ESET **NOD32 ANTIVIRUS 9**

Руководство пользователя

(для программы версии 9.0 и выше)

Microsoft® Windows® 10 / 8.1 / 8 / 7 / Vista / XP

Щелкните здесь, чтобы загрузить актуальную версию этого документа

ENJOY SAFER TECHNOLOGY™

ESET NOD32 ANTIVIRUS

Международная служба поддержки клиентов: www.eset.com/support

Версия 10/6/2015

Содержание

1. ESET NOD32 Antivirus

ESET NOD32 Antivirus представляет собой новый подход к созданию действительно комплексной системы безопасности компьютера. Новейшая версия модуля сканирования ThreatSense® работает быстро и точно для обеспечения безопасности компьютера. Таким образом, продукт представляет собой интеллектуальную систему непрерывной защиты от атак и вредоносных программ, которые могут угрожать безопасности компьютера.

ESET NOD32 Antivirus — это комплексное решение для обеспечения безопасности, в котором сочетается максимальная степень защиты и минимальное влияние на производительность компьютера. Наши современные технологии используют искусственный интеллект для предотвращения заражения вирусами, шпионскими, троянскими, рекламными программами, червями, руткитами и другими угрозами без влияния на производительность системы и перерывов в работе компьютера.

Возможности и преимущества

Улучшенный интерфейс	Интерфейс версии 9 значительным образом улучшен и упрощен с учетом результатов тестирования на предмет удобства использования. Все формулировки и уведомления, присутствующие в графическом интерфейсе пользователя, были тщательно проанализированы, и теперь интерфейс поддерживает языки с написанием справа налево, например иврит и арабский. **Интернет-справка** теперь интегрирована в ESET NOD32 Antivirus и содержит динамически обновляемые статьи по поддержке.
Защита от вирусов и шпионских программ	Упреждающее обнаружение и очистка большего количества известных и неизвестных вирусов, червей, троянских программ и руткитов. Метод **расширенной эвристики** идентифицирует даже раннее неизвестные вредоносные программы, обеспечивая защиту вашего компьютера от неизвестных угроз и нейтрализуя их до того, как они могут причинить какой-либо вред. Функции **защиты доступа в Интернет** и **защиты от фишинга** работают путем отслеживания обмена данными между веб-браузерами и удаленными серверами (в том числе SSL). Функция **защиты почтового клиента** обеспечивает контроль обмена сообщениями через протоколы POP3(S) и IMAP(S).
Регулярные обновления	Регулярное обновление базы данных сигнатур вирусов и программных модулей — наилучший способ обеспечить максимальный уровень безопасности компьютера.
ESET LiveGrid® (репутация на основе облака)	Вы можете проверить репутацию запущенных процессов и файлов непосредственно с помощью ESET NOD32 Antivirus.
Контроль устройств	Автоматически сканирует все USB-устройства флэш-памяти, карты памяти, а также компакт- и DVD-диски. Блокирует съемные носители на основании типа носителя, производителя, размера и других характеристик.
Функция HIPS	Вы можете более детально настроить поведение системы, задать правила для системного реестра, активных процессов и программ, а также точно настроить проверку состояния безопасности.
Игровой режим	Откладывает все всплывающие окна, обновления или другие действия, требующие большой нагрузки на систему, чтобы обеспечить экономию системных ресурсов для игр или других полноэкранных процессов.

Для работы функций ESET NOD32 Antivirus необходимо иметь активную лицензию. Рекомендуется продлевать лицензию ESET NOD32 Antivirus за несколько недель до истечения срока ее действия.

1.1 Новые возможности в версии 9

ESET NOD32 Antivirus версии 9 включает в себя следующие усовершенствования, перечисленные далее.

- **Улучшенный интерфейс**: графический интерфейс пользователя ESET NOD32 Antivirus полностью изменен, при этом внешний вид стал лучше, а работа с приложением — более интуитивно понятной. Теперь интерфейс поддерживает языки с написанием справа налево, например иврит и арабский. **Интернет-справка** теперь интегрирована в ESET NOD32 Antivirus и содержит динамически обновляемые статьи по поддержке.
- **Быстрая и более надежна установка**. В том числе первое сканирование, которое автоматически начинается через 20 минут после установки или перезагрузки компьютера.

Для получения дополнительной информации о новых функциях ESET NOD32 Antivirus, прочитайте статью базы знаний ESET:
Что нового в ESET Smart Security 9 и ESET NOD32 Antivirus 9?

1.2 Системные требования

Для правильной работы ESET NOD32 Antivirus система должна отвечать перечисленным ниже аппаратным и программным требованиям.

Процессор: Intel® или AMD x86–x64
Операционная система: Microsoft® Windows® 10/8.1/8/7/Vista/XP с пакетом обновления 3 (32-разрядная)/XP с пакетом обновления 2 (64-разрядная)/Home Server 2003 с пакетом обновления 2 (32-разрядная)/Home Server 2011 (64-разрядная)

1.3 Профилактика

При использовании компьютера, особенно во время работы в Интернете, необходимо помнить, что ни одна система защиты от вирусов не способна полностью устранить опасность заражений и атак. Чтобы достигнуть наивысшей степени безопасности и комфорта, важно использовать решение для защиты от вирусов надлежащим образом и следовать нескольким полезным правилам.

Регулярно обновляйте систему защиты от вирусов

Согласно статистическим данным, полученным от системы своевременного обнаружения ThreatSense, тысячи новых уникальных заражений появляются ежедневно. Они пытаются обойти существующие меры безопасности и приносят доход их авторам за счет убытков других пользователей. Специалисты исследовательской лаборатории ESET ежедневно анализируют такие угрозы, подготавливают и выпускают обновления для непрерывного повышения уровня защиты пользователей. Для максимальной эффективности этих обновлений важно настроить их надлежащим образом на компьютере пользователя. Дополнительные сведения о настройке обновлений см. в главе Настройка обновлений.

Загружайте пакеты обновлений операционной системы и других программ

Авторы вредоносных программ часто используют различные уязвимости в системе для увеличения эффективности распространения вредоносного кода. Принимая это во внимание, компании-производители программного обеспечения внимательно следят за появлением отчетов обо всех новых уязвимостях их приложений и регулярно выпускают обновления безопасности, стараясь уменьшить количество потенциальных угроз. Очень важно загружать эти обновления безопасности сразу же после их выпуска. ОС Microsoft Windows и веб-браузеры, такие как Internet Explorer, являются примерами программ, для которых регулярно выпускаются обновления безопасности.

Резервное копирование важных данных

Авторы вредоносных программ обычно не заботятся о пользователях, а действия их продуктов зачастую приводят к полной неработоспособности операционной системы и потере важной информации. Необходимо регулярно создавать резервные копии важных конфиденциальных данных на внешних носителях, таких как DVD-диски или внешние жесткие диски. Это позволяет намного проще и быстрее восстановить данные в

случае сбоя системы.

Регулярно сканируйте компьютер на наличие вирусов

Многие известные и неизвестные вирусы, черви, троянские программы и руткиты обнаруживаются модулем защиты файловой системы в режиме реального времени. Это означает, что при каждом открытии файла выполняется его сканирование на наличие признаков деятельности вредоносных программ. Рекомендуем выполнять полное сканирование компьютера по крайней мере один раз в месяц, поскольку вредоносные программы изменяются, а база данных сигнатур вирусов обновляется каждый день.

Следуйте основным правилам безопасности

Это наиболее эффективное и полезное правило из всех — всегда будьте осторожны. На данный момент для работы многих заражений (их выполнения и распространения) необходимо вмешательство пользователя. Если соблюдать осторожность при открытии новых файлов, можно значительно сэкономить время и силы, которые в противном случае будут потрачены на устранение заражений на компьютере. Ниже приведены некоторые полезные рекомендации.

- Не посещайте подозрительные веб-сайты с множеством всплывающих окон и анимированной рекламой.
- Будьте осторожны при установке бесплатных программ, пакетов кодеков и т. п.. Используйте только безопасные программы и посещайте безопасные веб-сайты.
- Будьте осторожны, открывая вложения в сообщения электронной почты (особенно это касается сообщений, рассылаемых массово и отправленных неизвестными лицами).
- Не используйте учетную запись с правами администратора для повседневной работы на компьютере.

2. Установка

Существует несколько способов установки ESET NOD32 Antivirus на компьютере. Способы установки могут отличаться в зависимости от страны и способа получения продукта.

- Интерактивный установщик можно загрузить с веб-сайта ESET. Пакет установки подходит для всех языков (выберите свой язык). Сам интерактивный установщик представляет собой файл небольшого размера; другие необходимые для установки ESET NOD32 Antivirus файлы загружаются автоматически.

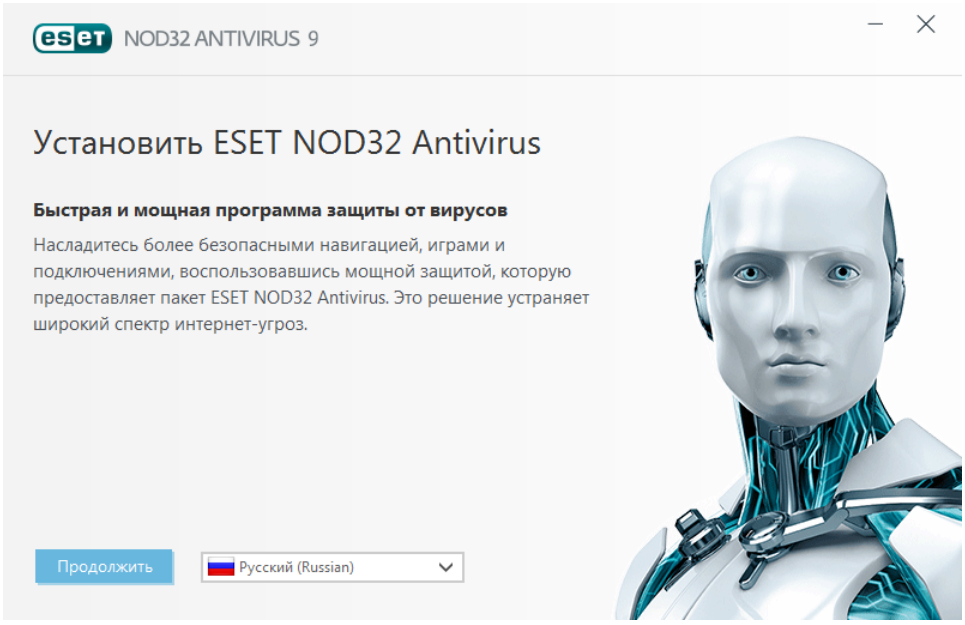
- Автономная установка: данный тип установки используется при установке программы с компакт-/DVD-диска. В рамках этого типа установки используется файл *.msi*, размер которого превышает размер файла интерактивного установщика, и не требуется подключение к Интернету или дополнительные файлы для завершения установки.

Внимание: Перед установкой ESET NOD32 Antivirus убедитесь, что на компьютере не установлены другие программы защиты от вирусов. Если на одном компьютере установлено два и более решения для защиты от вирусов, между ними может возникнуть конфликт. Рекомендуется удалить все прочие программы защиты от вирусов с компьютера. Список инструментов для удаления популярных антивирусных программ см. в статье базы знаний ESET (доступна на английском и на нескольких других языках).

2.1 Интерактивный установщик

После загрузки пакета установки *интерактивного установщика* дважды щелкните файл установки и следуйте пошаговым инструкциям в окне установщика.

Внимание! Для использования этого типа установки необходимо подключение к Интернету.



Выберите нужный язык в раскрывающемся меню и нажмите кнопку **Далее**. Подождите некоторое время, пока не будут загружены установочные файлы.

После принятия **лицензионного соглашения** отобразится запрос относительно настройки **ESET LiveGrid®**. ESET LiveGrid® помогает обеспечить незамедлительное и непрерывное информирование ESET о появлении новых угроз, чтобы защитить пользователей. С помощью этой системы вы можете отправлять новые угрозы в исследовательскую лабораторию ESET, где они анализируются, обрабатываются и добавляются в базу данных сигнатур вирусов.

По умолчанию установлен флажок **Я хочу присоединиться к ESET LiveGrid® (рекомендуется)**, который активирует данную функцию.

Следующим действием при установке является настройка обнаружения потенциально нежелательных приложений. Потенциально нежелательные приложения не обязательно являются вредоносными, но могут негативно влиять на работу операционной системы. Дополнительные сведения см. в главе Потенциально нежелательные приложения.

Чтобы запустить процесс установки, нажмите кнопку **Установить**.

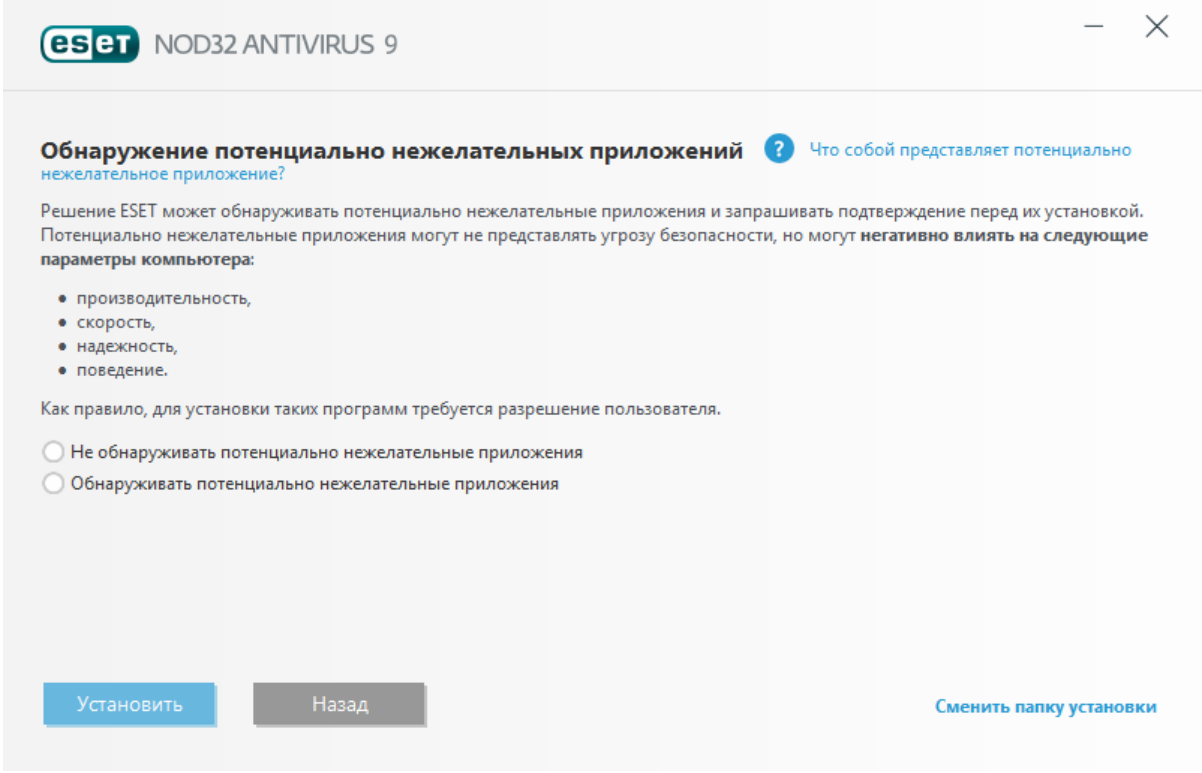
2.2 Автономная установка

После запуска пакета автономной установки (.msi) мастер установки поможет установить программу.

Сначала программа проверяет наличие более новой версии ESET NOD32 Antivirus. При обнаружении более новой версии вы будете уведомлены об этом на первом этапе установки. Если выбрать команду **Загрузить и установить новую версию**, будет загружена новая версия, после чего установка будет продолжена. Этот флажок отображается, если доступна более новая версия программы, чем та, которая устанавливается.

На следующем этапе на экран будет выведено лицензионное соглашение с конечным пользователем. Прочтите его и нажмите кнопку **Принять**, чтобы подтвердить свое согласие с условиями лицензионного соглашения с конечным пользователем. После принятия установка продолжится.

Дополнительные указания по поводу этапов установки, **ThreatSense** и **обнаружении потенциально нежелательных приложений** приведены в упомянутом выше разделе (см. раздел Интерактивный установщик).



2.2.1 Дополнительно

После выбора варианта **Дополнительно** необходимо будет выбрать папку для установки. По умолчанию программа устанавливается в указанную ниже папку.

C:\Program Files\ESET\ESET NOD32 Antivirus

Нажмите кнопку **Обзор...**, чтобы изменить папку (не рекомендуется).

Нажмите кнопку **Далее**, чтобы настроить интернет-соединение. Если используется прокси-сервер, он должен быть корректно сконфигурирован для обеспечения обновления сигнатур вирусов. Если вы не уверены, что для подключения к Интернету используется прокси-сервер, выберите параметр **Использовать параметры подключения Internet Explorer (рекомендуется)** и нажмите кнопку **Далее**. Если прокси-сервер не используется, выберите вариант **Я не использую прокси-сервер**.

Для конфигурирования параметров прокси-сервера выберите вариант **Я использую прокси-сервер** и нажмите кнопку **Далее**. Введите IP-адрес или URL-адрес прокси-сервера в поле **Адрес**. В поле **Порт** укажите порт, по которому этот прокси-сервер принимает запросы на соединение (по умолчанию 3128). Если прокси-сервер требует аутентификации, введите правильные **имя пользователя** и **пароль**, которые необходимы для доступа к нему. Параметры прокси-сервера также по желанию могут быть скопированы из параметров Internet Explorer. Нажмите **Применить** и подтвердите выбор.

При выборочной установке можно указать, как в системе будет обрабатываться автоматическое обновление программы. Нажмите **Изменить...** для доступа к дополнительным параметрам.

Если нет необходимости обновлять компоненты программы, выберите вариант **Никогда не обновлять компоненты программы**. Выберите параметр **Запросить подтверждение перед загрузкой компонентов**, чтобы перед каждой попыткой загрузить компоненты программы отображалось окно подтверждения. Для автоматической загрузки обновлений компонентов программы выберите вариант **Выполнять обновление компонентов программы, если доступно**.

ПРИМЕЧАНИЕ. После обновления компонентов программы обычно нужно перезагрузить компьютер. Рекомендуется выбрать вариант **Если необходимо, перезапустить компьютер без уведомления**.

В следующем окне предлагается создать пароль для защиты параметров программы. Выберите вариант **Защита параметров конфигурации паролем** и введите пароль в поле **Новый пароль** и **Подтвердить новый пароль**. Он будет необходим для доступа к параметрам ESET NOD32 Antivirus, а также для их изменения. Когда в обоих полях введены совпадающие пароли, нажмите кнопку **Далее**, чтобы продолжить.

Для выполнения следующих этапов установки (**ThreatSense** и **Обнаружение потенциально нежелательных приложений**) следуйте инструкциям, которые содержатся в разделе «Интерактивный установщик» (см. раздел Интерактивный установщик).

Чтобы отключить установку первого сканирования, которое обычно выполняется после завершения установки для проверки наличия вредоносного кода, снимите флажок рядом с пунктом **Включить сканирование после установки**. Нажмите **Установить** в окне **Все готово к установке**, чтобы завершить процесс установки.

2.3 Распространенные проблемы при установке

Если в процессе установки возникают какие-либо проблемы, см. наш список распространенных проблем при установке и их решений, чтобы найти решение для своей проблемы.

2.4 Активация программы

После завершения установки будет предложено активировать программный продукт.

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

- Если вы приобрели коробочную розничную версию программы, активируйте ее, используя **Лицензионный ключ**. Лицензионный ключ, как правило, расположен внутри упаковки продукта или на ее тыльной стороне. Для успешного выполнения активации лицензионный ключ необходимо ввести в том виде, в котором он предоставлен. Лицензионный ключ — это уникальная строка в формате XXXX-XXXX-XXXX-XXXX-XXXX или XXXX-XXXXXXXX, которая используется для идентификации владельца и активации лицензии.
- Если вы хотите оценить программу ESET NOD32 Antivirus, прежде чем покупать ее, выберите вариант **Лицензия на бесплатную пробную версию**. Укажите свои адрес электронной почты и страну, чтобы активировать ESET NOD32 Antivirus на ограниченный период времени. Тестовая лицензия будет отправлена вам по электронной почте. Каждый пользователь может активировать только одну пробную лицензию.
- Если у вас нет лицензии, но вы хотите купить ее, выберите вариант «Приобрести лицензию». В результате откроется веб-сайт местного распространителя ESET.

Если вы хотите сначала оценить программный продукт, не активируя его сразу же (например, чтобы сделать это позднее), выберите вариант **Активировать позже**.

Активировать копию ESET NOD32 Antivirus также можно из самой программы. Правой кнопкой мыши щелкните значок ESET NOD32 Antivirus  на панели задач и выберите пункт **Активировать продукт** в меню программы.

2.5 Ввод лицензионного ключа

Для того чтобы использовать программу наилучшим образом, необходимо регулярно обновлять ее. Это возможно только в том случае, если в окне **Настройка обновлений** указан правильный **лицензионный ключ**.

Если лицензионный ключ не был указан при установке, это можно сделать сейчас. В главном окне программы нажмите **Справка и поддержка**, а затем выберите **Активировать лицензию** и в окне «Активация программы» введите данные лицензии, полученные в комплекте с решением ESET для обеспечения безопасности.

При вводе **Лицензионного ключа** важно указывать его именно в том виде, в котором он получен.

- Это уникальная строка в формате XXXX-XXXX-XXXX-XXXX-XXXX, которая используется для идентификации владельца и активации лицензии.

Во избежание неточностей рекомендуется скопировать Лицензионный ключ из электронного письма с

регистрационными данными и вставить его в нужное поле.

2.6 Обновление до новой версии

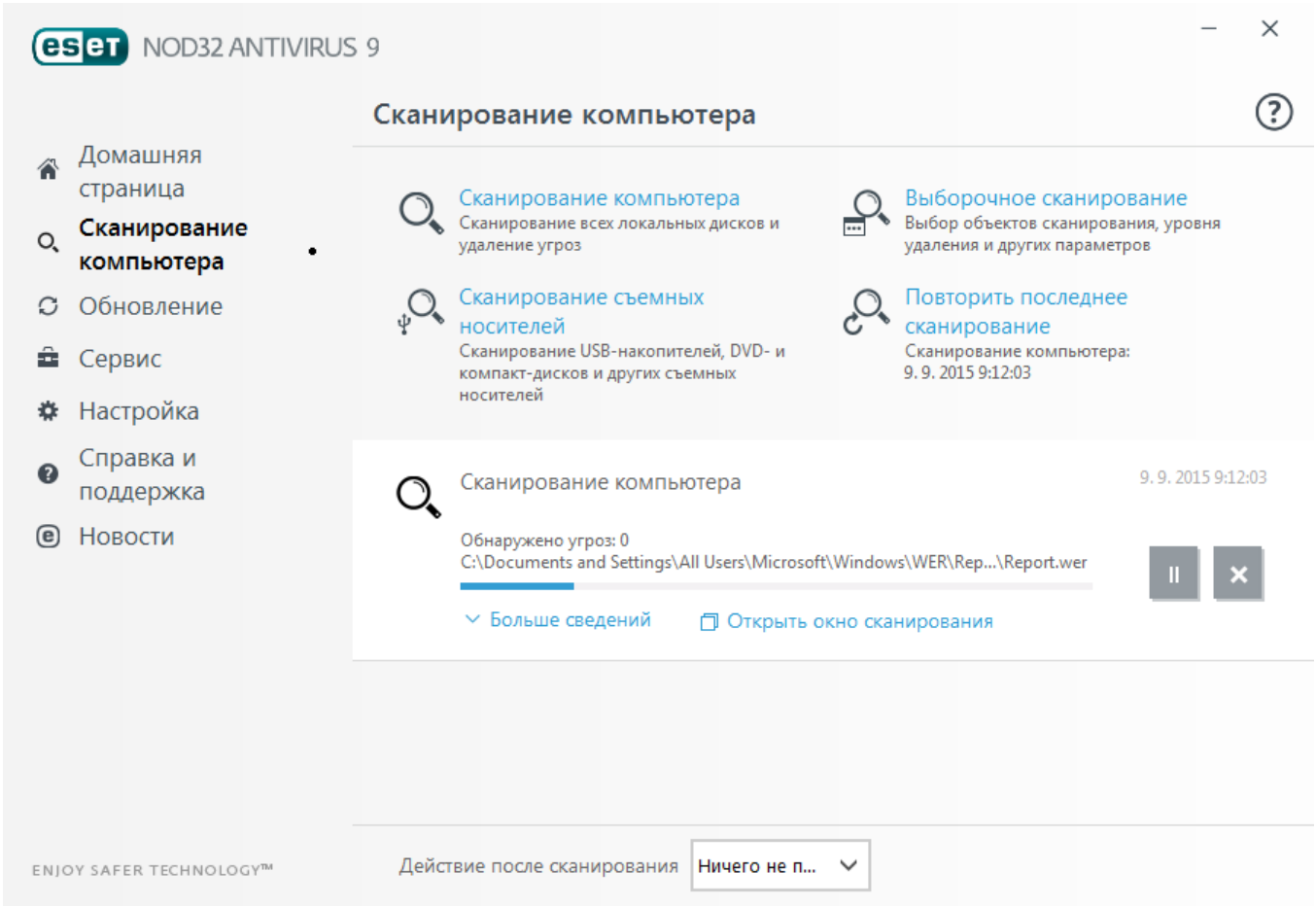
Новые версии ESET NOD32 Antivirus выпускаются для реализации улучшений или исправления проблем, которые не могут быть устранены автоматическим обновлением модулей программы. Обновление до новой версии можно выполнить одним из нескольких способов.

