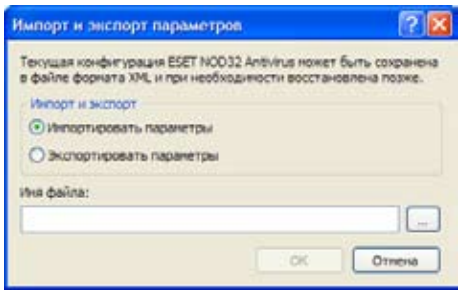
Кроме того, параметры прокси-сервера можно настроить в блоке **Дополнительная настройка обновления** (Advanced update setup) (в разделе **Обновления** (Update) дерева расширенной настройки). Эти настройки применяются к конкретному профилю обновлений и рекомендованы для переносных компьютеров. Дополнительные 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 Антивирус 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 текущих настроек системы ESET NOD32 Антивирус с целью использования ее в дальнейшем (по каким бы то ни было причинам). Возможность настройки экспорта может быть использована и пользователями, желающими применять свою конфигурацию ESET NOD32 Антивирус 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 Антивирус, 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 Антивирус 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	Каталог карантина ИМЯ_ПАПКИ
– Aind	Отобразить индикатор активности
– Auto	Просканировать все жесткие диски в режиме очистки

■ 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 этот предел, 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 карантина (дополнение к ДЕЙСТВИЮ)
– no-quarantine	Не копировать зараженные файлы в папку карантина

■ 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 чистые файлы в журнал (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 конец целевого файла. Вкратце действие компьютерного вируса можно описать следующим образом: после выполнения зараженного файла вирус самоактивируется (до того, как это сделает исходное приложение). Только после этого очередность выполнения передается исходному приложению. Вирус не может инфицировать компьютер до тех пор, пока пользователь (случайно или преднамеренно) не запустит 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,
- **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 им не требуется маскировка. 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, поскольку в нем может содержаться вредоносный код.

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

6.1.4 Руткиты

Руткиты – вредоносные программы, предоставляющие интернет-злоумышленникам неограниченный 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 интернет-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 фукнций отслеживания (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 нажатых 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 в своих 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.