1. Автоматически путем обновления программы.
   Поскольку обновления программы распространяются среди всех пользователей и могут повлиять на некоторые системные конфигурации, они выпускаются только после длительного тестирования с целью обеспечения бесперебойной работы на всех возможных конфигурациях. Чтобы перейти на новую версию сразу после ее выпуска, воспользуйтесь одним из перечисленных ниже способов.
2. Вручную в главном окне программы путем нажатия кнопки **Проверить наличие обновлений** в разделе **Обновление**.
3. Вручную путем загрузки и установки новой версии поверх предыдущей.

2.7 Первое сканирование после установки

Через 20 минут после установки ESET NOD32 Antivirus или перезагрузки компьютера начнется сканирование компьютера на наличие вредоносного кода.

Сканирование компьютера также можно запустить вручную в главном окне программы, выбрав **Сканирование компьютера** > **Сканировать компьютер**. Для получения дополнительных сведений о сканировании компьютера см. раздел Сканирование компьютера.



3. Руководство для начинающих

В этом разделе приводятся общие сведения о программном обеспечении ESET NOD32 Antivirus и его основных параметрах.

3.1 Главное окно программы

Главное окно ESET NOD32 Antivirus разделено на две основные части. Основное окно справа содержит информацию, относящуюся к параметру, выбранному в главном меню слева.

Ниже описаны пункты главного меню.

Домашняя страница - этот пункт предоставляет информацию о состоянии защиты ESET NOD32 Antivirus.

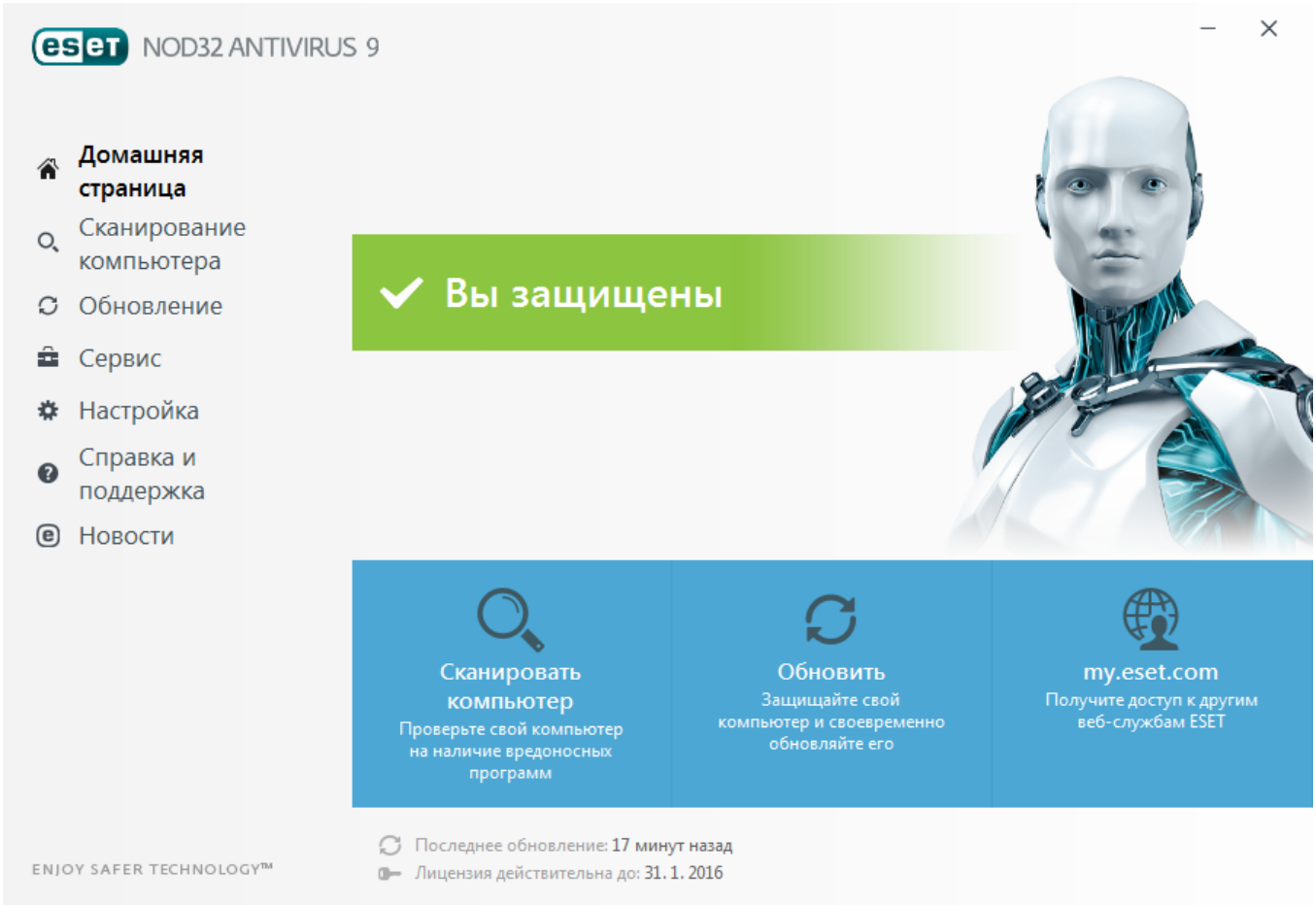
Сканирование компьютера: настройка и запуск сканирования компьютера или создание выборочного сканирования.

Обновление - выводит информацию об обновлениях базы данных сигнатур вирусов.

Сервис - позволяет открыть файлы журнала, статистику защиты, программу мониторинга, запущенные процессы, планировщик, ESET SysInspector и ESET SysRescue.

Настройка: — с помощью этого параметра можно настроить уровень безопасности для компьютера, Интернета.

Справка и поддержка — обеспечивает доступ к файлам справки, базе знаний ESET, веб-сайту ESET и ссылкам для отправки запросов в службу поддержки.

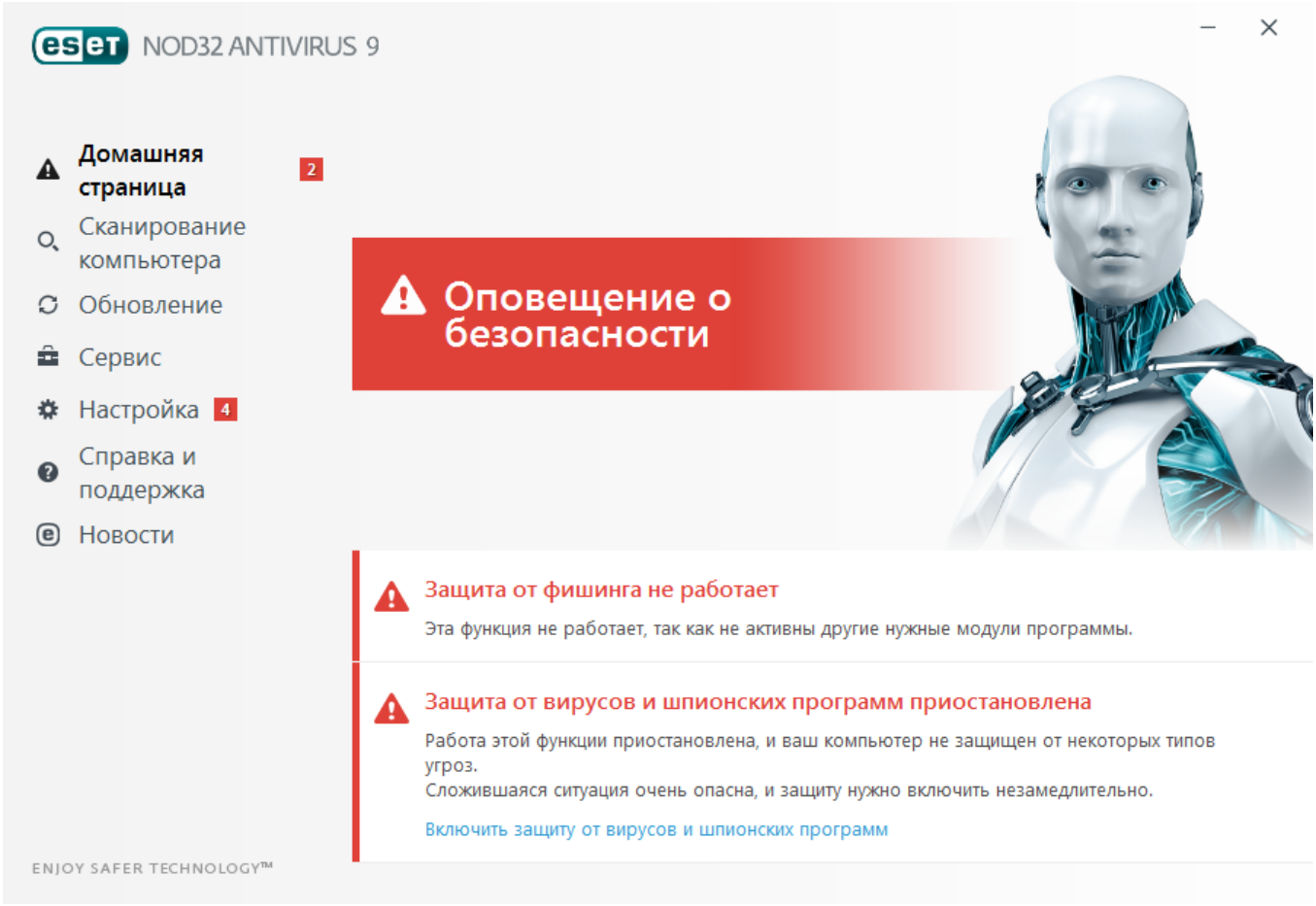


На экране **Домашняя страница** отображаются важные сведения о текущем уровне защиты компьютера. В окне состояния отображаются часто используемые функции ESET NOD32 Antivirus. Здесь также указаны сведения о последнем обновлении и дата окончания срока действия программы.

Зеленый значок и зеленый статус **Максимальная защита** сообщают о максимальном уровне защиты.

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

Если модуль активной защиты работает правильно, значок состояния защиты будет зеленым. Красный восклицательный знак или оранжевый значок уведомления означает, что максимальная степень защиты не обеспечивается. В **Главном меню** будут отображаться дополнительные сведения о состоянии защиты каждого модуля и предложены решения для восстановления полной защиты. Для изменения состояния отдельного модуля щелкните **Настройка** и выберите необходимый модуль.



Красный значок и красная надпись «Максимальная защита» не обязательно сигнализируют о критических проблемах.
Для отображения такого состояния может быть несколько причин.

- **Программа не активирована**: можно активировать программу ESET NOD32 Antivirusна **Домашней странице**, выбрав **Активировать продукт** или **Купить сейчас** возле сведений о состоянии защиты.
- **База данных сигнатур вирусов устарела**: эта ошибка появится после нескольких неудачных попыток обновить базу данных сигнатур вирусов. Рекомендуется проверить параметры обновлений. Наиболее частая причина этой ошибки — неправильно введенные данные для аутентификации или неверно сконфигурированные параметры подключения.
- **Защита от вирусов и шпионских программ отключена**: можно снова включить защиту от вирусов и шпионских программ, щелкнув ссылку **Запустить все модули защиты от вирусов и шпионских программ**.
- **Срок действия лицензии истек**: об этом сигнализирует красный значок состояния защиты. С этого момента программа больше не сможет выполнять обновления. Для продления лицензии следуйте инструкциям в окне предупреждения.

Оранжевый цвет значка указывает на то, что действует ограниченная защита. Например, существуют проблемы с обновлением программы или заканчивается срок действия лицензии.
Для отображения такого состояния может быть несколько причин.

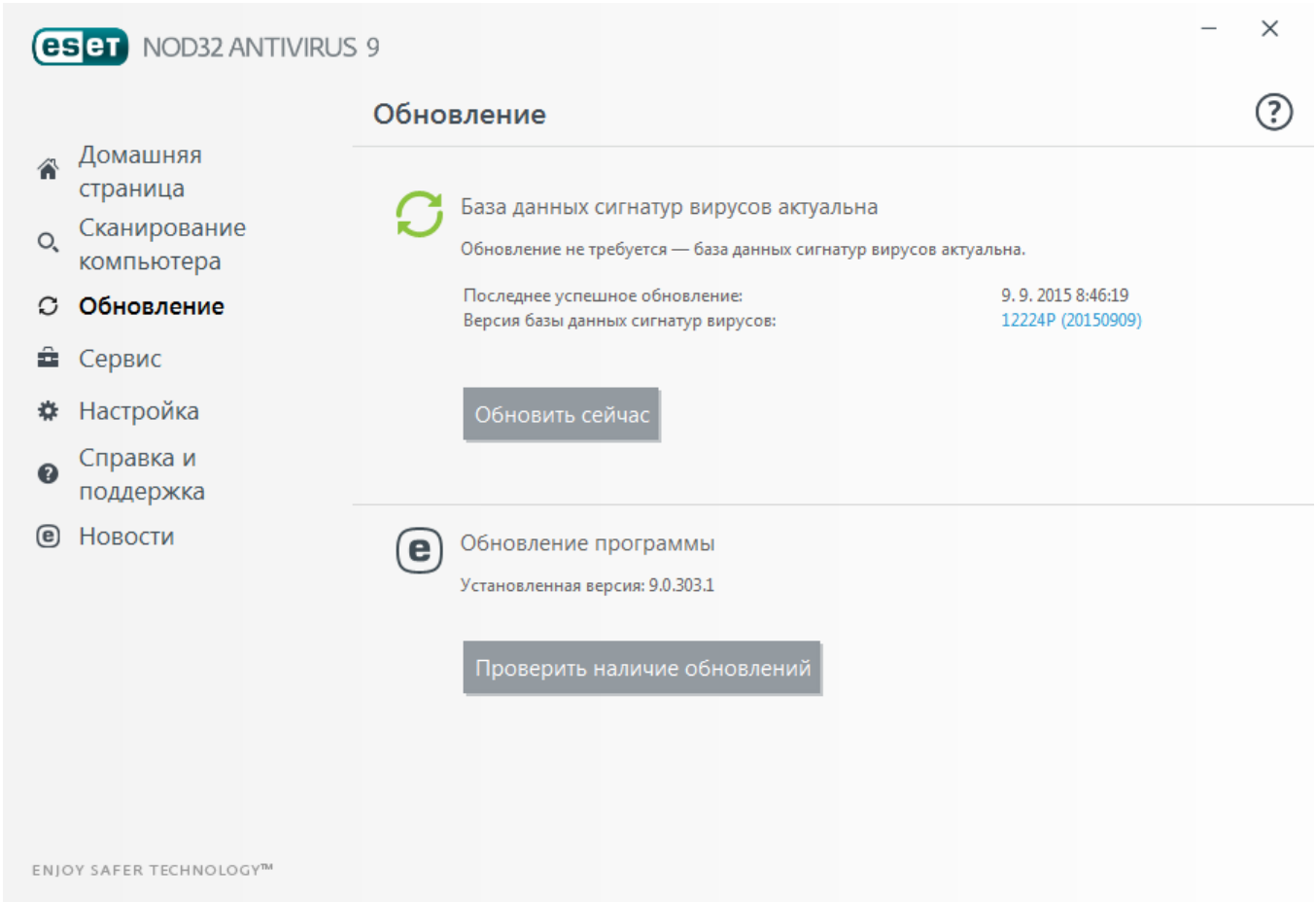
- **Игровой режим включен** : включение Игрового режима представляет потенциальный риск для безопасности. При включении этой функции блокируются все всплывающие окна и останавливаются все запланированные задачи.
- **Срок действия вашей лицензии скоро закончится**: признаком наличия этой проблемы является появление восклицательного знака в значке состояния защиты рядом с системными часами. После окончания срока действия лицензии программа больше не сможет выполнять обновления, а значок состояния защиты станет красным.

Если предложенные решения не позволяют устранить проблему, выберите элемент **Справка и поддержка** и просмотрите файлы справки или поищите нужную информацию в базе знаний ESET. Если вам по-прежнему нужна помощь, отправьте свой запрос в службу поддержки. Ее специалисты оперативно ответят на ваши вопросы и помогут найти решение.

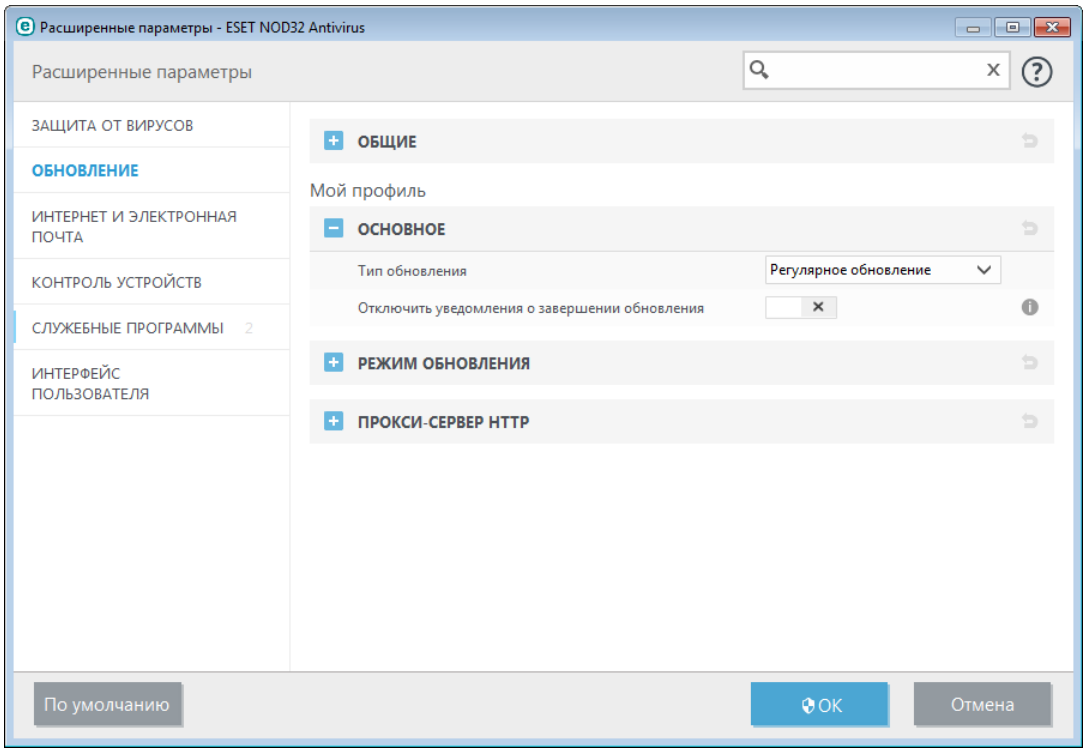
3.2 Обновления

Обновление базы данных сигнатур вирусов и компонентов программы является важной частью обеспечения защиты компьютера от вредоносного кода. Обратите особое внимание на их настройку и работу. В главном меню выберите пункт **Обновление**, а затем щелкните **Обновить сейчас**, чтобы проверить наличие обновлений базы данных сигнатур вирусов.

Если имя пользователя и пароль не вводились в процессе активации ESET NOD32 Antivirus, на этом этапе будет предложено указать их.

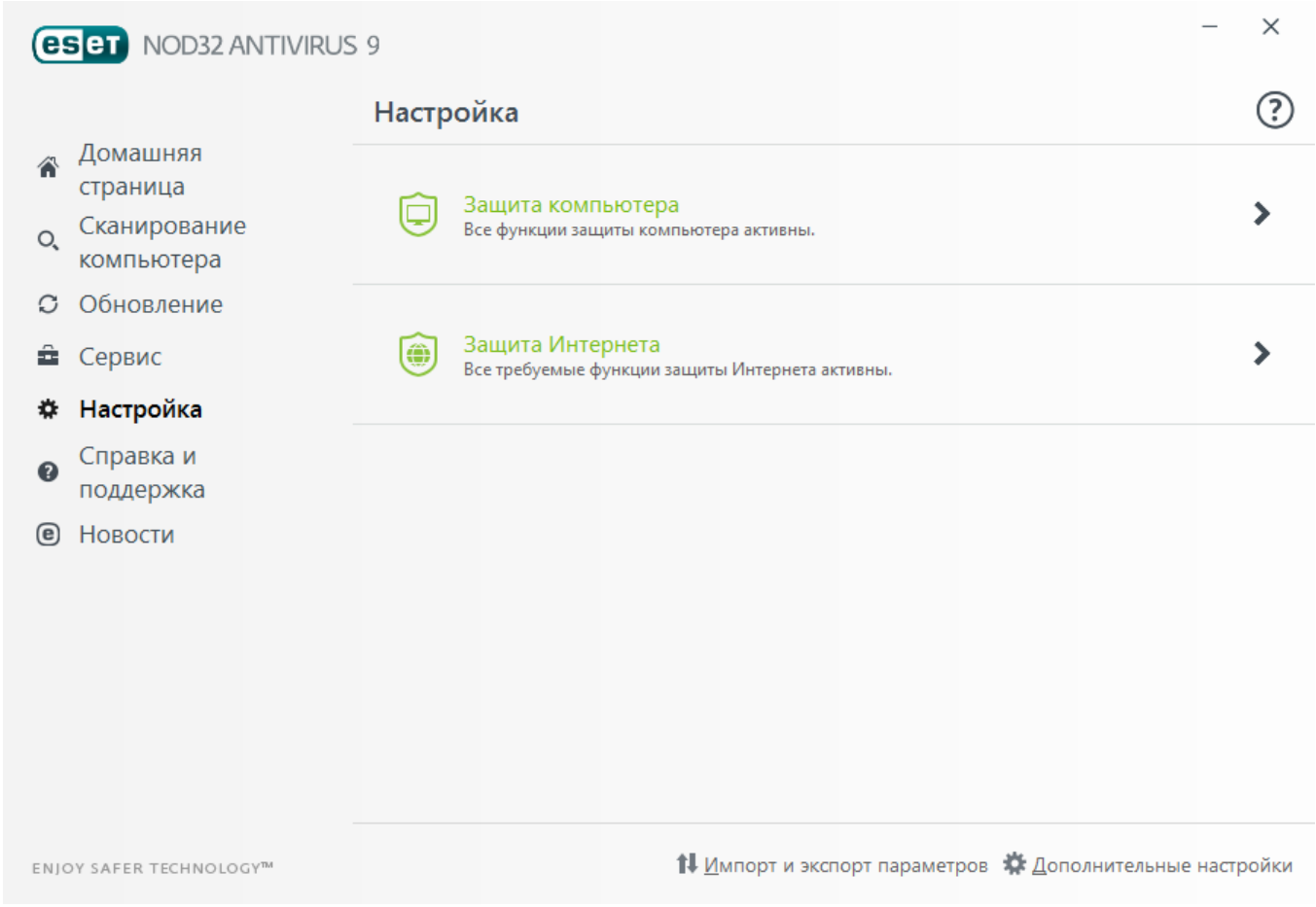


В окне **Дополнительные настройки** (выберите пункт **Настройка** в главном меню, после чего щелкните элемент **Дополнительные настройки** или нажмите клавишу F5) содержатся расширенные параметры обновления. Для настройки расширенных параметров обновления, таких как режим обновления, доступ через прокси-сервер и подключения к локальной сети, откройте соответствующую вкладку в окне **Обновление**.



4. Работа с ESET NOD32 Antivirus

Параметры настройки ESET NOD32 Antivirus дают пользователю возможность настраивать уровни защиты компьютера.



Меню **Настройка** содержит следующие разделы.

Защита компьютера

Защита в Интернете

Выберите компонент, чтобы настроить дополнительные параметры для соответствующего защитного модуля.

В настройках **защиты компьютера** можно включать и отключать следующие компоненты.

- **Защита файловой системы в режиме реального времени**: при открытии, создании или запуске любого файла на вашем компьютере выполняется сканирование на наличие вредоносного кода.
- **HIPS**: система предотвращения вторжений на узел отслеживает события в операционной системе и реагирует на них в соответствии с имеющимся набором правил.
- **Игровой режим**: включает или отключает игровой режим. После включения игрового режима на экран будет выведено предупреждение (о потенциальной угрозе безопасности), а для оформления главного окна будет применен оранжевый цвет.

В настройках **защиты в Интернете** можно включать и отключать следующие компоненты.

- **Защита доступа в Интернет**: если этот параметр включен, весь трафик по протоколам HTTP и HTTPS сканируется на наличие вредоносных программ.
- **Защита почтового клиента**: обеспечивает контроль обмена данными по протоколам POP3 и IMAP.
- **Защита от фишинга**: обеспечивает фильтрацию веб-сайтов, заподозренных в распространении содержимого, которое предназначено для манипулирования пользователем, с тем чтобы получить от него конфиденциальную информацию.

Для повторного включения отключенного компонента безопасности щелкните ползунок таким образом, чтобы отобразился зеленый флажок.

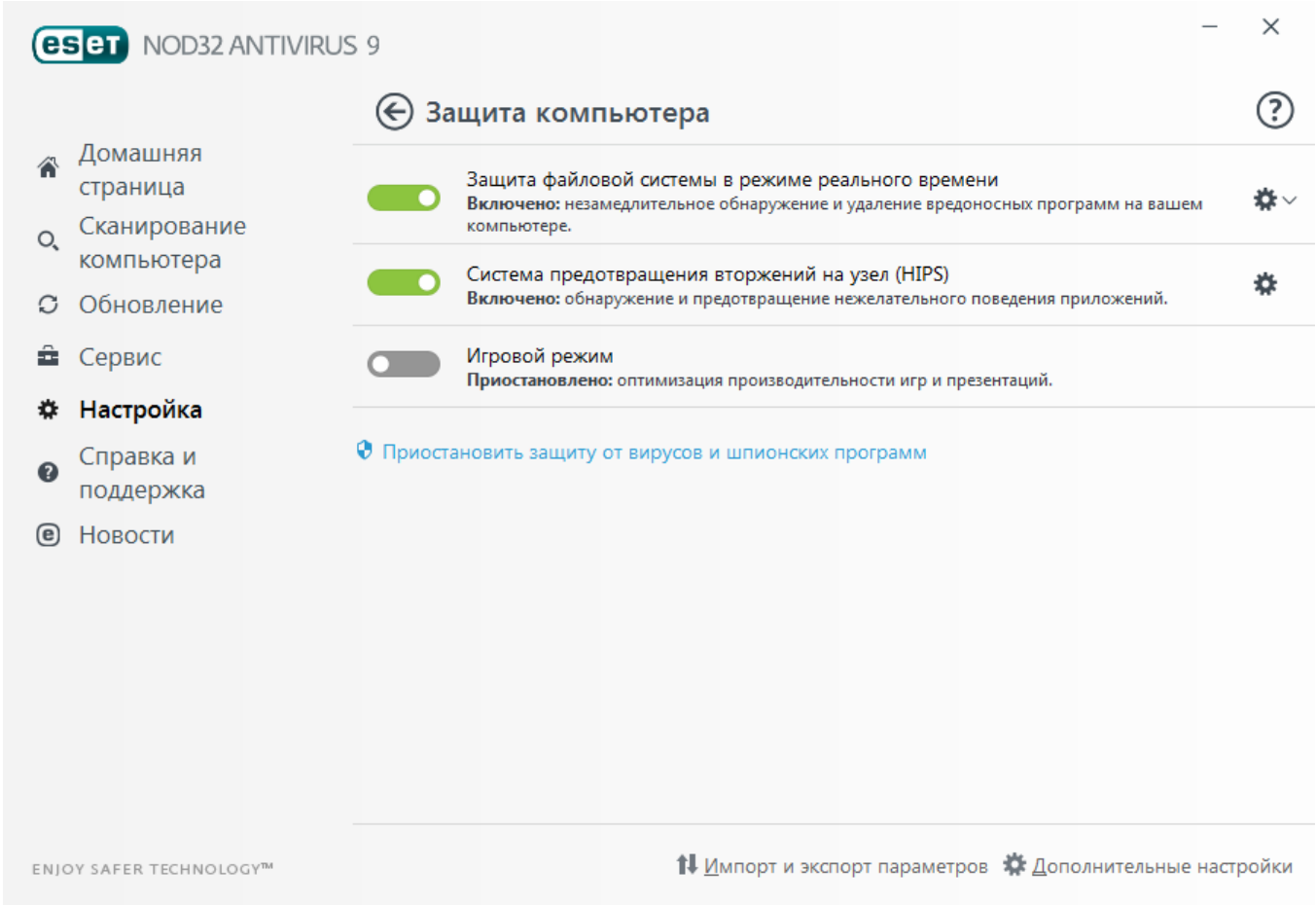
ПРИМЕЧАНИЕ. При отключении защиты таким способом все отключенные модули защиты будут повторно включены после перезагрузки компьютера.

В нижней части окна настройки есть дополнительные параметры. Чтобы выполнить более подробную настройку параметров для каждого модуля, перейдите по ссылке **Дополнительные настройки**. Чтобы загрузить параметры настройки из файла конфигурации в формате *XML* или сохранить текущие параметры настройки в файл конфигурации, воспользуйтесь функцией **Импорт и экспорт параметров**.

4.1 Защита компьютера

В окне «Настройка» щелкните параметр «Защита компьютера», чтобы просмотреть общие сведения обо всех модулях защиты. Чтобы временно отключить тот или иной модуль, щелкните . Обратите внимание, что при этом будет ослаблена защита вашего компьютера. Щелкните элемент рядом с модулем защиты, чтобы получить доступ к дополнительным настройкам для него.

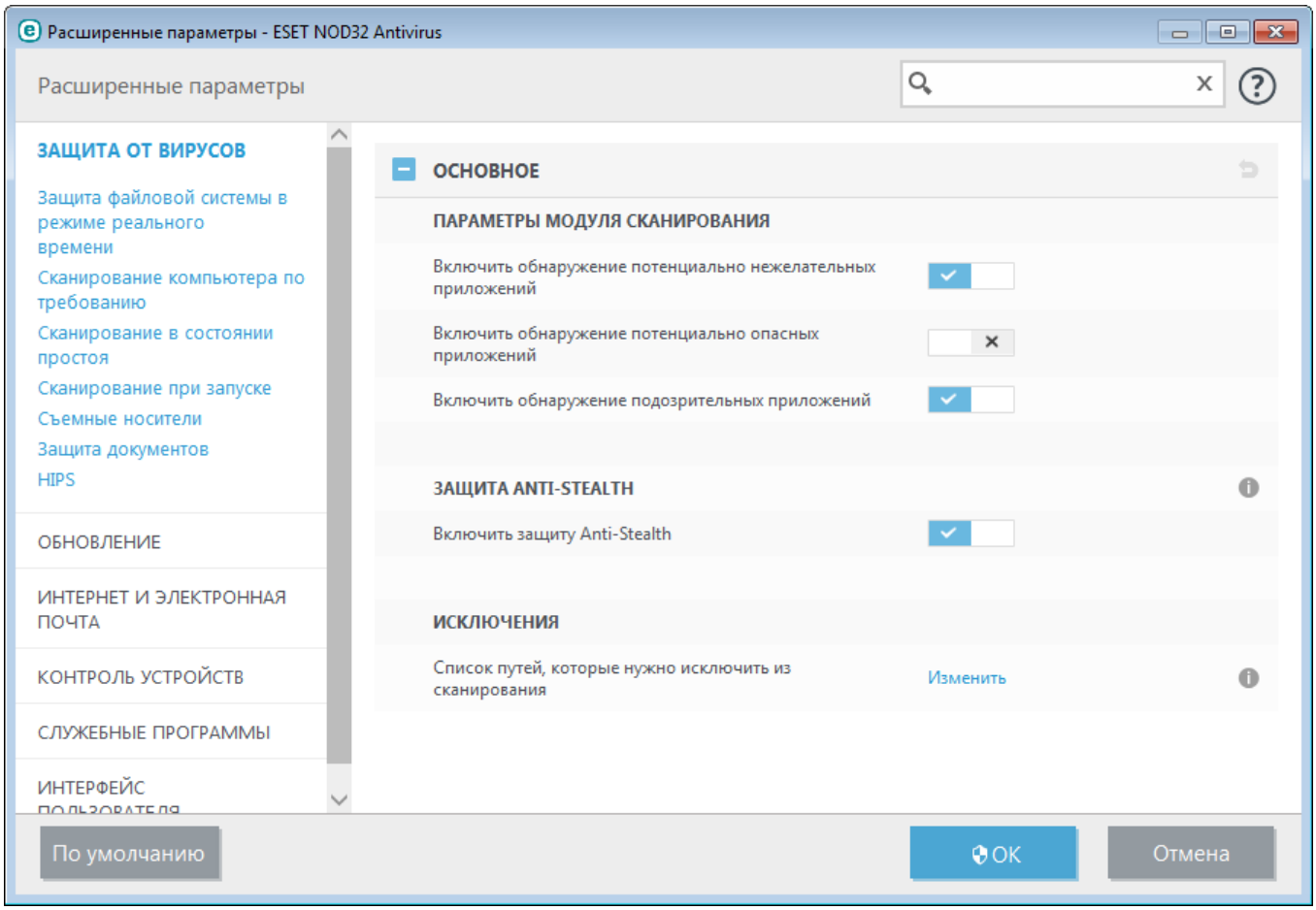
Щелкните элемент > **Изменить исключения** рядом с элементом**Защита файловой системы в режиме реального времени**, чтобы открыть окно настроек Исключение, в котором можно исключить файлы и папки из сканирования.



Приостановить защиту от вирусов и шпионских программ: отключение всех модулей защиты от вирусов и шпионских программ. При отключении защиты отображается соответствующее окно. С его помощью можно задать время, на которое будет отключена защита, выбрав значение в раскрывающемся меню **Время**. Нажмите кнопку **ОК** для подтверждения.

4.1.1 Защита от вирусов

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



Параметры модуля сканирования позволяют для всех модулей защиты (например, защиты файловой системы в режиме реального времени, защиты доступа в Интернет и т. д.) включить или отключить обнаружение следующих элементов.

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

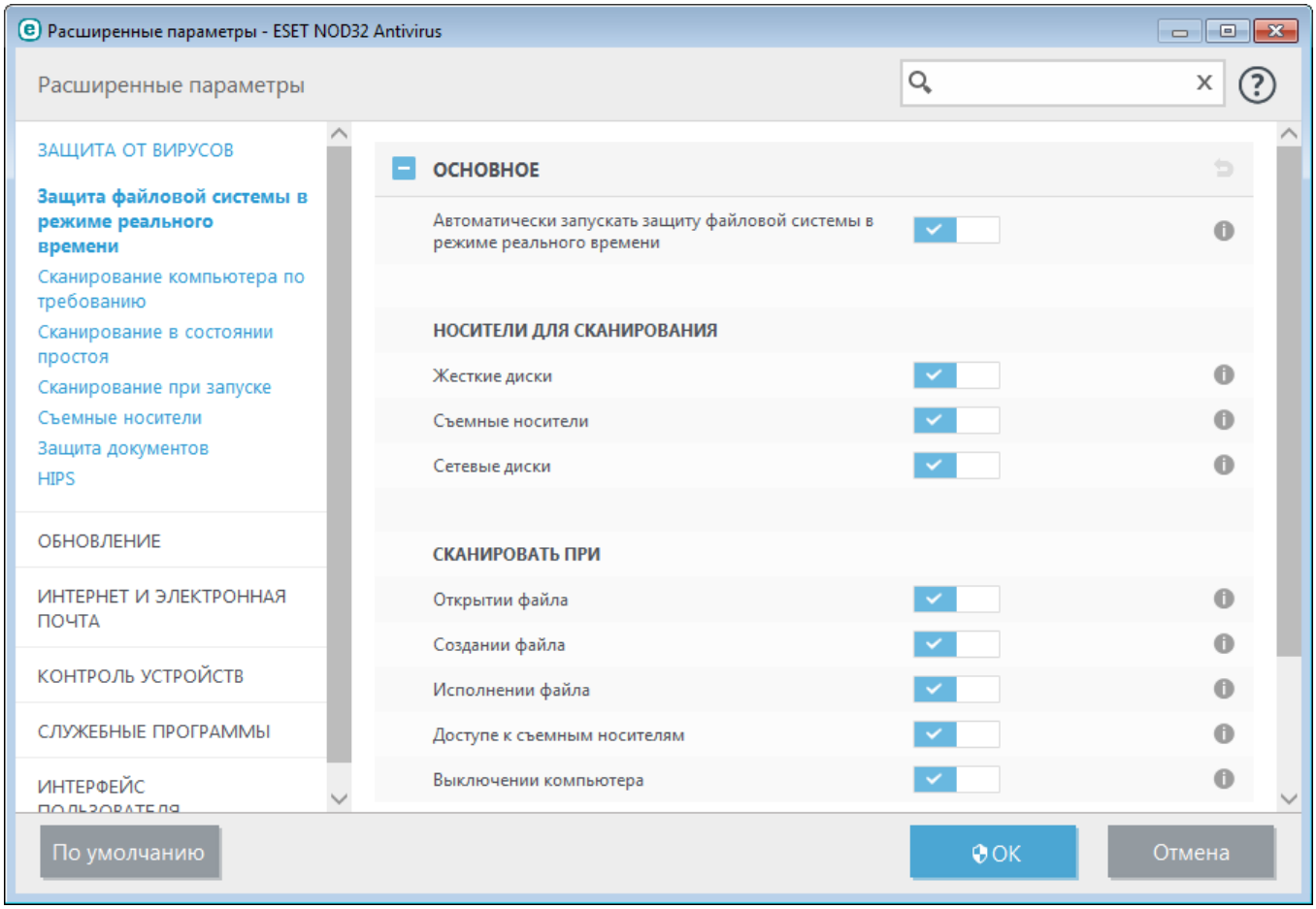
Технология Anti-Stealth является сложной системой, обеспечивающей обнаружение опасных программ, таких как руткиты, которые могут скрываться от операционной системы. Это значит, что такие программы невозможно обнаружить с помощью обычных методов тестирования.

Исключения позволяют исключить файлы и папки из сканирования. Чтобы обеспечить сканирование всех объектов на наличие угроз, рекомендуется создавать исключения только в случае крайней необходимости. Однако в некоторых случаях все же необходимо исключать объекты, например большие базы данных, которые замедляют работу компьютера при сканировании, или программы, конфликтующие с процессом

сканирования. Сведения об исключении объекта из области сканирования см. в разделе Исключения.

4.1.1.1 Защита файловой системы в режиме реального времени

Функция защиты файловой системы в режиме реального времени контролирует все события в системе, относящиеся к защите от вирусов. При открытии, создании или запуске файлов все они сканируются на наличие вредоносного кода. Защита файловой системы в режиме реального времени запускается при загрузке операционной системы.



По умолчанию функция защиты файловой системы в режиме реального времени запускается при загрузке системы и обеспечивает постоянное сканирование. В особых случаях (например, при возникновении конфликта с другим модулем сканирования в реальном времени) защиту файловой системы в реальном времени можно выключить. Для этого нужно открыть окно **Дополнительные настройки** и в разделе **Защита файловой системы в реальном времени** > **Основное** снять флажок **Автоматически запускать защиту файловой системы в режиме реального времени**.

Носители для сканирования

По умолчанию все типы носителей сканируются на наличие возможных угроз.

Локальные диски: контролируются все жесткие диски, существующие в системе.
Съемные носители: контролируются компакт-/DVD-диски, USB-устройства хранения, Bluetooth-устройства и т. п.
Сетевые диски: сканируются все подключенные сетевые диски.

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

Сканировать при

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

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

Защита файловой системы в режиме реального времени проверяет все типы носителей и запускается различными событиями, такими как доступ к файлу. За счет использования методов обнаружения ThreatSense (как описано в разделе Настройка параметров модуля ThreatSense) защиту файловой системы в режиме реального времени можно настроить для создаваемых и уже существующих файлов по-разному. Например, можно настроить защиту файловой системы в режиме реального времени так, чтобы она более тщательно отслеживала вновь созданные файлы.

Для снижения влияния на производительность компьютера при использовании защиты в режиме реального времени файлы, которые уже сканировались, не сканируются повторно, пока не будут изменены. Файлы сканируются повторно сразу после каждого обновления базы данных сигнатур вирусов. Такое поведение контролируется с использованием **оптимизации Smart**. Если **Оптимизация Smart** отключена, все файлы сканируются при каждом к ним доступе. Для изменения этого параметра нажмите F5, чтобы открыть окно **Дополнительные настройки**, и перейдите к разделу **Защита от вирусов** > **Защита файловой системы в режиме реального времени**. Последовательно щелкните элементы **Настройка параметров модуля ThreatSense** > **Другое** и снимите или установите флажок **Включить интеллектуальную оптимизацию**.

4.1.1.1.1 Дополнительные параметры ThreatSense

Дополнительные параметры ThreatSense для только что созданных и измененных файлов

Вероятность заражения только что созданных или измененных файлов выше по сравнению с аналогичным показателем для существующих файлов. Именно поэтому программа проверяет эти файлы с дополнительными параметрами сканирования. ESET NOD32 Antivirus вместе с обычными методами сканирования, основанными на сигнатурах, применяет расширенную эвристики, что делает возможным обнаружение новых угроз еще до выпуска обновлений базы данных сигнатур вирусов. В дополнение к только что созданным файлам выполняется также сканирование **самораспаковывающихся архивов** (.sfx) и **упаковщиков** (исполняемых файлов с внутренним сжатием). По умолчанию проверяются архивы с глубиной вложенности до 10 независимо от их фактического размера. Для изменения параметров сканирования архивов снимите флажок **Параметры сканирования архива по умолчанию**.

Дополнительные параметры ThreatSense для исполняемых файлов

Расширенный эвристический анализ при запуске файлов: по умолчанию при запуске файлов применяется расширенная эвристика. Если этот параметр включен, настоятельно рекомендуется включить оптимизацию Smart и ESET LiveGrid®, чтобы уменьшить воздействие на производительность системы.

Расширенная эвристика запуска файлов со съемных носителей: прежде чем разрешить запуск кода со съемного носителя, система расширенного эвристического анализа эмулирует код в виртуальной среде и оценивает его поведение.

4.1.1.1.2 Уровни очистки

Защита в режиме реального времени предусматривает три уровня очистки (для доступа к ним щелкните **Настройка параметров модуля ThreatSense** в разделе **Защита файловой системы в режиме реального времени**, а затем щелкните **Очистка**).

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

Стандартная очистка: программа пытается автоматически очистить или удалить зараженный файл на основе предварительно определенного действия (в зависимости от типа заражения). Обнаружение и удаление зараженных файлов сопровождается уведомлением, отображающимся в правом нижнем углу экрана. Если

невозможно выбрать правильное действие автоматически, программа предложит выбрать другое действие. То же самое произойдет в том случае, если предварительно определенное действие невозможно выполнить.

Тщательная очистка: программа очищает или удаляет все зараженные файлы. Исключение составляют только системные файлы. Если очистка невозможна, на экран выводится окно предупреждения, в котором пользователю предлагается выполнить определенное действие.

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

4.1.1.1.3 Момент изменения конфигурации защиты в режиме реального времени

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

После установки ESET NOD32 Antivirus все параметры оптимизированы для максимальной защиты системы. Для восстановления настроек по умолчанию щелкните ↩ возле каждой вкладки в окне (**Дополнительные настройки** > **Антивирус** > **Защита файловой системы в режиме реального времени**).

4.1.1.1.4 Проверка модуля защиты в режиме реального времени

Чтобы убедиться, что защита в режиме реального времени работает и обнаруживает вирусы, используйте проверочный файл eicar.com. Этот тестовый файл является безвредным, и его обнаруживают все программы защиты от вирусов. Файл создан компанией EICAR (Европейский институт антивирусных компьютерных исследований) для проверки функционирования программ защиты от вирусов. Файл доступен для загрузки с веб-сайта http://www.eicar.org/download/eicar.com.

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

В этом разделе описаны проблемы, которые могут возникнуть при использовании защиты в режиме реального времени, и способы их устранения.

Защита файловой системы в режиме реального времени отключена

Если защита файловой системы в режиме реального времени непреднамеренно была отключена пользователем, ее нужно включить. Для повторной активации защиты в режиме реального времени в главном окне программы перейдите в раздел **Настройка** и нажмите **Защита компьютера** > **Защита файловой системы в режиме реального времени**.

Если защита файловой системы в режиме реального времени не запускается при загрузке системы, обычно это связано с тем, что отключен параметр **Автоматический запуск защиты файловой системы в режиме реального времени**. Чтобы включить этот параметр, перейдите в раздел «Дополнительные настройки» (**F5**) и последовательно выберите **Защита от вирусов** > **Защита файловой системы в режиме реального времени**.

Защита в режиме реального времени не обнаруживает и не очищает заражения

Убедитесь в том, что на компьютере не установлены другие программы защиты от вирусов. Если на компьютере установлено сразу две антивирусных программы, они могут конфликтовать между собой. Перед установкой ESET рекомендуется удалить с компьютера все прочие программы защиты от вирусов.

Защита файловой системы в режиме реального времени на запускается

Если защита не запускается при загрузке системы, но функция **Автоматический запуск защиты файловой системы в режиме реального времени** включена, возможно, возник конфликт с другими приложениями. Чтобы получить помощь для решения этой проблемы, обратитесь в службу поддержки клиентов ESET.

4.1.1.2 Сканирование компьютера

Модуль сканирования компьютера по требованию является важной частью решения, обеспечивающего защиту от вирусов. Он используется для сканирования файлов и папок на компьютере. С точки зрения обеспечения безопасности принципиально важно выполнять сканирование компьютера регулярно, а не только при возникновении подозрений о заражении. Рекомендуется регулярно выполнять полное сканирование компьютера для обнаружения вирусов, которые не были найдены защитой файловой системы в режиме реального времени при записи на диск. Это может произойти, если в тот момент защита файловой системы в режиме реального времени была отключена, база данных сигнатур вирусов была устаревшей или же файл не был распознан как вирус при сохранении на диск.

Доступно два типа **сканирования ПК**. **Сканировать компьютер**: быстрое сканирование системы, не требующее уточнения параметров сканирования. **Выборочное сканирование** позволяет выбрать один из предварительно определенных профилей сканирования для проверки специальных папок, а также позволяет указывать конкретные объекты сканирования.

 **Сканировать компьютер**

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

 **Выборочное сканирование**

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

 **Сканирование съемных носителей**

Подобно сканированию компьютера данная функция быстро запускает сканирование съемных носителей (таких, как компакт-диски, DVD-диски, накопители USB), которые подключены к компьютеру в данный момент. Это может быть удобно при подключении к компьютеру USB-устройства флэш-памяти, содержимое которого необходимо просканировать на наличие вредоносных программ и других потенциальных угроз.

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

 **Повторить последнее сканирование**

Быстрый запуск последнего выполненного сканирования с использованием тех же настроек.

См. главу Ход сканирования для получения дополнительных сведений о процессе сканирования.

ПРИМЕЧАНИЕ: Рекомендуется запускать сканирование компьютера не реже одного раза в месяц. Можно настроить сканирование как запланированную задачу в меню **Служебные программы** > **Планировщик**. Планирование еженедельного сканирования компьютера

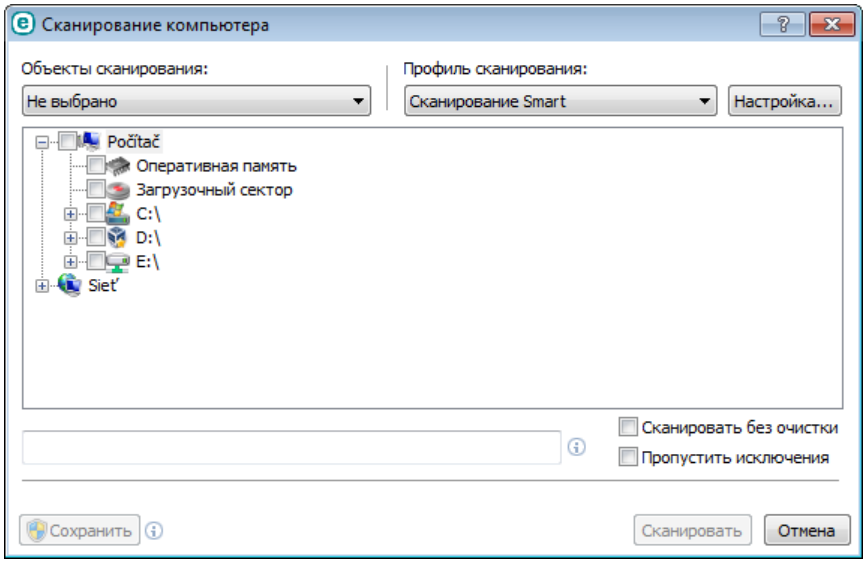
4.1.1.2.1 Средство запуска выборочного сканирования

Если необходимо сканировать не весь диск, а только определенный объект на этом диске, можно использовать выборочное сканирование. Для этого необходимо выбрать **Сканирование компьютера** > **Выборочное сканирование** и выбрать необходимый вариант в раскрывающемся меню **Объекты сканирования** или же указать нужные объекты в дереве папок.

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

- **Используя Настройки профиля**: выбираются объекты, указанные в выделенном профиле сканирования.
- **Сменные носители**: выбираются дискеты, USB-устройства хранения, компакт- и DVD-диски.
- **Локальные диски**: выбираются все жесткие диски, существующие в системе.
- **Сетевые диски**: выбираются все подключенные сетевые диски.
- **Не выбрано**: отменяется выбор объектов.

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



Зараженные элементы не очищаются автоматически. Сканирование без очистки можно использовать для получения общих сведений о текущем состоянии защиты. Если нужно только выполнить сканирование системы без дополнительных действий по очистке, выберите параметр **Сканировать без очистки**. Кроме того, можно выбрать один из трех уровней очистки, щелкнув **Настройки...** > **Очистка**. Информация о сканировании сохраняется в журнале сканирования.

Если выбран параметр **Пропустить исключения**, файлы с расширениями, которые ранее были исключены из сканирования, будут просканированы без каких-либо исключений.

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

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

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

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

4.1.1.2.2 Ход сканирования

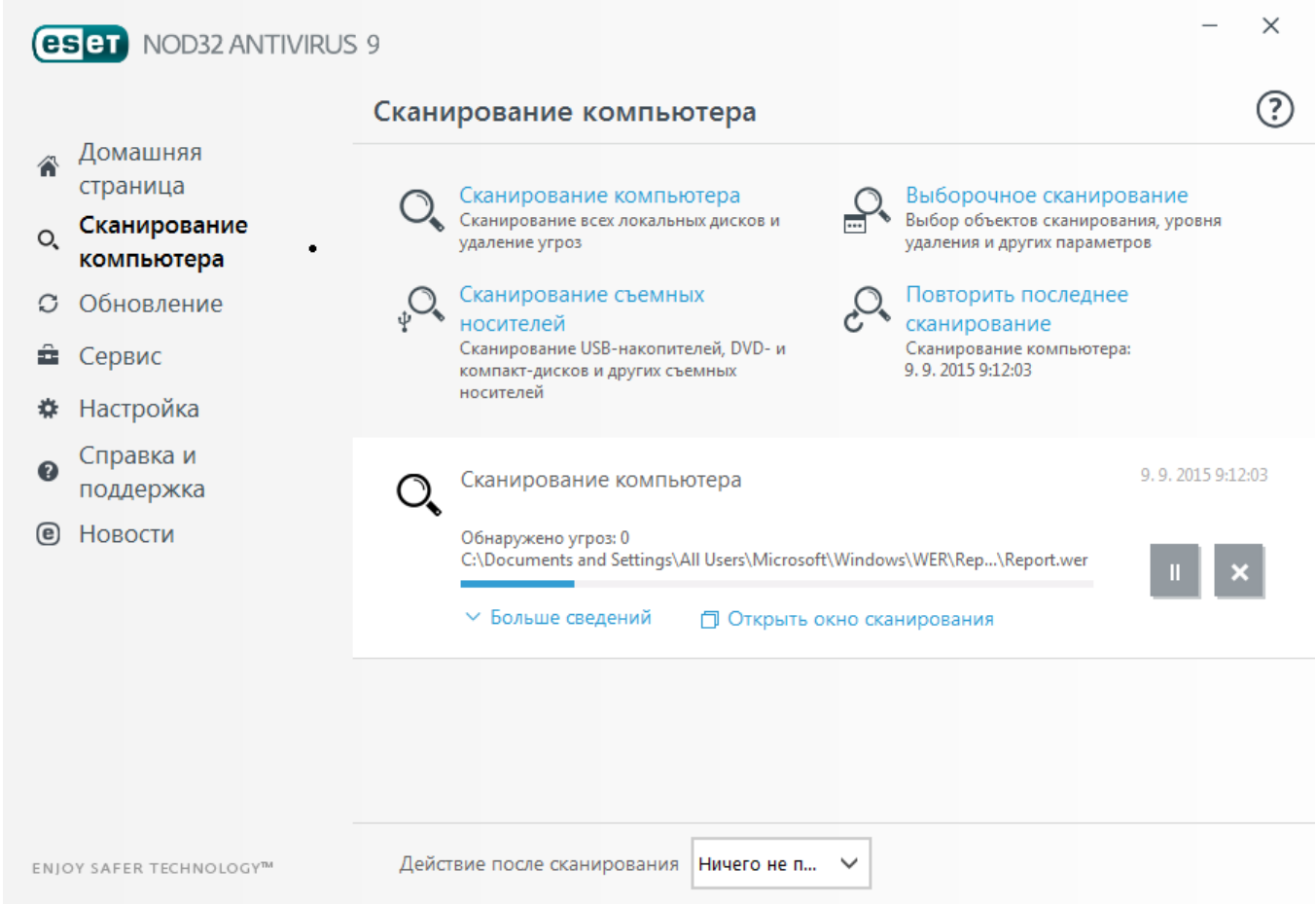
В окне хода сканирования отображается текущее состояние сканирования и информация о количестве файлов, в которых обнаружен злонамеренный код.

ПРИМЕЧАНИЕ. Нормальной ситуацией является невозможность сканирования некоторых файлов, например защищенных паролем файлов или файлов, используемых исключительно операционной системой (обычно *pagefile.sys* и некоторых файлов журналов).

Ход сканирования: индикатор выполнения показывает состояние уже просканированных объектов по сравнению с объектами, ожидающими сканирования. Состояние выполнения сканирования формируется на основе общего количества объектов, включенных в сканирование.
Объект: имя и расположение объекта, который сканируется в настоящий момент.
Найдены угрозы: отображается общее количество просканированных файлов и угроз, обнаруженных и удаленных во время сканирования.
Пауза: приостановка сканирования.
Продолжить: этот параметр отображается после приостановки выполнения сканирования. Нажмите **Возобновить**, чтобы продолжить сканирование.
Остановить: прекращение сканирования.
Прокрутить журнал сканирования: если этот параметр активирован, журнал сканирования будет прокручиваться автоматически при добавлении новых записей, чтобы отображались самые свежие из них.

ПОДСКАЗКА.

Щелкните экранную лупу или стрелку, чтобы просмотреть сведения о текущем сканировании.
Можно параллельно запустить другое сканирование, щелкнув **Сканировать компьютер** или **Выборочное сканирование**.



Действие после сканирования: выполнение запланированного завершения работы или перезагрузки по окончании сканирования компьютера. После завершения сканирования на экран будет выведено диалоговое окно подтверждения завершения работы. Оно будет активно в течение 60 секунд.

4.1.1.2.3 Профили сканирования

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

Для создания профиля откройте окно «Дополнительные настройки» (F5) и щелкните **Защита от вирусов** > **Сканирование компьютера по требованию** > **Основное** > **Список профилей**. В окне **Диспетчер профилей** есть раскрывающееся меню **Выбранный профиль**, в котором перечисляются существующие профили сканирования и есть возможность создать новый. Для создания профиля сканирования в соответствии с конкретными потребностями см. раздел Настройка параметров модуля ThreatSense, в котором описывается каждый параметр, используемый для настройки сканирования.

Пример. Предположим, пользователю требуется создать собственный профиль сканирования, причем конфигурация **Сканировать компьютер** частично устраивает его, но не нужно сканировать упаковщики или потенциально опасные приложения, но при этом нужно применить **тщательную очистку**. Введите имя нового профиля в окне **Диспетчер профилей** и нажмите кнопку **Добавить**. Выберите новый профиль в раскрывающемся меню **Выбранный профиль** и настройте остальные параметры в соответствии со своими требованиями, а затем нажмите кнопку **ОК**, чтобы сохранить новый профиль.

4.1.1.3 Сканирование файлов, исполняемых при запуске системы

При загрузке компьютера и обновлении базы данных сигнатур вирусов автоматически проверяются файлы, исполняемые при запуске системы. Это сканирование зависит от конфигурации и задач планировщика.

Сканирование файлов, исполняемых при запуске системы, входит в задачу планировщика **Проверка файлов, исполняемых при запуске системы**. Для изменения его настроек выберите команду **Служебные программы** > **Планировщик**, щелкните элемент **Автоматически проверять файлы при запуске системы**, а затем **Изменить**. На последнем этапе отобразится диалоговое окно Автоматическая проверка файлов при запуске системы (дополнительные сведения см. в следующем разделе).

Более подробные инструкции по созданию задач в планировщике и управлению ими см. в разделе Создание новой задачи.

4.1.1.3.1 Автоматическая проверка файлов при запуске системы

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

В раскрывающемся меню **Обычно используемые файлы** указывается глубина сканирования файлов, исполняемых при запуске системы. Сканирование выполняется на основе секретного сложного алгоритма. Файлы упорядочены по убыванию в соответствии со следующими критериями.

- **Все зарегистрированные типы файлов** (наибольшее количество сканируемых файлов)
- **Редко используемые файлы**
- **Обычно используемые файлы**
- **Часто используемые файлы**
- **Только наиболее часто используемые файлы** (наименьшее количество сканируемых файлов)

Также существуют две особые группы.

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

Списки подлежащих сканированию файлов являются фиксированными для каждой описанной выше группы.

Приоритет сканирования: уровень приоритетности, используемый для определения условий начала сканирования.

- **При бездействии**: задача будет выполняться только при бездействии системы.
- **Низкий**: минимальная нагрузка на систему.
- **Ниже среднего**: низкая нагрузка на систему.
- **Средний**: средняя нагрузка на систему.

4.1.1.4 Сканирование в состоянии простоя

Можно разрешить сканирование в состоянии простоя, выбрав пункт **Дополнительные настройки** в меню **Антивирус** > **Сканирование в состоянии простоя** > **Основное**. Установите переключатель **Разрешить сканирование в состоянии простоя** в положение **Вкл.**, чтобы разрешить использование этой функции. Когда компьютер находится в состоянии простоя, автоматически выполняется сканирование всех локальных дисков. Полный список условий для запуска сканирования в состоянии простоя см. в Условиях запуска обнаружения в состоянии простоя..

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

Установите переключатель **Включить ведение журналов** в области, отображаемой по команде **Дополнительные настройки** > **Служебные программы** > **ESET LiveGrid®**, чтобы результаты сканирования компьютера регистрировались в разделе Файлы журналов (в главном окне программы перейдите в область **Служебные программы** > **Файлы журналов** и выберите элемент **Сканирование компьютера** в раскрывающемся списке **Журнал**).

Обнаружение в состоянии простоя будет запущено в случае пребывания компьютера в одном из следующих режимов.

- Заставка
- Блокировка компьютера
- Выход пользователя

Сведения о том, как изменить параметры сканирования (например, методов обнаружения) для сканирования в состоянии простоя, см. в разделе Настройка параметров модуля ThreatSense.

4.1.1.5 Исключения

Исключения позволяют исключить файлы и папки из сканирования. Чтобы обеспечить сканирование всех объектов на наличие угроз, рекомендуется создавать исключения только в случае крайней необходимости. Однако в некоторых случаях все же необходимо исключать объекты, например большие базы данных, которые замедляют работу компьютера при сканировании, или программы, конфликтующие с процессом сканирования.

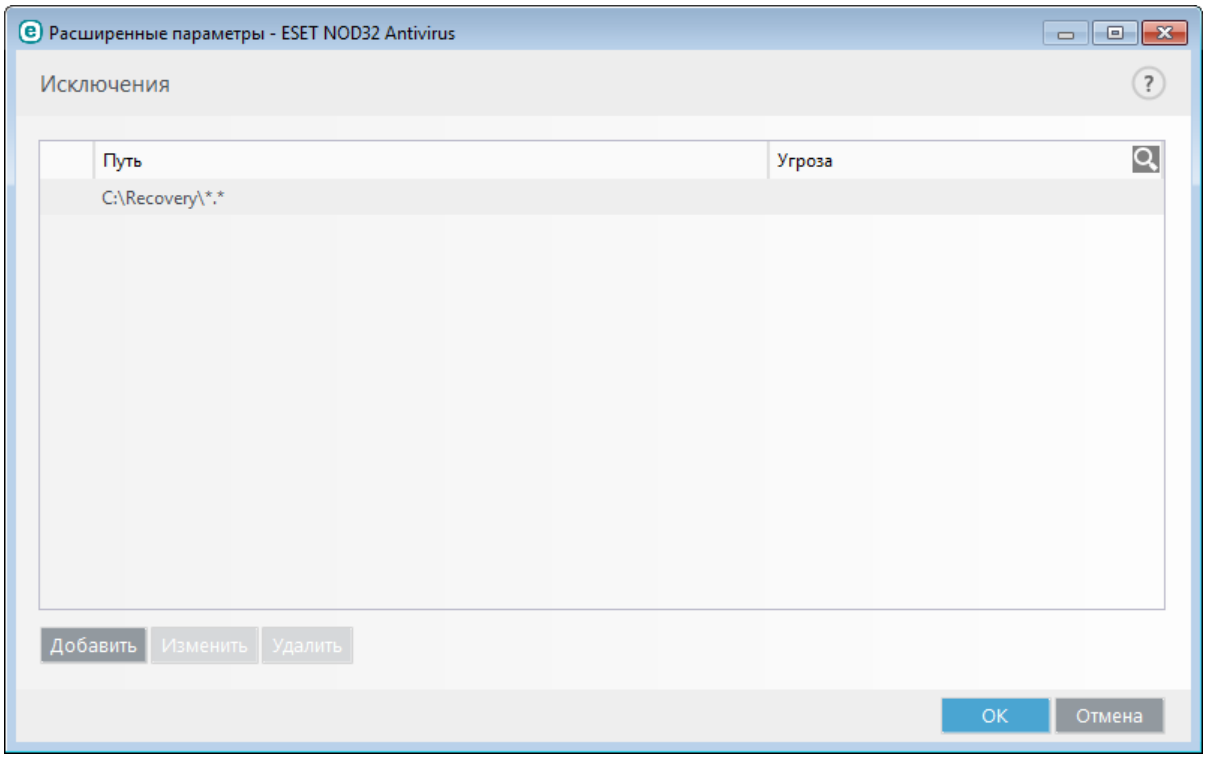
Для исключения объекта из сканирования выполните следующие действия.

1. Нажмите кнопку **Добавить**.
2. Введите путь к объекту или выделите его в древовидной структуре.

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

Примеры

- Если нужно исключить все файлы в папке, следует ввести путь к папке и использовать маску «*.*».
- Для того чтобы исключить весь диск, в том числе все файлы и подпапки на нем, используйте маску «D:*».
- Если нужно исключить только файлы с расширением .doc, используйте маску «*.doc».
- Если имя исполняемого файла содержит определенное количество символов (и символы могут меняться), причем известна только первая буква имени (скажем, «D»), следует использовать следующий формат: «D????.exe». Вопросительные знаки замещают отсутствующие (неизвестные) символы.



ПРИМЕЧАНИЕ. Угроза в файле не будет обнаружена модулем защиты файловой системы в режиме реального времени или модулем сканирования компьютера, если файл соответствует критериям для исключения из сканирования.

Столбцы

Путь — путь к исключаемым файлам и папкам.

Угроза: если рядом с исключаемым файлом указано имя угрозы, файл не сканируется только на наличие этой угрозы, а не вообще. Если этот файл позже окажется заражен другой вредоносной программой, модуль защиты от вирусов ее обнаружит. Исключения такого типа могут использоваться только с определенными типами заражений м могут создаваться в окне предупреждения об угрозе, в котором сообщается о заражении (последовательно щелкните элементы **Показать расширенные параметры** > **Исключить из обнаружения**). В качестве альтернативы для создания исключения выберите элементы **Служебные программы** > **Карантин**, после чего щелкните правой кнопкой мыши находящийся в карантине файл и выберите в контекстном меню команду **Восстановить и исключить из обнаружения**.

Элементы управления

Добавить: исключение объектов из области сканирования.

Изменить: изменение выделенных записей.

Удалить: удаление выделенных записей.

4.1.1.6 Параметры ThreatSense

ThreatSense — это технология, в которой реализован ряд сложных методов обнаружения угроз. Эта технология является упреждающей, т. е. защищает от новой угрозы уже в самом начале ее распространения. А сочетание анализа и моделирования кода, применения обобщенных сигнатур и сигнатур вирусов позволяет значительно повысить уровень безопасности компьютера. Модуль сканирования способен контролировать несколько потоков данных одновременно, благодаря чему максимизируются эффективность и количество обнаруживаемых угроз. ThreatSense обеспечивает к тому же успешное уничтожение руткитов.

ThreatSense для модуля можно настроить несколько параметров сканирования:

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

Чтобы открыть окно параметров, щелкните **Параметры ThreatSense** в окне «Дополнительные настройки» любого модуля, использующего технологию ThreatSense (см. ниже). Разные сценарии обеспечения безопасности могут требовать различных настроек. Поэтому технологию ThreatSense можно настроить отдельно для каждого из перечисленных далее модулей защиты.

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

ThreatSense параметры хорошо оптимизированы для каждого из модулей, а их изменение значительно влияет на поведение системы. Например, изменение параметров сканирования упаковщиков в режиме реального времени или включение расширенной эвристики в модуле защиты файловой системы в режиме реального времени может замедлить работу системы (обычно только новые файлы сканируются с применением этих методов). Рекомендуется не изменять параметры ThreatSense по умолчанию ни для каких модулей, кроме модуля «Сканирование компьютера».

Сканируемые объекты

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

Оперативная память: выполняется сканирование на наличие угроз, направленных на оперативную память системы.

Загрузочные секторы: загрузочные секторы сканируются на наличие вирусов в основной загрузочной записи.

Почтовые файлы: программа поддерживает расширения DBX (Outlook Express) и EML.

Архивы: программа поддерживает расширения ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE и многие другие.

Самораспаковывающиеся архивы: самораспаковывающиеся архивы (файлы с расширением SFX) — это архивы, для распаковки которых не нужны специальные программы.

Упаковщики: в отличие от архивов стандартных типов, запущенные упаковщики исполняемых файлов распаковываются прямо в оперативную память. Благодаря эмуляции кода модуль сканирования распознает не только стандартные статические упаковщики (UPX, yoda, ASPack, FGS и т. д.), но и множество других типов упаковщиков.

Параметры сканирования

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

Эвристический анализ: анализ злонамеренной деятельности программ с помощью специального алгоритма. Главным достоинством этого метода является способность идентифицировать вредоносные программы, сведения о которых отсутствуют в существующей базе данных сигнатур вирусов. Недостатком же является вероятность (очень небольшая) ложных тревог.

Расширенная эвристика/DNA/Сигнатуры Smart: метод расширенной эвристики базируется на уникальном эвристическом алгоритме, разработанном компанией ESET, оптимизированном для обнаружения компьютерных червей и троянских программ и реализованном на языках программирования высокого уровня. Использование расширенной эвристики значительным образом увеличивает возможности продуктов ESET по обнаружению угроз. С помощью сигнатур осуществляется точное обнаружение и идентификация вирусов. Система автоматического обновления обеспечивает доступность новых сигнатур через несколько часов после обнаружения угрозы. Недостатком же сигнатур является то, что они позволяют обнаруживать только известные вирусы (или их незначительно модифицированные версии).

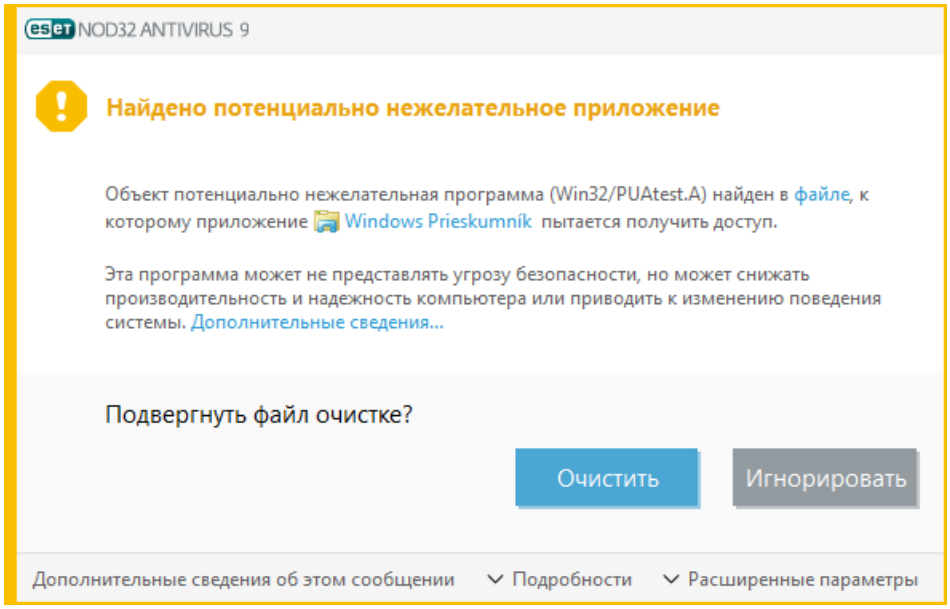
Потенциально нежелательное приложение — это программа, которая содержит рекламу, устанавливает

панели инструментов или выполняет другие неясные функции. В некоторых ситуациях может показаться, что преимущества такого потенциально нежелательного приложения перевешивают риски. Поэтому компания ESET помещает эти приложения в категорию незначительного риска, в отличие от других вредоносных программ, например троянских программ или червей.

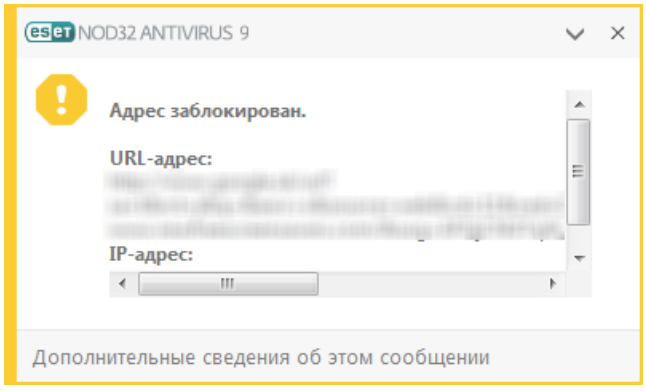
Предупреждение — обнаружена потенциальная угроза

Когда обнаруживается потенциально нежелательное приложение, вы можете самостоятельно решить, какое действие нужно выполнить.

1. **Очистить/отключить**: действие прекращается, и потенциальная угроза не попадает в систему.
2. **Пропустить**: эта функция позволяет потенциальной угрозе проникнуть на компьютер.
3. Чтобы разрешить приложению и впредь работать на компьютере без прерываний, щелкните элемент **Расширенные параметры** и установите флажок **Исключить из обнаружения**.

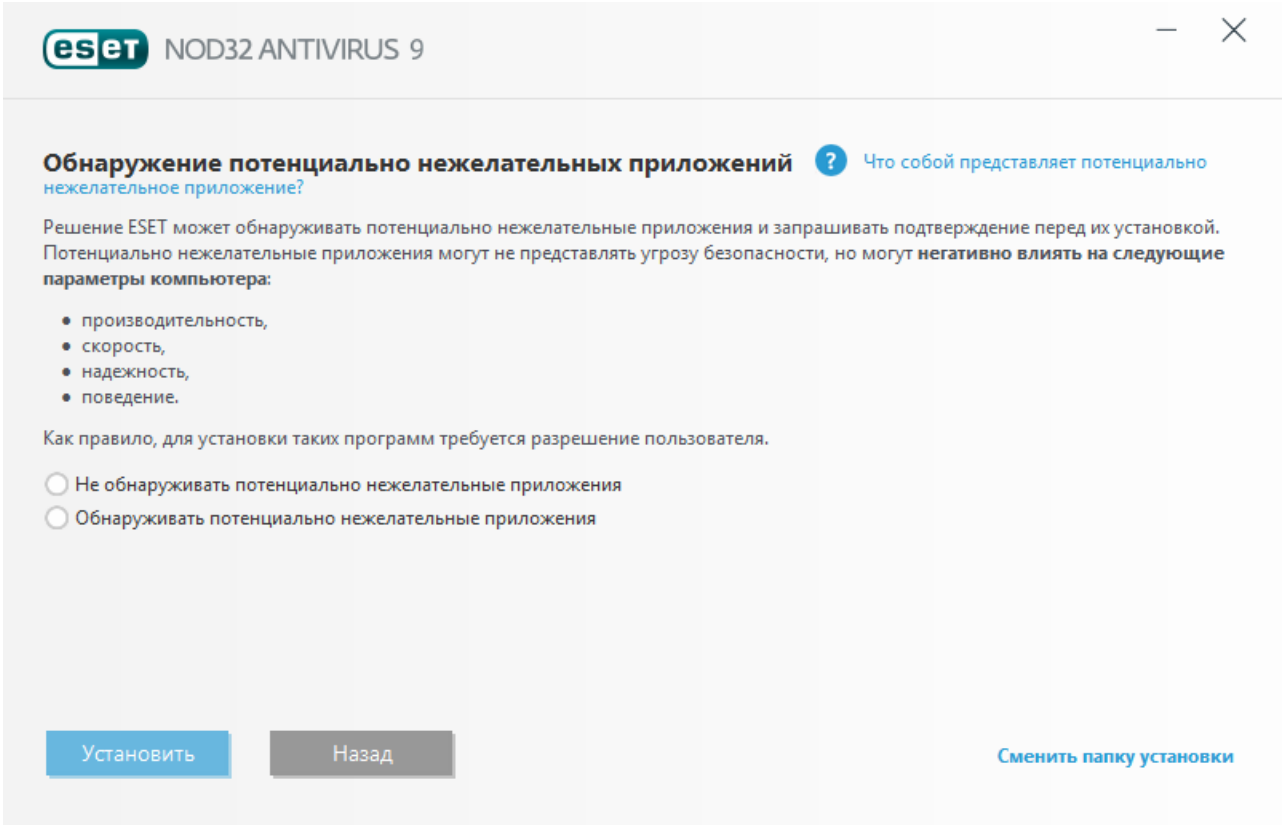


Если обнаружено потенциально нежелательное приложение и его невозможно очистить, в правом нижнем углу экрана отобразится окно уведомлений **Адрес заблокирован**. Для получения дополнительных сведений об этом событии перейдите из главного меню в раздел **Служебные программы** > **Файлы журналов** > **Отфильтрованные веб-сайты**.



Потенциально нежелательные приложения — параметры

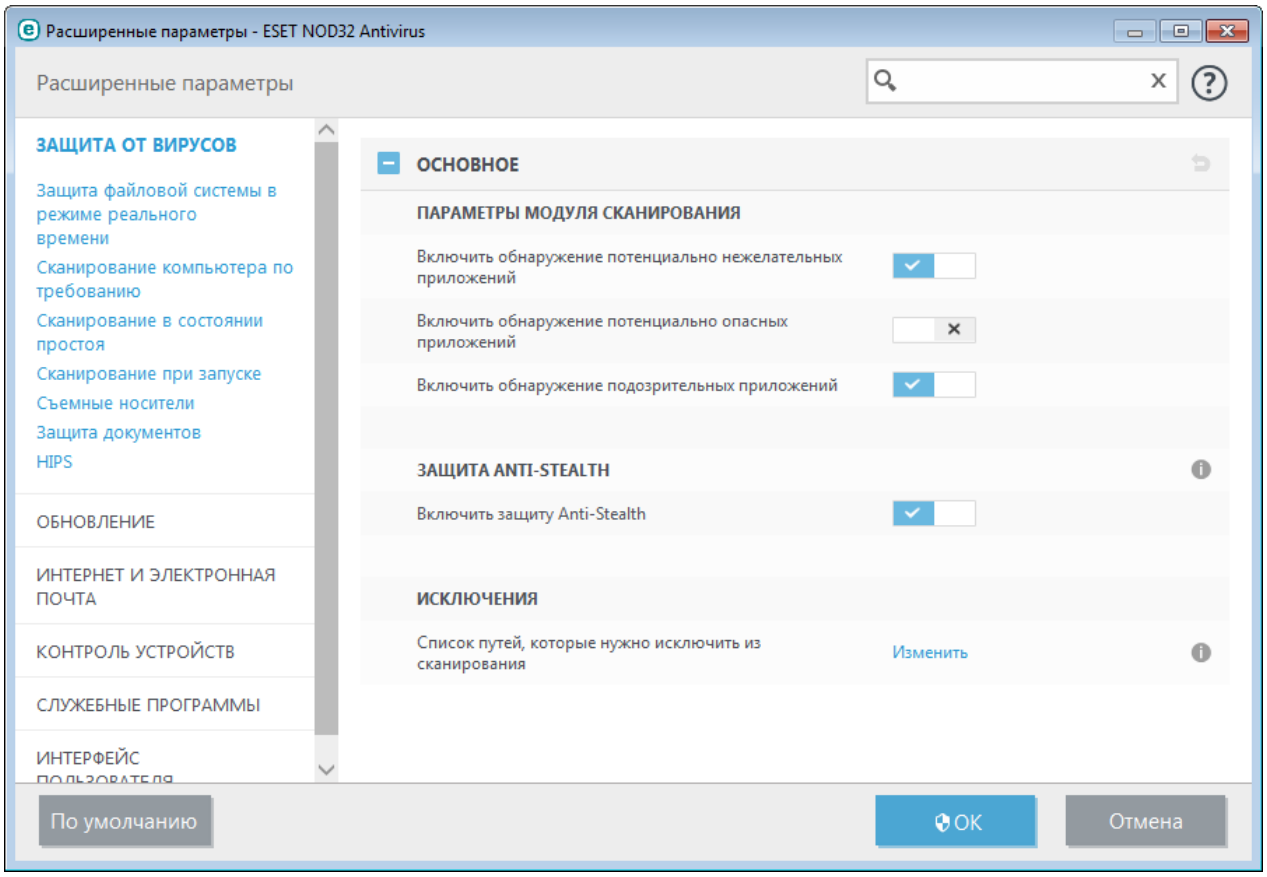
При установке программы ESET можно включить обнаружение потенциально нежелательных приложений (см. изображение ниже).



Потенциально нежелательные приложения могут устанавливать рекламные программы и панели инструментов или содержать рекламу и другие нежелательные и небезопасные программные компоненты.

Эти параметры можно в любое время изменить в разделе параметров программы. Чтобы включить или отключить обнаружение потенциально нежелательных, небезопасных или подозрительных приложений, следуйте приведенным ниже инструкциям.

1. Откройте программу ESET. Как открыть программу ESET на моем компьютере?
2. Нажмите клавишу **F5**, чтобы перейти к разделу **Дополнительные настройки**.
3. Щелкните элемент **Антивирус** и на свое усмотрение включите или отключите параметры **Включить обнаружение потенциально нежелательных приложений**, **Включить обнаружение потенциально опасных приложений** и **Включить обнаружение подозрительных приложений**. Чтобы сохранить настройки, нажмите кнопку **ОК**.



Потенциально нежелательные приложения — оболочки

Оболочка — специальное приложение, используемое на некоторых файлообменных ресурсах. Это стороннее средство, устанавливающее программу, которую нужно загрузить, в комплекте с другим программным обеспечением, например панелью инструментов или рекламной программой, которые могут изменить домашнюю страницу браузера или параметры поиска. При этом файлообменные ресурсы часто не уведомляют поставщиков программного обеспечения или получателей загруженных файлов о внесенных изменениях, а отказаться от этих изменений непросто. Именно поэтому компания ESET считает оболочки потенциально нежелательными приложениями и дает пользователям возможность отказаться от их загрузки.

Обновленную версию данной страницы справки см. в этой статье базы знаний ESET.

Потенциально опасные приложения. Потенциально опасные приложения — это обозначение для не являющихся вредоносными коммерческих программ, таких как средства удаленного доступа, приложения для взлома паролей и клавиатурные шпионы (программы, записывающие каждое нажатие клавиши на клавиатуре). По умолчанию этот параметр отключен.

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

Исключения

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

Другое

При настройке параметров модуля ThreatSense для сканирования компьютера по требованию также доступны описанные ниже параметры из раздела **Другое**.

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

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

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

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

Сохранить отметку о времени последнего доступа: установите этот флажок, чтобы сохранять исходную отметку о времени доступа к сканируемым файлам, не обновляя ее (например, для использования с системами резервного копирования данных).

Ограничения

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

Параметры объектов

Максимальный размер объекта: определяет максимальный размер объектов, подлежащих сканированию. Данный модуль защиты от вирусов будет сканировать только объекты меньше указанного размера. Этот параметр рекомендуется менять только опытным пользователям, у которых есть веские основания для исключения из сканирования больших объектов. Значение по умолчанию: *не ограничено*.

Максимальное время сканирования объекта (с): определяет максимальное время, в течение которого будет сканироваться объект. Если пользователь укажет здесь собственное значение, модуль защиты от вирусов прекратит сканирование объекта по истечении указанного времени вне зависимости от того, завершено ли сканирование. Значение по умолчанию: *не ограничено*.

Настройки сканирования архивов

Уровень вложенности архивов: определяет максимальную глубину сканирования архивов. Значение по умолчанию: *10*.

Максимальный размер файла в архиве: этот параметр позволяет задать максимальный размер подлежащих сканированию файлов в архиве (имеется в виду размер, который будут иметь извлеченные файлы). Значение по умолчанию: *не ограничено*.

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

4.1.1.6.1 Очистка

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

4.1.1.6.2 Исключенные из сканирования расширения файлов

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

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

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

С помощью кнопок **Добавить** и **Удалить** можно изменять содержимое списка, разрешая или запрещая сканирование файлов с определенными расширениями. Для добавления в список нового расширения нажмите кнопку **Добавить**, введите расширение в пустом поле и нажмите кнопку **ОК**. Выбрав вариант **Введите несколько значений**, можно добавить несколько расширений имен файлов, разделив их символами перевода строки, запятой или точки с запятой. Если разрешен ввод нескольких значений, расширения будут отображаться в виде списка. Чтобы удалить расширение из списка, выберите это расширение и нажмите кнопку **Удалить**. Для изменения выбранного расширения нажмите кнопку **Изменить**.

Можно использовать символы шаблона «*» (звездочка) и «?» (вопросительный знак). Символ звездочки обозначает любую последовательность символов, а вопросительный знак — любой символ.

4.1.1.7 Действия при обнаружении заражения

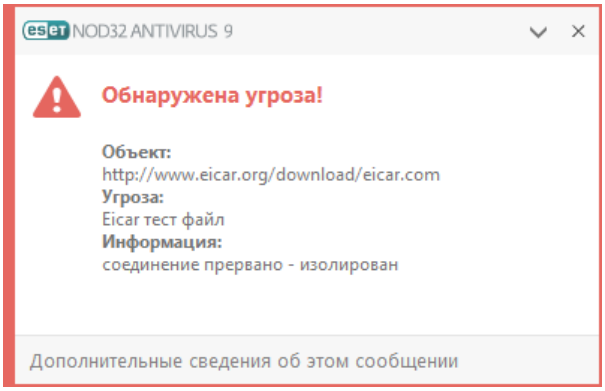
Заражения могут попасть на компьютер из различных источников, таких как веб-сайты, общие папки, электронная почта или съемные носители (накопители USB, внешние диски, компакт- или DVD-диски, дискеты и т. д.).

Стандартное поведение

Обычно ESET NOD32 Antivirus обнаруживает заражения с помощью перечисленных ниже модулей.

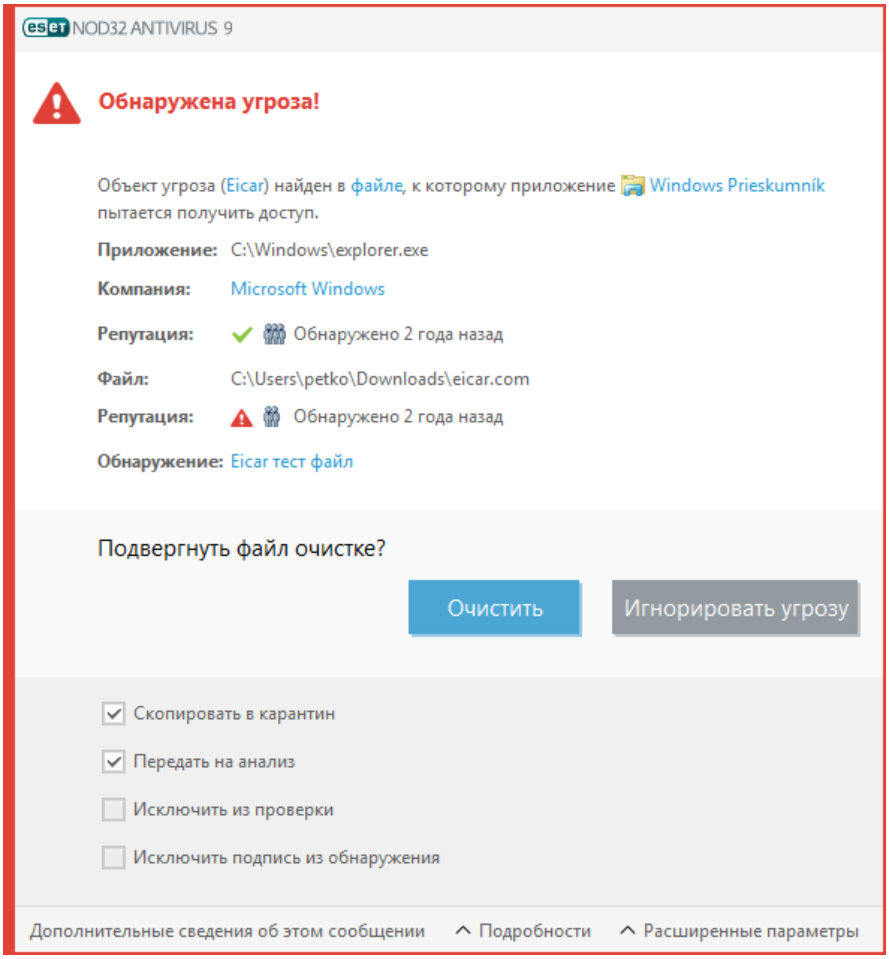
- Защита файловой системы в режиме реального времени
- Защита доступа в Интернет
- Защита почтового клиента
- Сканирование компьютера по требованию

Каждый модуль использует стандартный уровень очистки и пытается очистить файл, поместить его в карантин или прервать подключение. В правом нижнем углу экрана отображается окно уведомлений. Дополнительные сведения об уровнях очистки и поведении см. в разделе Очистка.



Очистка и удаление

Если действие по умолчанию для модуля защиты файловой системы в режиме реального времени не определено, пользователю предлагается выбрать его в окне предупреждения. Обычно доступны варианты **Очистить**, **Удалить** или **Ничего не предпринимать**. Не рекомендуется выбирать действие **Ничего не предпринимать**, поскольку при этом зараженные файлы не будут очищены. Исключение допустимо только в том случае, если вы уверены, что файл безвреден и был обнаружен по ошибке.



Очистку следует применять, если файл был атакован вирусом, который добавил к нему вредоносный код. В этом случае сначала программа пытается очистить зараженный файл, чтобы восстановить его первоначальное состояние. Если файл содержит только вредоносный код, он будет удален.

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

Множественные угрозы

Если при сканировании компьютера какие-либо зараженные файлы не были очищены (или для параметраУровень очистки было установлено значение **Без очистки**), на экране отобразится окно предупреждения, в котором вам будет предложено выбрать действие для таких файлов. Следует выбрать действия для файлов (действия выбираются отдельно для каждого файла в списке), а затем нажать кнопку **Готово**.

Удаление файлов из архивов

В режиме очистки по умолчанию архив удаляется целиком только в том случае, если он содержит только зараженные файлы. Иначе говоря, архивы, в которых есть незараженные файлы, не удаляются. Однако следует проявлять осторожность при сканировании в режиме тщательной очистки, так как при этом архив удаляется, если содержит хотя бы один зараженный файл, независимо от состояния других файлов в архиве.

Если на компьютере возникли признаки заражения вредоносной программой (например, он стал медленнее работать, часто зависает и т. п.), рекомендуется выполнить следующие действия.

- Откройте ESET NOD32 Antivirus и выберите команду «Сканирование компьютера».
- Выберите вариант **Сканировать компьютер** (дополнительную информацию см. в разделе Сканирование компьютера).
- После окончания сканирования проверьте в журнале количество просканированных, зараженных и очищенных файлов.

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

4.1.1.8 Защита документов

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

Параметр **Интеграция с системой** активирует систему защиты. Для изменения этого параметра нажмите F5, чтобы открыть окно **Дополнительные настройки**, и перейдите к разделу **Защита от вирусов** > **Защита документов дерева расширенных параметров**.

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

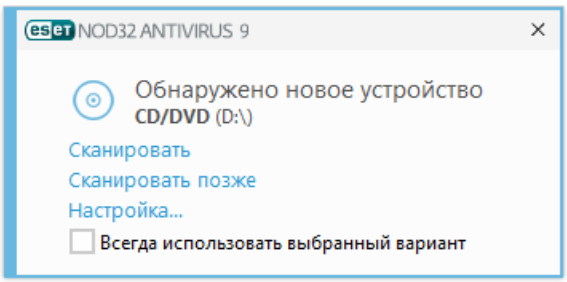
4.1.2 Съемные носители

ESET NOD32 Antivirus обеспечивает автоматическое сканирование съемных носителей (компакт- и DVD-дисков, USB-устройств и т. п.). Данный модуль позволяет сканировать вставленный носитель. Это может быть удобно, если администратор компьютера хочет предотвратить подключение пользователями съемных носителей с нежелательным содержимым.

Действие, которое следует предпринять после подключения съемного носителя: выбор действия по умолчанию, которое будет выполняться при подключении к компьютеру съемного носителя (компакт-диска, DVD-диска, USB-устройства). Если выбран вариант **Показать параметры сканирования**, на экран будет выведено уведомление, с помощью которого можно выбрать нужное действие.

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

Когда вставляется съемный носитель, отображается следующее диалоговое окно:



Сканировать сейчас: начнется сканирование съемного носителя.

Сканировать позже: сканирование съемного носителя будет отложено.

Настройки: отобразятся «Дополнительные настройки».

Всегда использовать выбранный вариант: если установить этот флажок, выбранное действие будет выполняться каждый раз, когда вставляется съемный носитель.

Кроме того, в ESET NOD32 Antivirus есть модуль контроля устройств, позволяющий задавать правила использования внешних устройств на указанном компьютере. Дополнительные сведения об этом модуле см. в разделе Контроль устройств.

4.1.3 Контроль устройств

ESET NOD32 Antivirus обеспечивает автоматическое управление устройствами (компакт- и DVD-дисками, USB-устройствами и т. п.). Данный модуль позволяет сканировать, блокировать и изменять расширенные фильтры и разрешения, а также указывать, может ли пользователь получать доступ к конкретному устройству и работать с ним. Это может быть удобно, если администратор компьютера хочет предотвратить использование устройств с нежелательным содержимым.

Поддерживаемые внешние устройства:

- Дисковый накопитель (жесткий диск, съемный USB-диск)
- Компакт-/DVD-диск
- USB-принтер
- FireWire-хранилище
- Устройство Bluetooth
- Устройство чтения смарт-карт
- Устройство обработки изображений
- Модемы
- LPT/COM-порты
- Переносное устройство
- Все типы устройств

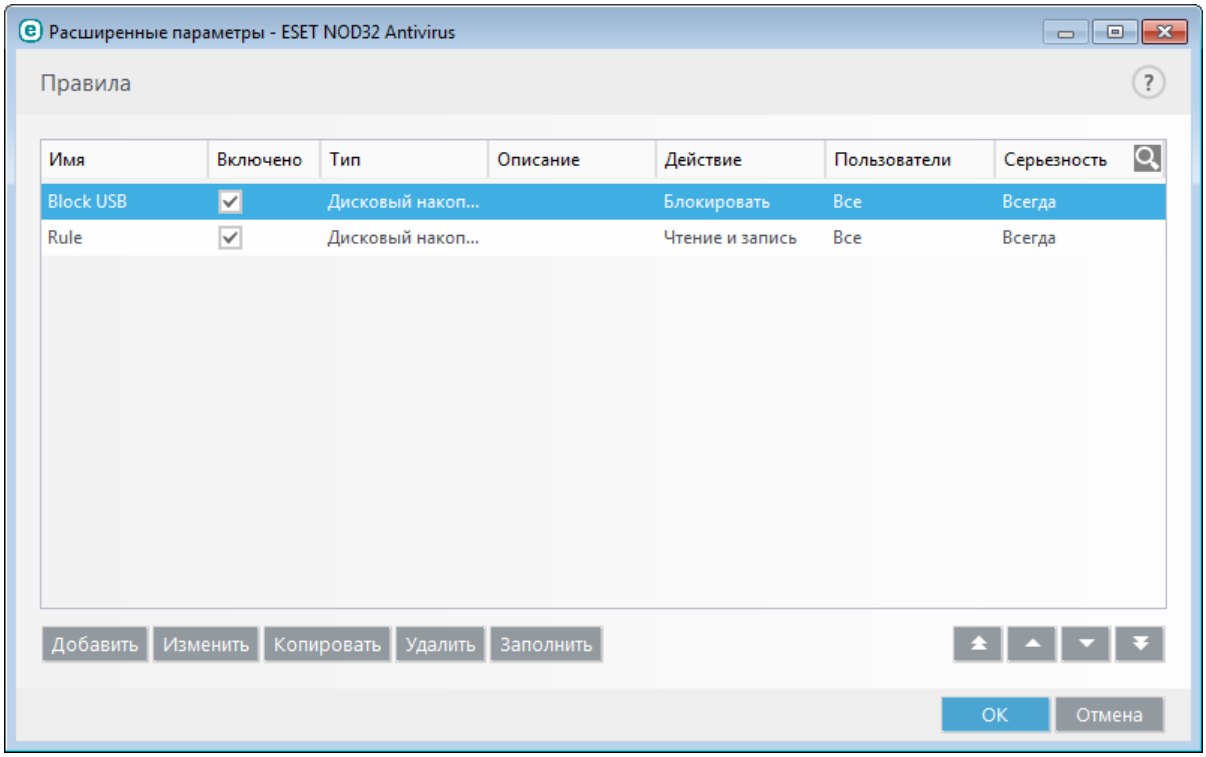
Параметры контроля устройств можно изменить в разделе **Дополнительные настройки** (F5) > **Контроль устройств**.

Если активировать переключатель **\Интеграция с системой**, в программе ESET NOD32 Antivirus будет включена функция контроля устройств. Чтобы это изменение вступило в силу, необходимо перезагрузить компьютер. После включения контроля устройств кнопка **Редактор правил** станет активной и вы сможете открыть окно Редактор правил.

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

4.1.3.1 Редактор правил для контроля устройств

В окне **Редактор правил для контроля устройств** отображаются существующие правила. С его помощью можно контролировать внешние устройства, которые пользователи подключают к компьютеру.



Вы можете разрешить или заблокировать определенные устройства для конкретных пользователей или их групп, а также в соответствии с дополнительными параметрами, которые задаются в конфигурации правил. В списке правил для каждого правила отображается описание, включающее название и тип внешнего устройства, действие, выполняемое после его подключения к компьютеру, а также серьезность для журнала.

Для управления правилом используйте кнопки **Добавить** или **Изменить**. Чтобы создать правило с использованием заранее заданных параметров из другого правила, нажмите кнопку **Копировать**. XML-строки, которые отображаются, если щелкнуть правило, можно скопировать в буфер обмена. Кроме того, они могут помочь системным администраторам экспортировать или импортировать эти данные, а также использовать их, например, в ESET Remote Administrator.

Чтобы выделить несколько правил, щелкните их, удерживая нажатой клавишу CTRL. Затем их можно будет одновременно удалить либо переместить к началу или концу списка. Флажок **Включено** позволяет включить или отключить правило. Это может быть полезно, если вы не хотите полностью удалять правило, чтобы воспользоваться им позднее.

Управление основано на правилах, которые отсортированы по приоритету: правила с более высоким приоритетом находятся в начале.

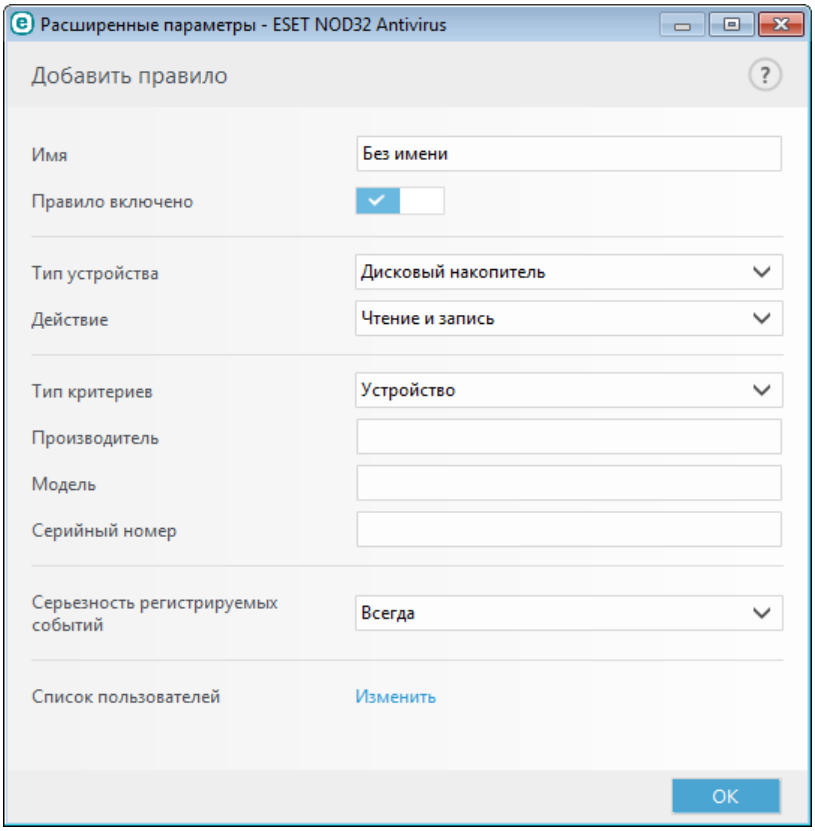
Записи журнала можно просмотреть в главном окне ESET NOD32 Antivirus в разделе **Служебные программы** > **Файлы журнала**.

В журнал контроля устройств записываются все случаи, когда срабатывает функция контроля устройств.

Щелкните **Заполнить**, чтобы выполнить автоматическое заполнение параметров для съемных носителей, подключенных к компьютеру.

4.1.3.2 Добавление правил контроля устройств

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



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

Тип устройства

В раскрывающемся списке выберите тип внешнего устройства (дисковый накопитель, портативное устройство, Bluetooth, FireWire и т. д.). Сведения о типе устройства поступают от операционной системы. Их можно просмотреть с помощью диспетчера устройств, если устройство подключено к компьютеру. К накопителям относятся внешние диски и традиционные устройства чтения карт памяти, подключенные по протоколу USB или FireWire. Устройства чтения смарт-карт позволяют читать карты со встроенными микросхемами, такие как SIM-карты или идентификационные карточки. Примерами устройств обработки изображений служат сканеры и камеры. Так как эти устройства предоставляют сведения только о своих действиях, а не о пользователях, заблокировать их можно только глобально.

Действие

Доступ к устройствам, не предназначенным для хранения данных, можно только разрешить или заблокировать. Напротив, правила для устройств хранения данных позволяют выбрать одно из указанных ниже прав.

- **Чтение и запись**: будет разрешен полный доступ к устройству.
- **Блокировать**: доступ к устройству будет заблокирован.
- **Только чтение**: будет разрешено только чтение данных с устройства.
- **Предупредить**: при каждом подключении устройства пользователь получает уведомление о том, разрешено это устройство или заблокировано, и при этом создается запись в журнале. Устройства не запоминаются. Уведомления отображаются при каждом повторном подключении одного и того же устройства.

Обратите внимание, что полный список действий (разрешений) доступен не для всех типов устройств. Если

устройство относится к типу хранилищ, будут доступны все четыре действия. Если устройство не предназначено для хранения данных, будут доступны только три действия. Например, разрешение **Только чтение** неприменимо к Bluetooth-устройствам, поэтому доступ к ним можно только разрешить, заблокировать или разрешить с предупреждением.

Тип критериев Выберите элемент **Группа устройств** или **Устройство**.

С помощью указанных ниже дополнительных параметров можно точно настраивать и изменять правила для конкретных устройств. Все параметры не зависят от регистра.

- **Производитель**: фильтрация по имени или идентификатору производителя.
- **Модель**: наименование устройства.
- **Серийный номер**: у внешних устройств обычно есть серийные номера. Когда речь идет о компакт- или DVD-диске, то это серийный номер конкретного носителя, а не дисковода компакт-дисков.

ПРИМЕЧАНИЕ. Если для этих параметров не заданы значения, во время сопоставления правило игнорирует эти поля. Для параметров фильтрации во всех текстовых полях не учитывается регистр и не поддерживаются подстановочные знаки (*, ?).

ПОДСКАЗКА. Для просмотра сведений об этом устройстве создайте правило для соответствующего типа устройств, подключите устройство к компьютеру и ознакомьтесь со сведениями об устройстве в журнале контроля устройств.

Серьезность регистрируемых событий

Персональный файервол ESET NOD32 Antivirus сохраняет данные обо всех важных событиях в файле журнала, который можно открыть из главного меню. Щелкните **Служебные программы** > **Файлы журналов** и выберите в раскрывающемся списке **Журнал** элемент **Контроль устройств**.

- **Всегда** : записываются все события.
- **Диагностика**: регистрируется информация, необходимая для тщательной настройки программы.
- **Информационные**: записываются информационные сообщения, в том числе сообщения об успешном выполнении обновления, а также все перечисленные выше записи.
- **Предупреждение**: записывается информация обо всех критических ошибках и предупреждениях.
- **Ничего**: журналы не создаются.

Правила можно назначать только для некоторых пользователей или их групп, добавленных в **список пользователей**.

- **Добавить**: открывается диалоговое окно **Типы объектов: пользователи и группы**, в котором можно выбрать нужных пользователей.
- **Удалить**: выбранный пользователь удаляется из фильтра.

ПРИМЕЧАНИЕ. Все устройства можно фильтровать по пользовательским правилам (например, устройства обработки изображений предоставляют информацию только о действиях, но не о пользователях).

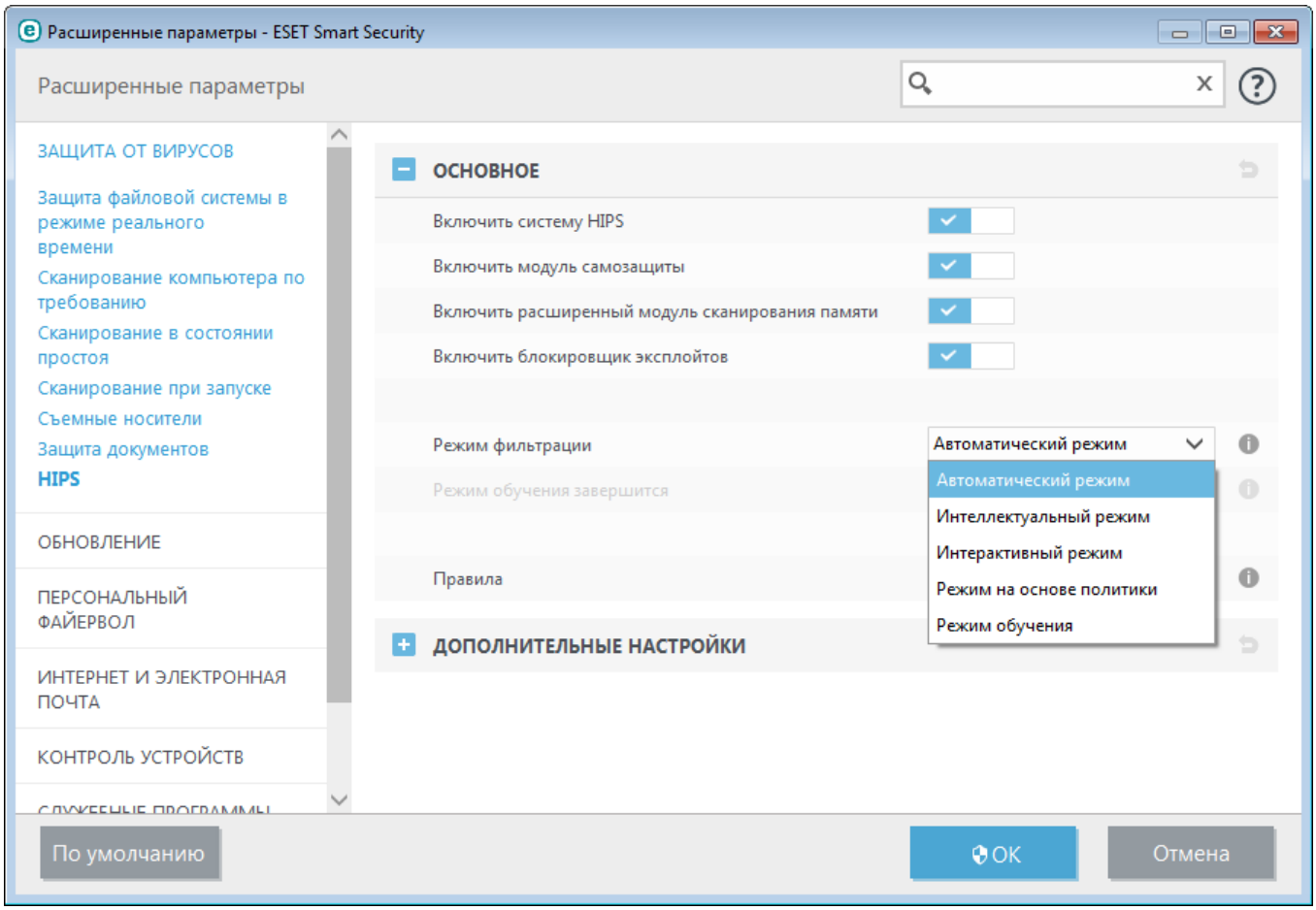
4.1.4 Система предотвращения вторжений на узел (HIPS)


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

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

Параметры HIPS доступны в разделе **Дополнительные настройки** (F5) > **Антивирус** > **Система предотвращения вторжений на узел** > **Основные сведения**. Состояние HIPS (включено/отключено) отображается в главном окне

программы ESET NOD32 Antivirus, в разделе **Установка** > **Защита компьютера**.



ESET NOD32 Antivirus использует встроенную технологии **самозащиты**, которая не позволяет вредоносным программам повреждать или отключать защиту от вирусов и шпионских программ. Благодаря этому пользователь всегда уверен в защищенности компьютера. Чтобы отключить систему HIPS или функцию самозащиты, требуется перезагрузить Windows.

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

Блокировщик эксплойтов предназначен для защиты приложений, которые обычно уязвимы для эксплойтов, например браузеров, программ для чтения PDF-файлов, почтовых клиентов и компонентов MS Office. Блокировщик эксплойтов по умолчанию включен. Дополнительную информацию об этом типе защиты см. в глоссарии.

Доступны четыре режима фильтрации.

Автоматический режим: включены все операции за исключением тех, что заблокированы посредством предварительно заданных правил, предназначенных для защиты компьютера.

Интеллектуальный режим: пользователь будет получать уведомления только об очень подозрительных событиях.

Интерактивный режим: пользователю будет предлагаться подтверждать операции.

Режим на основе политики: операции блокируются.

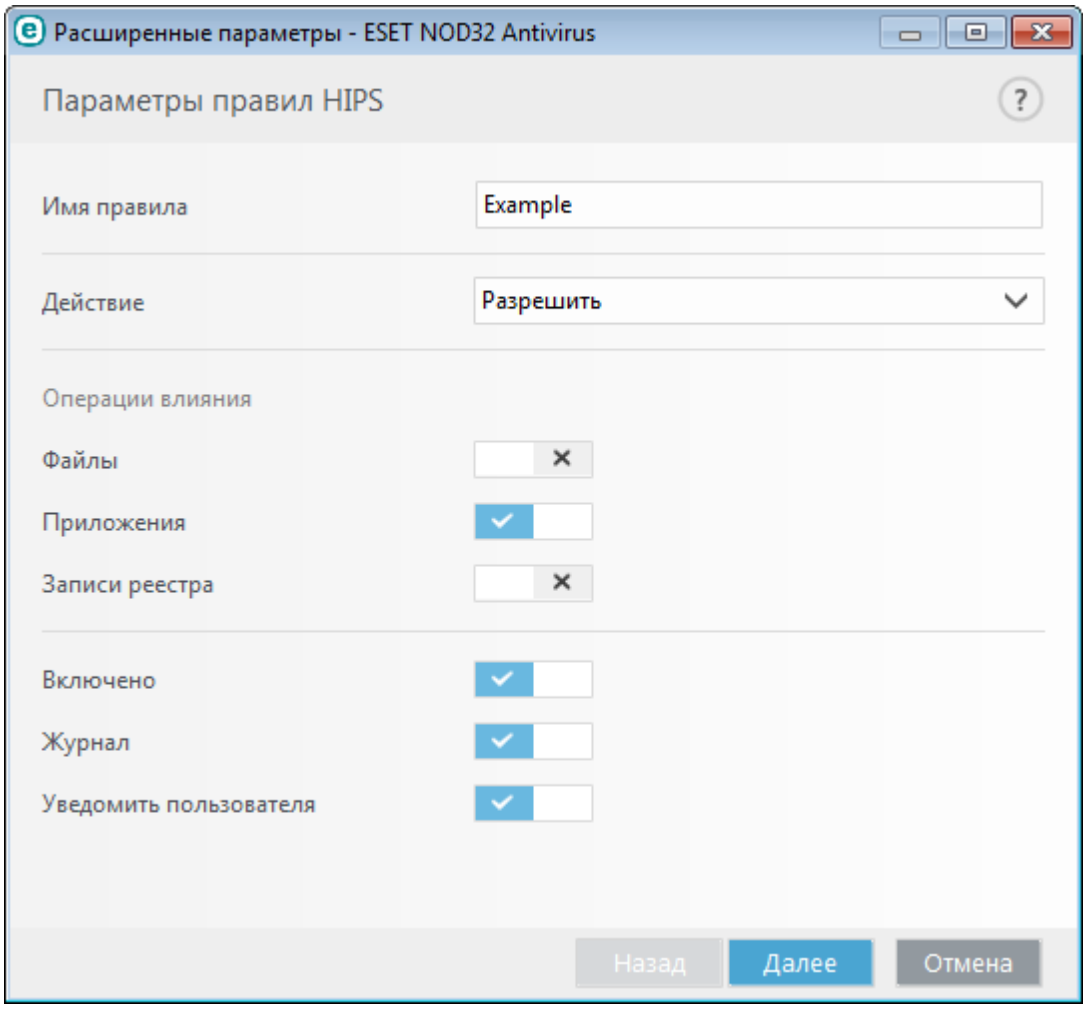
Режим обучения: операции включены, причем после каждой операции создается правило. Правила, создаваемые в таком режиме, можно просмотреть в редакторе правил, но их приоритет ниже, чем у правил, создаваемых вручную или в автоматическом режиме. Если в раскрывающемся списке режимов фильтрации HIPS выбран режим обучения, становится доступным параметр **Режим обучения завершится**. Выберите

длительность для режима обучения. Максимальная длительность — 14 дней. Когда указанный период завершится, вам будет предложено изменить правила, созданные системой HIPS в режиме обучения. Кроме того, можно выбрать другой режим фильтрации или отложить решение и продолжить использовать режим обучения.

Система предотвращения вторжений на узел отслеживает события в операционной системе и реагирует на них соответствующим образом на основе правил, которые аналогичны правилам персонального файервола. Нажмите кнопку **Изменить**, чтобы открыть окно управления правилами системы HIPS. Здесь можно выбирать, создавать, изменять и удалять правила.

В следующем примере будет показано, как ограничить нежелательное поведение приложений.

1. Присвойте правилу имя и выберите **Блокировать** в раскрывающемся меню **Действие**.
2. Активируйте переключатель **Уведомить пользователя**, чтобы уведомление отображалось при каждом применении правила.
3. Выберите хотя бы одну операцию, к которой будет применяться правило. В окне **Исходные приложения** выберите в раскрывающемся списке вариант **Все приложения**. Новое правило будет применяться ко всем приложениям, которые будут пытаться выполнить любое из выбранных действий по отношению к указанным приложениям.
4. Выберите **Изменить состояние другого приложения** (все операции описаны в справке по программе, которую можно открыть, нажав клавишу F1)..
5. Выберите в раскрывающемся списке вариант **Определенные приложения** и **добавьте** одно или несколько приложений, которые нужно защитить.
6. Нажмите кнопку **Готово**, чтобы сохранить новое правило.



4.1.4.1 Дополнительные настройки

Перечисленные далее параметры полезны для отладки и анализа поведения приложения.

Драйверы, загрузка которых разрешена всегда: загрузка выбранных драйверов разрешена всегда, вне зависимости от настроенного режима фильтрации, если они не заблокированы явно посредством пользовательского правила.

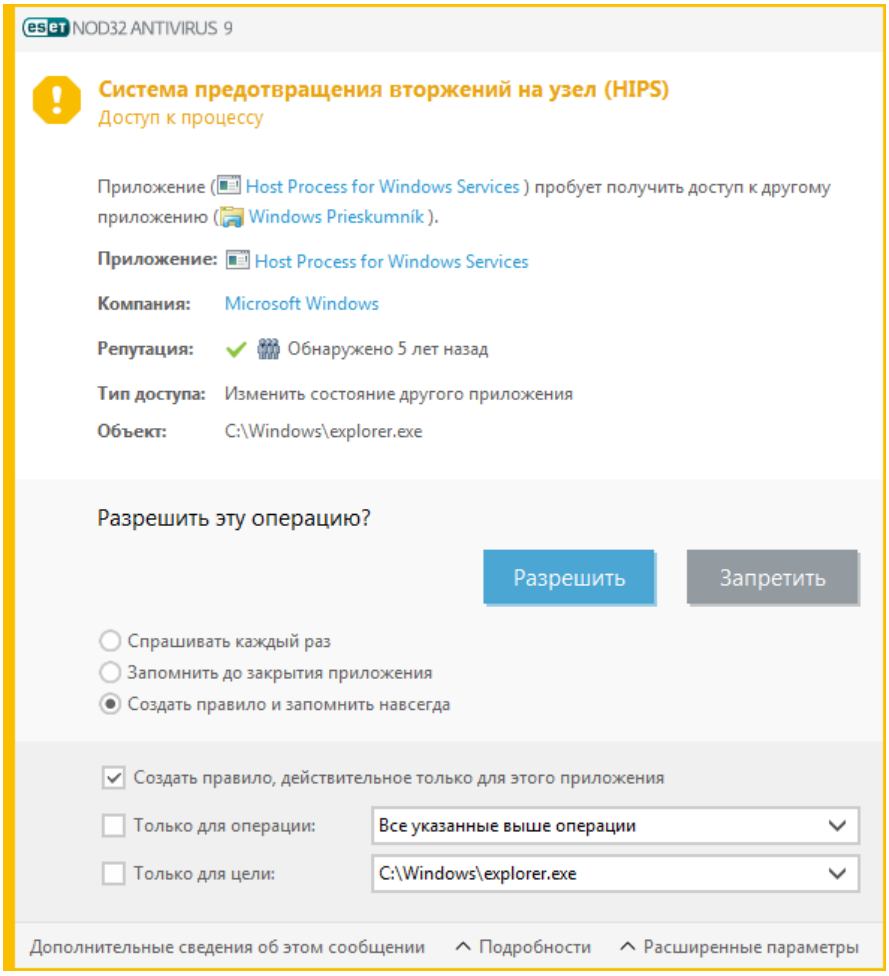
Регистрировать все заблокированные операции: все заблокированные операции будут записываться в журнал системы предотвращения вторжений на узел.

Сообщать об изменениях приложений, загружаемых при запуске системы: при добавлении или удалении приложения, загружаемого при запуске системы, на рабочем столе отображается уведомление.

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

4.1.4.2 Интерактивное окно HIPS

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



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

Временно запомнить это действие для данного процесса — если выбрать эту установку, действие (**Разрешить/**

Запретить) будет использоваться до тех пор, пока не изменятся правила или режимы фильтрации, не будет обновлен модуль системы HIPS или не будет выполнена перезагрузка компьютера. После выполнения любого из этих трех действий временные правила удаляются.

4.1.5 Игровой режим

Игровой режим — это функция для тех, кто стремится избежать перерывов в работе программного обеспечения и появления отвлекающих всплывающих окон, а также желает свести к минимуму нагрузку на процессор. Его также можно использовать во время презентаций, которые нельзя прерывать деятельностью модуля защиты от вирусов. При включении этой функции отключаются все всплывающие окна, а работа планировщика полностью останавливается. Защита системы по-прежнему работает в фоновом режиме, но не требует какого-либо вмешательства со стороны пользователя.

Включение и отключение игрового режима осуществляется в главном окне программы, в области, открываемой командой **Настройка** > **Защита компьютера**  или щелчком на пиктограмме  рядом с **Игровой режим**. Включая игровой режим, вы подвергаете систему угрозе, поэтому значок состояния защиты на панели задач станет оранжевого цвета, чтобы тем самым предупредить вас. Данное предупреждение также отобразится в главном окне программы: в нем отобразится надпись оранжевого цвета **Игровой режим включен**.

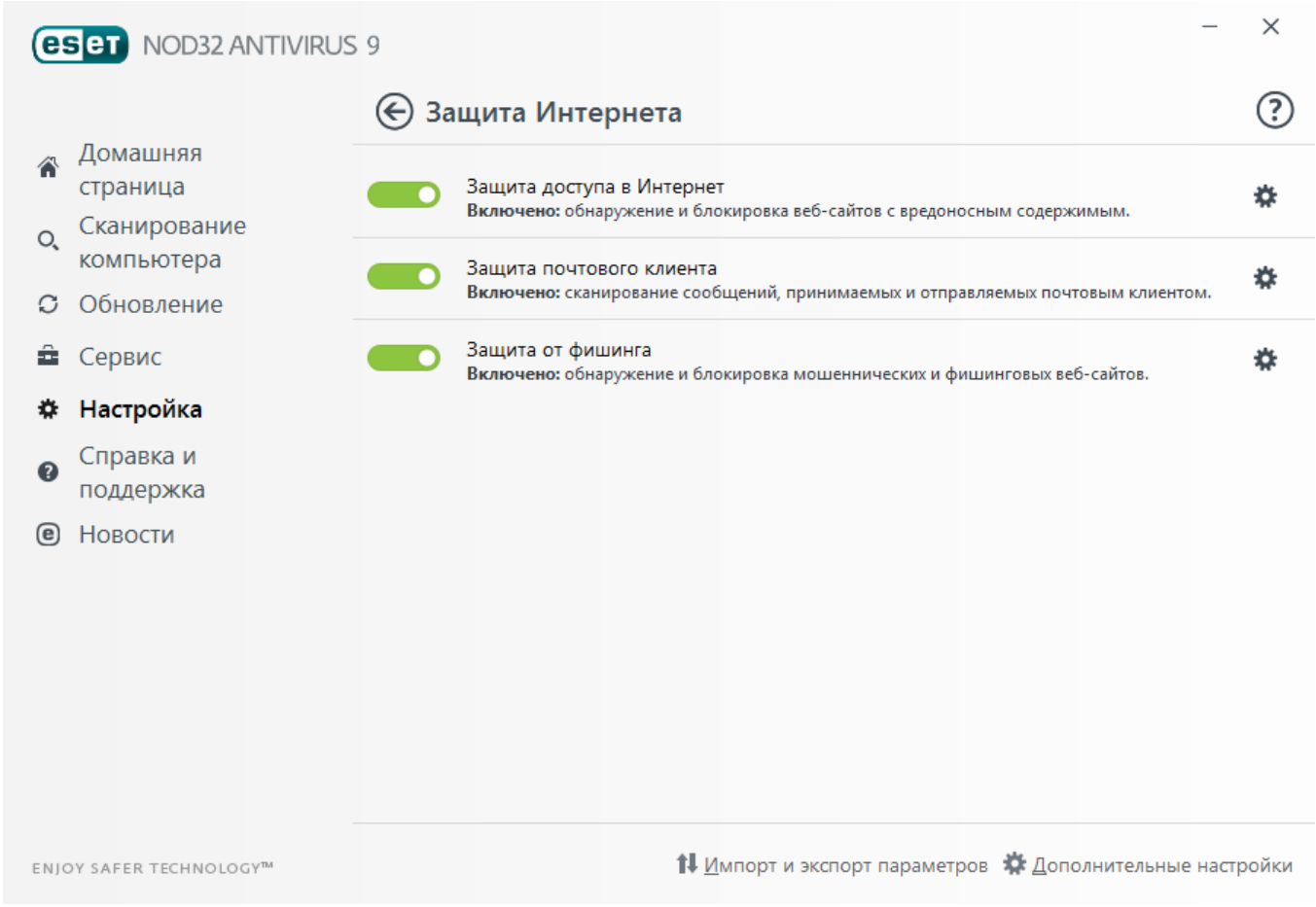
Игровой режим можно включить в дереве «Дополнительные настройки» (F5), развернув ветвь **Компьютер**, щелкнув элемент **Игровой режим** и установив флажок рядом с элементом **Включить игровой режим**.

Выберите элемент **Автоматически включать игровой режим при выполнении приложений в полноэкранном режиме** в дереве Дополнительные настройки (F5), чтобы игровой режим включался при переводе любого приложения в полноэкранный режим и выключался при выходе из полноэкранного режима.

Выберите установку **Автоматически отключать игровой режим через**, чтобы определить время, спустя которое игровой режим будет автоматически отключаться.

4.2 Защита в Интернете

Конфигурация параметров Интернета и электронной почты доступна на панели **Настройка**, которая появляется при нажатии параметра **Защита в Интернете**. В этом окне предоставляется доступ к более подробным настройкам программы.



Подключение к Интернету стало стандартной функцией персонального компьютера. К сожалению, Интернет также стал и основным средством распространения вредоносного кода. Поэтому крайне важно уделить особое внимание **защите доступа в Интернет**.

Щелкните , чтобы открыть параметры защиты в Интернете/защиты электронной почты/защиты от фишинга в разделе «Дополнительные настройки».

Защита почтового клиента обеспечивает контроль обмена данными электронной почты по протоколам POP3 и IMAP. При использовании подключаемого модуля для почтового клиента ESET NOD32 Antivirus позволяет контролировать весь обмен данными, осуществляемый почтовым клиентом (по протоколам POP3, MAPI, IMAP, HTTP).

Защита от фишинга дает возможность блокировать веб-страницы, на которых есть фишинговое содержимое. Настоятельно рекомендуется оставить все опции защиты от фишинга включенными.

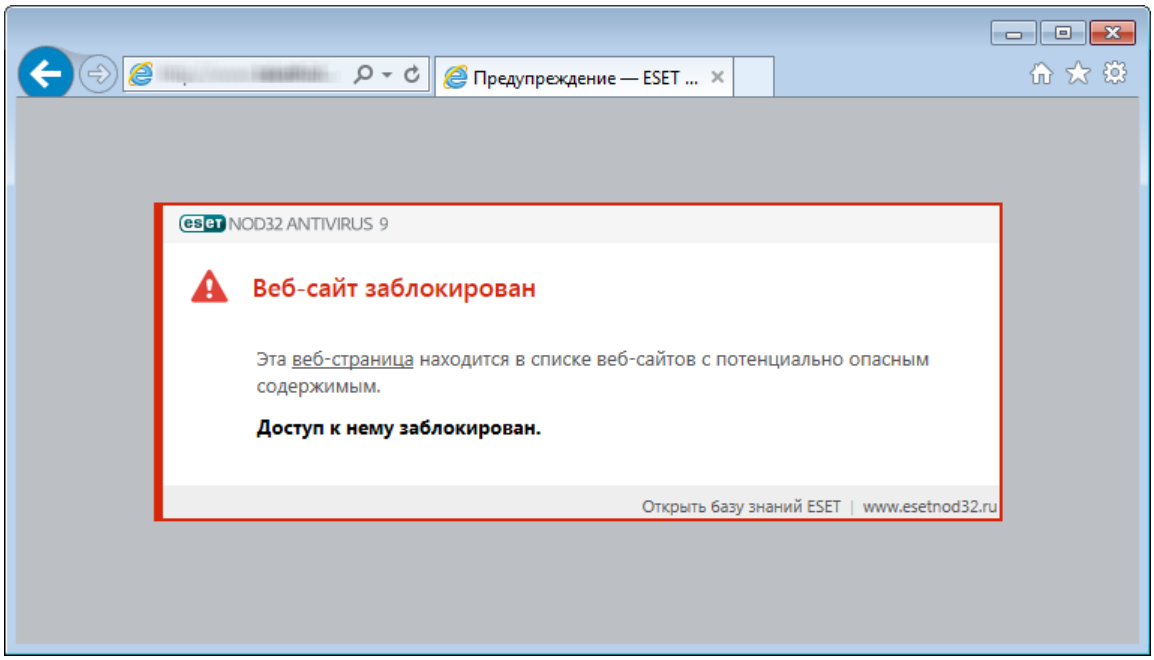
Вы можете отключить модули защиты от фишинга, защиты в Интернете/защиты электронной почты на некоторое время, щелкнув пункт .

4.2.1 Защита доступа в Интернет

Подключение к Интернету стало стандартной функцией персонального компьютера. К сожалению, Интернет также стал и основной средой распространения вредоносного кода. Защита доступа в Интернет работает путем отслеживания соединений между веб-браузерами и удаленными серверами в соответствии с правилами протоколов HTTP и HTTPS.

Доступ к веб-страницам, которые содержат заведомо вредоносное содержимое, блокируется до его загрузки. Все остальные веб-страницы при загрузке сканируются модулем сканирования ThreatSense и блокируются в случае обнаружения вредоносного содержимого. Защита доступа в Интернет предполагает два уровня: блокировка на основании «черного» списка и блокировка на основании содержимого.

Настоятельно рекомендуется не отключать защиту доступа в Интернет. Чтобы получить доступ к этой функции, в главном окне программы ESET NOD32 Antivirus выберите команду **Настройка** > **Интернет и электронная почта** > **Защита доступа в Интернет**.



В разделе **Дополнительные настройки** (F5) > **Интернет и электронная почта** > **Защита доступа в Интернет** доступны следующие параметры.

- **Веб-протоколы**: позволяет настроить отслеживание для стандартных протоколов, используемых в большинстве веб-браузеров.
- **Управление URL-адресами**: здесь можно задавать HTTP-адреса, которые следует блокировать, разрешить или исключать из проверки.
- **ThreatSense параметры** — Расширенная настройка модуля сканирования: позволяет настраивать определенные параметры, например тип сканируемых объектов (сообщения электронной почты, архивы и т. д.), методы обнаружения для защиты доступа в Интернет и т. д.

4.2.1.1 Основное

Включить защиту доступа в Интернет: когда этот параметр отключен, защита доступа в Интернет и защита от фишинга не обеспечиваются.

ПРИМЕЧАНИЕ. Настоятельно рекомендуется оставить все флажки установленными.

4.2.1.2 Веб-протоколы

По умолчанию ESET NOD32 Antivirus настроен на отслеживание протокола HTTP, используемого большинством интернет-браузеров.

Настройка модуля сканирования HTTP

В Windows Vista и более поздних версиях, HTTP-трафик отслеживается для всех портов и приложений. В операционной системе Windows XP можно вносить изменения в параметр **Порты, используемые протоколом HTTP** в окне, открываемом с помощью команды **Дополнительные настройки** (F5) > **Интернет и электронная почта** > **Защита доступа в интернет** > **Веб-протоколы**. HTTP-трафик всех приложений отслеживается по указанным портам для всех приложений и по всем портам для приложений, помеченных как веб-клиенты и почтовые клиенты.

Настройка модуля сканирования HTTPS

ESET NOD32 Antivirus также поддерживает проверку протокола HTTPS. При взаимодействии по протоколу HTTPS для передачи данных между сервером и клиентом используется зашифрованный канал. ESET NOD32 Antivirus осуществляет мониторинг передаваемых данных с использованием протоколов SSL (Secure Socket Layer) и TLS (Transport Layer Security). Программа осуществляет сканирование только тех портов, которые помечены как **Порты, используемые протоколом HTTPS**, вне зависимости от версии операционной системы.

Зашифрованные соединения не будут сканироваться. Чтобы включить сканирование зашифрованного обмена данными и просмотреть настройки модуля сканирования, перейдите к параметрам SSL/TLS в разделе «Дополнительные настройки», щелкните **Интернет и электронная почта** > **SSL/TLS** и установите флажок **Включить фильтрацию протоколов SSL/TLS**.

4.2.1.3 Управление URL-адресами

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

Посещение веб-сайтов, включенных в **Список заблокированных адресов невозможно**, кроме случаев, когда их адреса также включены в **Список разрешенных адресов**. Веб-сайты, добавленные в **Список адресов, для которых отключена проверка**, загружаются без проверки на наличие вредоносного кода.

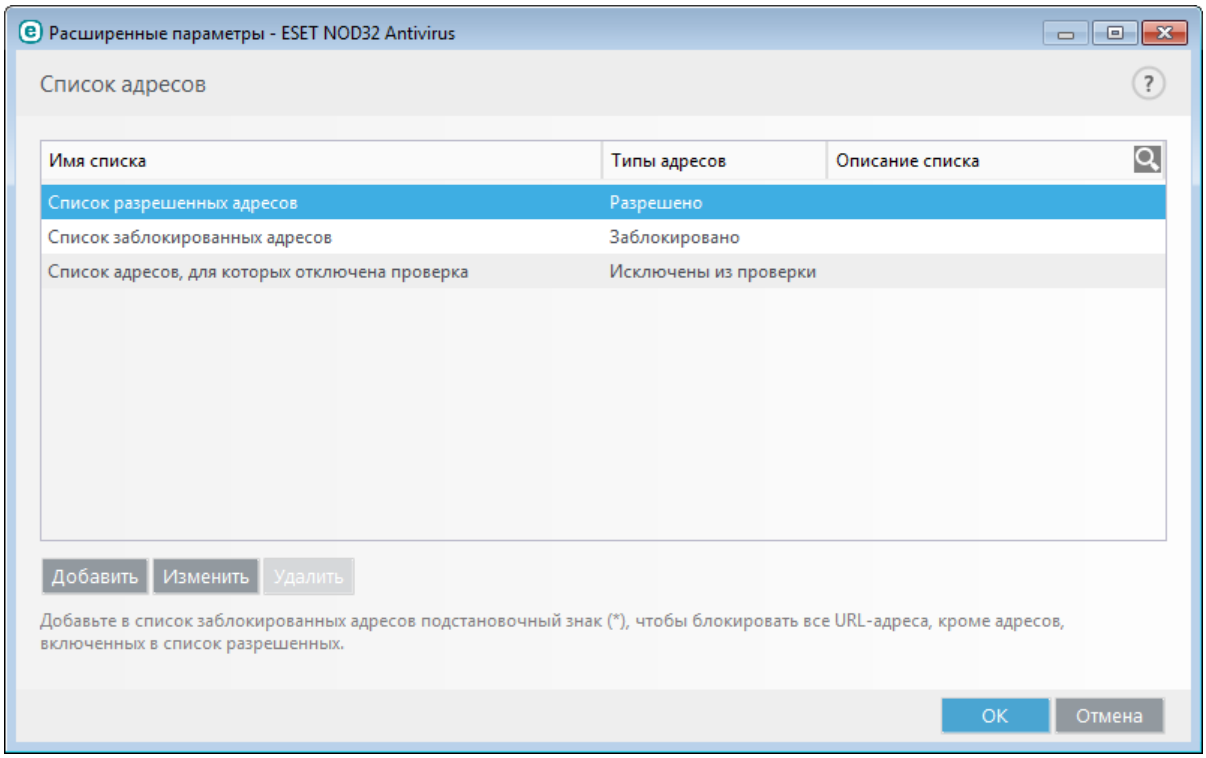
Включить фильтрацию протоколов SSL/TLS — это установка, предусмотренная на случай, когда кроме HTTP-сайтов требуется также фильтровать сайты, использующие протокол HTTPS. В противном случае в список будут добавлены только посещенные вами домены HTTPS-сайтов, а не полный URL-адрес.

Если добавить URL-адрес в **Список адресов, для которых отключена фильтрация**, этот адрес будет исключен из процесса сканирования. Также можно разрешать или блокировать определенные адреса, добавляя их соответственно в **Список разрешенных адресов** или в **Список заблокированных адресов**.

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

В списках можно использовать такие специальные символы, как «*» (звездочка) и «?» (вопросительный знак). Символ звездочки заменяет любую последовательность символов, а вопросительный знак — любой символ. Особое внимание следует уделить указанию адресов, исключенных из проверки, поскольку в этот список должны входить только доверенные и надежные адреса. Точно так же нужно убедиться в том, что символы шаблона в этом списке используются правильно. Сведения о том, как можно безопасно обозначить целый домен, включая все поддомены, см. в разделе Добавление HTTP-адреса или маски домена. Чтобы активировать список, установите флажок **Список активен**. Если вы хотите получать уведомления о том, что в адресную строку вводится адрес из текущего списка, установите флажок **Уведомлять о применении**.

ПОДСКАЗКА. Функция управления URL-адресами позволяет также блокировать или разрешать открытие файлов определенных типов при просмотре веб-страниц. Например, если не требуется открывать исполняемые файлы, выберите в раскрывающемся списке список, в котором хотите блокировать эти файлы, и введите маску «**.exe».



Элементы управления

Добавить: создание нового списка, дополняющего уже имеющиеся. Это может быть полезно в случае, если вы хотите логически разделить разные группы адресов. Например, один список заблокированных адресов может содержать адреса, полученные из какого-либо внешнего публичного черного списка, а второй — адреса, добавленные вами. Таким образом внешний список можно будет легко обновить, не внося изменений в ваш личный список.

Изменить: редактирование списков. Используйте эту установку для добавления или удаления адресов.

Удалить: удаление списков. Только для списков, созданных посредством команды **Добавить**. Удаление списков по умолчанию невозможно.

4.2.2 Защита почтового клиента

4.2.2.1 Почтовые клиенты

Интеграция ESET NOD32 Antivirus с почтовыми клиентами увеличивает уровень активной защиты от вредоносного кода в сообщениях электронной почты. Если используемый почтовый клиент поддерживается, в ESET NOD32 Antivirus можно настроить интеграцию. Если интеграция активирована, панель инструментов ESET NOD32 Antivirus добавляется непосредственно в почтовый клиент, обеспечивая более эффективную защиту электронной почты (панель инструментов для последних версий Почты Windows Live не добавляется). Параметры интеграции доступны в разделе **Настройка** > **Дополнительные настройки** > **Интернет и электронная почта** > **Защита почтового клиента** > **Почтовые клиенты**.

Интеграция с почтовым клиентом

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

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

Включите параметр **Отключить проверку при изменении содержимого папки "Входящие"**, если при

работе с почтовым клиентом наблюдается замедление работы системы (только для MS Outlook). Это возможно при извлечении сообщения электронной почты из хранилища Kerio Outlook Connector Store.

Сканируемая электронная почта

Полученные сообщения: включение или отключение проверки входящих сообщений.
Отправленные сообщения: включение или отключение проверки отправленных сообщений.
Прочитанные сообщения: включение или отключение проверки прочитанных сообщений.

Действие, применяемое к зараженному сообщению

Ничего не предпринимать: программа будет выявлять зараженные вложения, но не станет выполнять никаких действий с сообщениями электронной почты.
Удалить сообщение: программа будет уведомлять пользователя о заражениях и удалять сообщение.
Переместить сообщение в папку "Удаленные": зараженные сообщения будут автоматически перемещаться в папку «Удаленные».
Переместить сообщение в папку: зараженные сообщения будут автоматически перемещаться в указанную папку.

Папка: выбор папки, куда будут перемещаться обнаруженные зараженные сообщения электронной почты.

Повторить сканирование после обновления: включение или отключение повторного сканирования после обновления базы данных сигнатур вирусов.

Включить результаты сканирования другими модулями: если установлен этот флажок, модуль защиты электронной почты будет принимать результаты сканирования от других модулей защиты (сканирование каталогов POP3, IMAP).

4.2.2.2 Протоколы электронной почты

IMAP и POP3 — самые распространенные протоколы, используемые для получения электронной почты в почтовых клиентах. IMAP — это интернет-протокол для получения электронной почты, имеющий определенные преимущества перед POP3. Например, несколько клиентов могут одновременно подключаться к одному и тому же почтовому ящику и передавать сведения о состоянии сообщения, в частности сведения о том, что сообщение было прочитано, удалено или на него был дан ответ. ESET NOD32 Antivirus обеспечивает защиту этих протоколов вне зависимости от используемого почтового клиента и без необходимости перенастраивать почтовый клиент.

Модуль защиты, обеспечивающий такой контроль, автоматически запускается при запуске системы и остается активным в памяти. Проверка протокола IMAP осуществляется автоматически без дополнительной настройки почтового клиента. По умолчанию сканируются все данные, проходящие через порт 143, но при необходимости можно добавить и другие порты. Номера портов следует разделять запятыми.

Настроить проверку протоколов IMAP/IMAPS и POP3/POP3S можно в области дополнительных настроек. Для доступа к этим настройкам последовательно выберите элементы **Интернет и электронная почта** > **Защита почтового клиента** > **Протоколы электронной почты**.

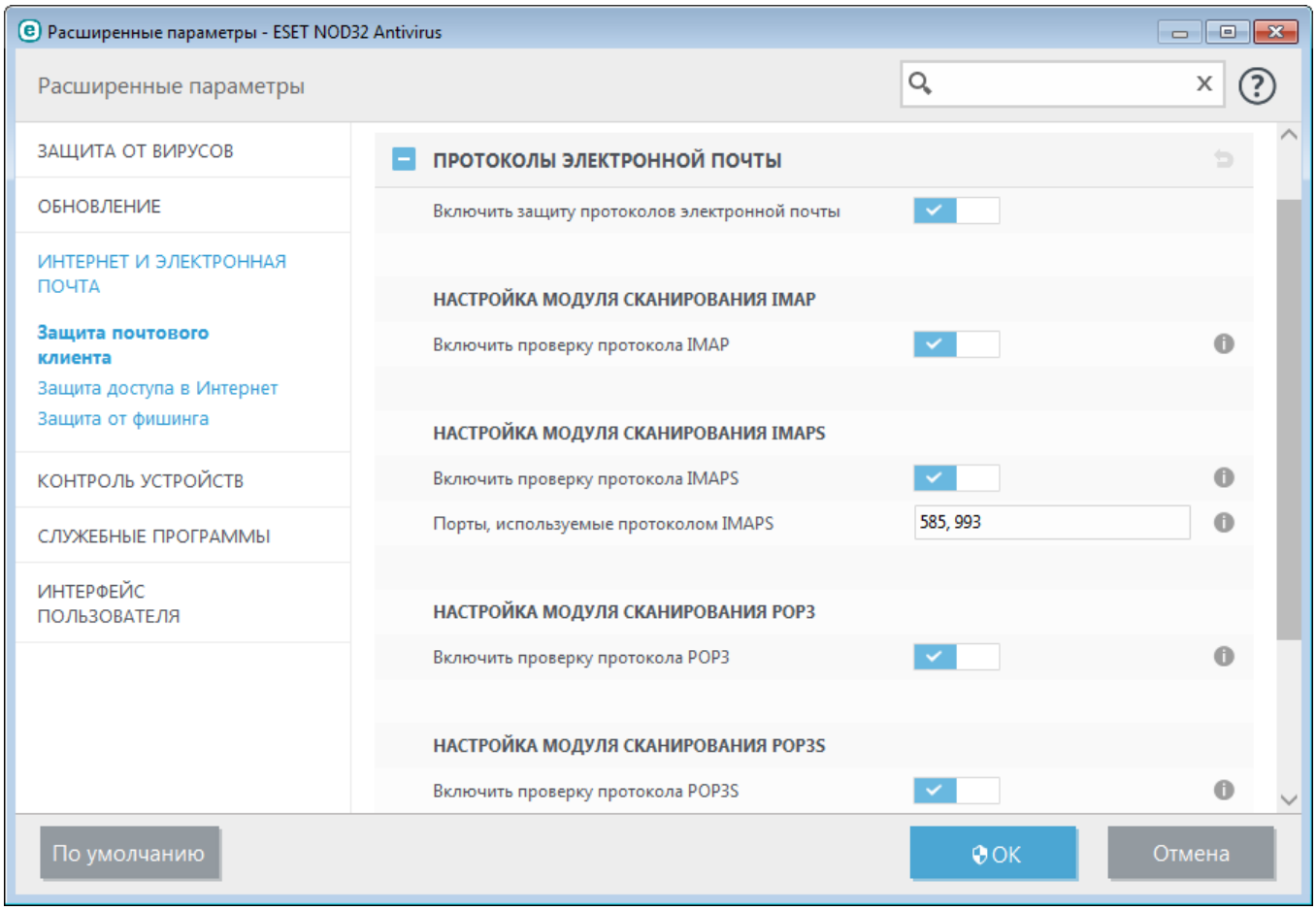
Включить защиту протоколов электронной почты: включение проверки протоколов электронной почты.

В Windows Vista и более поздних версиях протоколы IMAP и POP3 автоматически определяются и сканируются на всех портах. В Windows XP для всех приложений сканируются только настроенные **Порты, используемые протоколом IMAP или POP3**. Кроме того, все порты сканируются для приложений, отмеченных как Веб-клиенты и почтовые клиенты.

ESET NOD32 Antivirus также поддерживает сканирование протоколов IMAPS и POP3S, которые для передачи информации между сервером и клиентом используют зашифрованный канал. ESET NOD32 Antivirus осуществляет мониторинг передаваемых данных с использованием протоколов SSL (Secure Socket Layer) и TLS (Transport Layer Security). Программа будет выполнять сканирование трафика только для портов, указанных как **Порты, используемые протоколом IMAPS или POP3S**, вне зависимости от версии операционной системы.

Зашифрованные соединения не будут сканироваться. Чтобы включить сканирование зашифрованного обмена данными и просмотреть настройки модуля сканирования, перейдите к параметрам SSL/TLS в разделе

«Дополнительные настройки», щелкните **Интернет и электронная почта** > **SSL/TLS** и установите флажок **Включить фильтрацию протоколов SSL/TLS**.



4.2.2.3 Предупреждения и уведомления

Защита электронной почты обеспечивает контроль безопасности обмена данными по протоколам POP3 и IMAP. При использовании подключаемого модуля для Microsoft Outlook и других почтовых клиентов ESET NOD32 Antivirus позволяет контролировать весь обмен данными, осуществляемый почтовым клиентом (по протоколам POP3, MAPI, IMAP, HTTP). При проверке входящих сообщений программа использует все современные методы сканирования, обеспечиваемые модулем сканирования ThreatSense. Это позволяет обнаруживать вредоносные программы даже до того, как данные о них попадают в базу данных сигнатур вирусов. Сканирование соединений по протоколам POP3 и IMAP не зависит от используемого почтового клиента.

Параметры для этой функции настраиваются в области **Дополнительные настройки**, раздел **Интернет и электронная почта** > **Защита почтового клиента** > **Предупреждения и уведомления**.

ThreatSense параметры: расширенная настройка модуля сканирования для защиты от вирусов, которая позволяет настраивать объекты сканирования, способы обнаружения и т. д. Щелкните этот элемент, чтобы отобразилось окно тщательной настройки модуля сканирования.

После проверки к сообщению электронной почты может быть прикреплено уведомление с результатами сканирования. Вы можете выбрать **Добавление уведомлений к полученным и прочитанным сообщениям**, **Добавление примечаний в поле темы полученных и прочитанных зараженных сообщений** или **Добавление уведомлений к отправленным сообщениям**. Обратите внимание, что в некоторых случаях уведомления могут быть опущены в проблемных HTML-сообщениях или сфабрикованы некоторыми вирусами. Уведомления могут быть добавлены к входящим и прочитанным сообщениям или к исходящим сообщениям (или и к тем, и к другим). Доступны следующие варианты.

- **Никогда**: уведомления не будут добавляться вообще.
- **Только для инфицированных сообщений**: будут отмечены только сообщения, содержащие злонамеренные программы (по умолчанию).
- **Во все просканированные сообщения электронной почты**: программа будет добавлять уведомления ко всем просканированным сообщениям электронной почты.

Добавление примечаний в поле темы отправленных сообщений: установите этот флажок, если необходимо, чтобы подсистема защиты электронной почты добавляла предупреждения о вирусах в тему зараженных сообщений. Эта функция позволяет осуществлять простую фильтрацию зараженных сообщений по теме (если поддерживается почтовым клиентом). Также она повышает уровень доверия для получателя, а в случае обнаружения заражения предоставляет важную информацию об уровне угрозы для конкретного сообщения или отправителя.

Шаблон добавления к теме зараженных писем: этот шаблон можно изменить, если нужно отредактировать формат префикса, добавляемого ко всем зараженным сообщениям. Эта функция заменит тему сообщения *Hello* при заданном значении префикса *[virus]* на такой формат: *[virus] Hello*. Переменная *%VIRUSNAME%* представляет обнаруженную угрозу.

4.2.2.4 Интеграция с почтовыми клиентами

Интеграция ESET NOD32 Antivirus с почтовыми клиентами увеличивает уровень активной защиты от вредоносного кода в сообщениях электронной почты. Если используемый почтовый клиент поддерживается, в ESET NOD32 Antivirus можно настроить интеграцию. Если интеграция активирована, панель инструментов ESET NOD32 Antivirus вставляется непосредственно в почтовый клиент, обеспечивая более эффективную защиту электронной почты. Параметры интеграции доступны в разделе **Настройка** > **Перейти к дополнительным настройкам...** > **Интернет и электронная почта** > **Защита почтового клиента** > **Интеграция с почтовым клиентом**.

В настоящий момент поддерживаются следующие почтовые клиенты: Microsoft Outlook, Outlook Express, почта Windows, почта Windows Live. Полный список поддерживаемых почтовых клиентов и их версий см. в статье базы знаний ESET.

Установите флажок **Отключить проверку при изменении содержимого папки "Входящие"**, если при работе с почтовым клиентом наблюдается замедление работы системы. Это возможно при извлечении сообщения электронной почты из хранилища Kerio Outlook Connector Store.

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

4.2.2.4.1 Конфигурация защиты почтового клиента

Модуль защиты электронной почты поддерживает следующие почтовые клиенты: Microsoft Outlook, Outlook Express, почта Windows, почта Windows Live. Защита электронной почты реализована в этих программах в виде подключаемого модуля. Главное преимущество подключаемого модуля заключается в том, что он не зависит от используемого протокола. При получении почтовым клиентом зашифрованного сообщения оно расшифровывается и передается модулю сканирования.

4.2.2.5 Фильтр POP3, POP3S

POP3 — самый распространенный протокол, используемый для получения электронной почты в почтовых клиентах. ESET NOD32 Antivirus обеспечивает защиту этого протокола вне зависимости от используемого почтового клиента.

Модуль защиты, обеспечивающий эту функцию, автоматически инициируется при запуске операционной системы и остается активным в оперативной памяти. Для нормальной работы модуля убедитесь в том, что он включен. Проверка протокола POP3 осуществляется автоматически без необходимости в настройке почтового клиента. По умолчанию сканируются все соединения по порту 110, однако при необходимости могут быть добавлены и другие порты. Номера портов следует разделять запятыми.

Зашифрованные соединения не будут сканироваться. Чтобы включить сканирование зашифрованного обмена

данными и просмотреть настройки модуля сканирования, перейдите к параметрам SSL/TLS в разделе «Дополнительные настройки», щелкните **Интернет и электронная почта** > **SSL/TLS** и установите флажок **Включить фильтрацию протоколов SSL/TLS**.

В этом разделе можно конфигурировать проверку протоколов POP3 и POP3S.

Включить проверку писем: при включении этого параметра весь трафик, проходящий по протоколу POP3, проверяется на предмет наличия вредоносных программ.

Порты, используемые протоколом POP3: перечень портов, используемых протоколом POP3 (110 по умолчанию).

ESET NOD32 Antivirus также поддерживает проверку протокола POP3S. В этом типе соединения для передачи информации между сервером и клиентом используется зашифрованный канал. ESET NOD32 Antivirus проверяет соединения, использующие методы шифрования SSL и TLS.

Не проверять протокол POP3S: зашифрованные соединения не будут проверяться.

Проверять протокол POP3S на указанных портах: соединения по протоколу POP3S проверяются только на портах, указанных в параметре **Используемые протоколом POP3S порты**.

Используемые протоколом POP3S порты: перечень портов, используемых протоколом POP3S, которые следует проверять (995 по умолчанию).

4.2.3 Фильтрация протоколов

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

Включить фильтрацию содержимого, передаваемого по протоколам приложений: может использоваться для отключения фильтрации протоколов. Учтите, что многие компоненты ESET NOD32 Antivirus (защита доступа в Интернет, защита протоколов электронной почты, защита от фишинга и контроль доступа в Интернет) зависят от этого параметра и не смогут работать в случае его отключения.

Исключенные приложения: позволяет исключить указанные приложения из фильтрации протоколов. Полезно, если фильтрация протоколов вызывает проблемы совместимости.

Исключенные IP-адреса: позволяет исключить указанные удаленные адреса из процесса фильтрации протоколов. Полезно, если фильтрация протоколов вызывает проблемы совместимости.

Веб-клиенты и почтовые клиенты: используется только в операционных системах Windows XP и позволяет выбирать приложения, трафик которых будет подвергаться фильтрации протоколов, вне зависимости от используемого порта.

4.2.3.1 Клиенты Интернета и электронной почты

ПРИМЕЧАНИЕ. Начиная с ОС Windows Vista с пакетом обновления 1 и Windows Server 2008, для проверки сетевых соединений используется новая архитектура платформы фильтрации Windows (WFP). Так технология платформы фильтрации Windows использует особые методы отслеживания, раздел **Клиенты Интернета и электронной почты** недоступен.

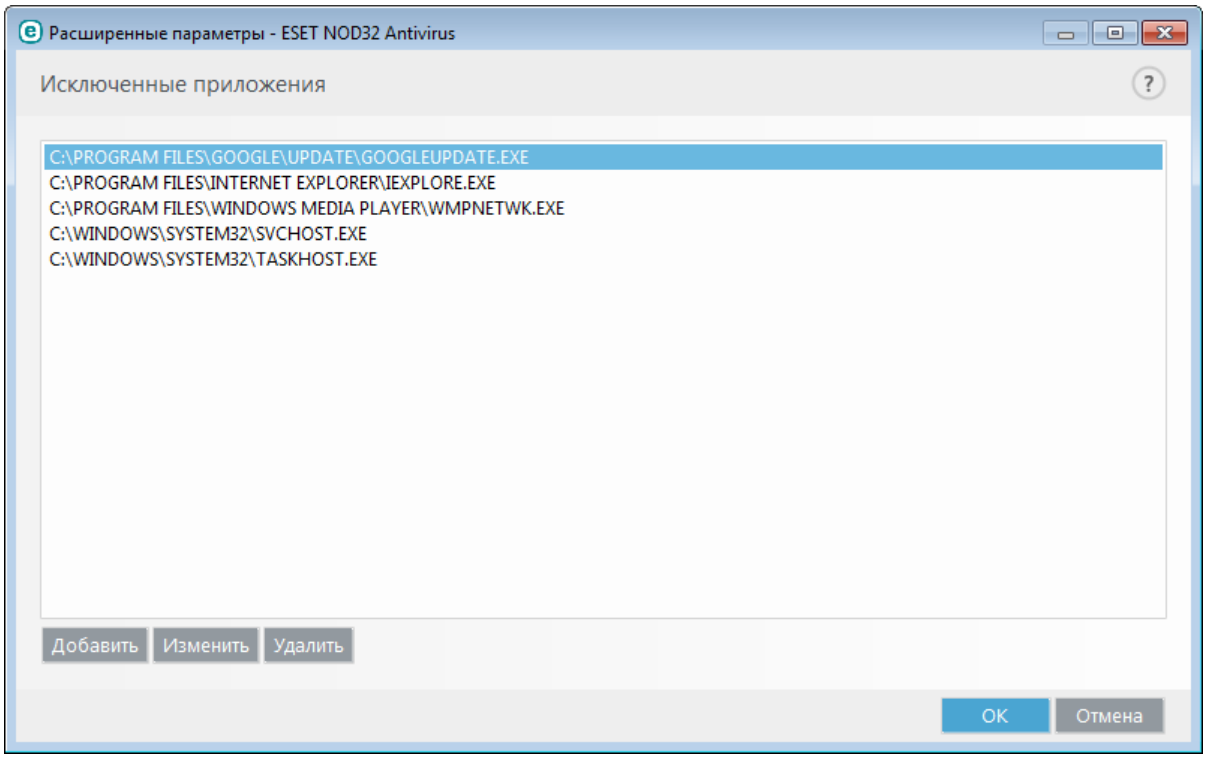
В условиях перенасыщенности Интернета вредоносными программами безопасное посещение веб-страниц является важным аспектом защиты компьютера. Уязвимости веб-браузеров и мошеннические ссылки позволяют вредоносным программам незаметно проникать в систему. Именно поэтому в программном обеспечении ESET NOD32 Antivirus основное внимание уделяется обеспечению безопасности веб-браузеров. Каждое приложение, обращающееся к сети, может быть помечено как веб-браузер. Флажок имеет два состояния.

- **Не установлен**: подключения приложений фильтруются только для указанных портов.
- **Установлен**: подключения всегда фильтруются (даже если задан другой порт).

4.2.3.2 Исключенные приложения

Для исключения соединений определенных сетевых приложений из фильтрации содержимого выделите их в списке. Соединения выделенных приложений по протоколам HTTP/POP3/IMAP не будут проверяться на наличие угроз. Рекомендуется использовать эту возможность только для тех приложений, которые работают некорректно, если их соединения проверяются.

Запуск приложений и служб будет доступен автоматически. Нажмите кнопку **Добавить**, чтобы вручную выбрать приложение, отсутствующее в списке фильтрации протоколов.

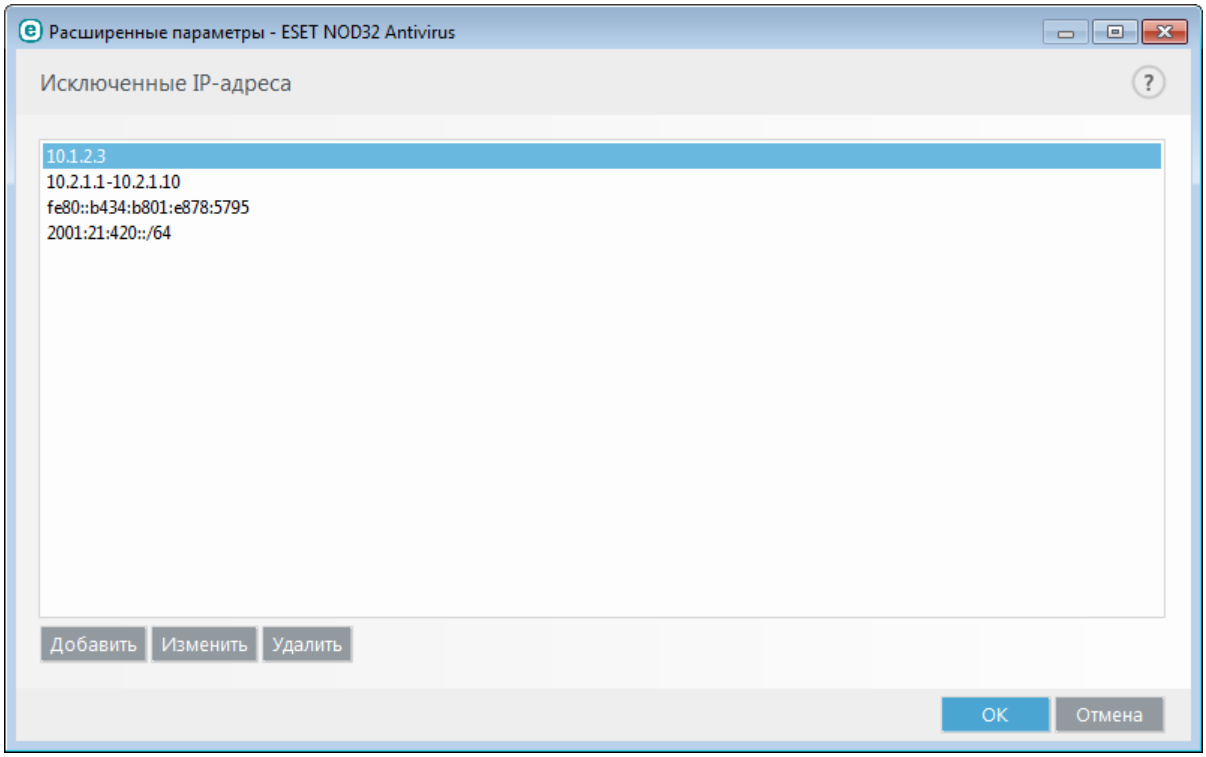


4.2.3.3 Исключенные IP-адреса

Записи в списке будут исключены из фильтрации содержимого протоколов. Соединения по протоколам HTTP/POP3/IMAP, в которых участвуют выбранные адреса, не будут проверяться на наличие угроз. Этот параметр рекомендуется использовать только для заслуживающих доверия адресов.

Нажмите кнопку **Добавить**, чтобы исключить IP-адрес, диапазон адресов или подсеть удаленного узла, не отображаемого в списке фильтрации протокола.

Нажмите кнопку **Удалить**, чтобы удалить выделенные записи из списка.



4.2.3.3.1 Добавить адрес IPv4

Этот функция позволяет добавить IP-адрес, диапазон адресов или маску подсети удаленной конечной точки, к которой должно быть применено правило. Интернет-протокол версии 4 (IPv4) — это устаревшая версия, но она до сих пор широко используется.

Отдельный адрес: добавляет IP-адрес отдельного компьютера, для которого должно быть применено правило (например, *192.168.0.10*).

Диапазон адресов: введите начальный и конечный IP-адреса, чтобы задать тем самым диапазон IP-адресов (или несколько компьютеров), к которым следует применить правило (например, от *192.168.0.1* до *192.168.0.99*).

Подсеть: подсеть (группа компьютеров), заданная IP-адресом и маской.

Например, *255.255.255.0* — это маска сети для префикса *192.168.1.0/24*, который означает диапазон адресов от *192.168.1.1* до *192.168.1.254*.

4.2.3.3.2 Добавить адрес IPv6

Этот функция позволяет добавить IPv6-адрес или маску подсети удаленной конечной точки, к которой должно быть применено правило. Это новейшая версия интернет-протокола, и в будущем она заменит более старую версию 4.

Отдельный адрес: добавляет IP-адрес отдельного компьютера, для которого должно быть применено правило (например, *2001:718:1c01:16:214:22ff:fec9:ca5*).

Подсеть: подсеть (группа компьютеров), заданная IP-адресом и маской (например, *2002:c0a8:6301:1::1/64*).

4.2.3.4 SSL/TLS

ESET NOD32 Antivirus может проверять обмен данных посредством протокола SSL на наличие угроз. Можно использовать различные режимы сканирования для защищенных SSL-соединений, для которых используются доверенные сертификаты, неизвестные сертификаты или сертификаты, исключенные из проверки защищенных SSL-соединений.

Включить фильтрацию протокола SSL: если фильтрация протокола отключена, программа не сканирует обмен данными по протоколу SSL.

Режим фильтрации протоколов SSL/TLS доступен со следующими параметрами.

Автоматический режим: используемый по умолчанию режим, в котором сканируются только соответствующие приложения, такие как браузеры и почтовые клиенты. Его можно переопределить, выбрав приложения, для которых будет сканироваться передача данных.

Интерактивный режим: при выполнении входа на новый защищенный SSL-сайт (с неизвестным сертификатом) на экран выводится диалоговое окно выбора. Этот режим позволяет создавать список сертификатов SSL, которые будут исключены из сканирования.

Режим политики: выберите этот вариант, чтобы сканировать все защищенные SSL-соединения, кроме тех, что защищены исключенными из проверки сертификатами. Если устанавливается новое соединение, использующее неизвестный заверенный сертификат, пользователь не получит уведомления, а само соединение автоматически будет фильтроваться. При доступе к серверу с ненадежным сертификатом, который помечен пользователем как доверенный (добавлен в список доверенных сертификатов), соединение с этим сервером разрешается, а содержимое канала связи фильтруется.

Список приложений, отфильтрованных с помощью SSL: позволяет настраивать поведение ESET NOD32 Antivirus для заданных приложений.

Список известных сертификатов: позволяет настроить поведение ESET NOD32 Antivirus в отношении конкретных сертификатов SSL.

Исключить обмен данными, защищенный с помощью сертификатов высокой надежности (EV): когда этот параметр включен, обмен данными с таким типом сертификата SSL будет исключен из проверки. SSL-сертификаты высокой надежности гарантируют, что осуществляется просмотр именно требуемого сайта, а не идентично выглядящего поддельного (обычно поддельными бывают фишинговые сайты).

Блокировать шифрованное соединение с использованием устаревшего протокола SSL версии 2: соединения, использующие более раннюю версию протокола SSL, будут автоматически блокироваться.

Корневой сертификат

Добавить корневой сертификат в известные браузеры: для нормальной работы SSL-подключений в браузерах и почтовых клиентах необходимо добавить корневой сертификат ESET в список известных корневых сертификатов (издателей). При включении этого параметра ESET NOD32 Antivirus автоматически добавляет корневой сертификат ESET в известные браузеры (например, Opera и Firefox). Для браузеров, использующих системное хранилище сертификатов (например, Internet Explorer), сертификат добавляется автоматически.

Для установки сертификата в неподдерживаемые браузеры последовательно выберите элементы **Просмотреть сертификат** > **Дополнительно** > **Копировать в файл...**, а затем вручную импортируйте этот

сертификат в браузер.

Срок действия сертификата

Если проверить сертификат с помощью хранилища сертификатов TRCA не удается: в некоторых случаях сертификат невозможно проверить с помощью хранилища доверенных корневых центров сертификации. Это значит, что у сертификата существует собственная подпись какого-либо другого субъекта (например, администратора веб-сервера или небольшой компании) и принятие решения о выборе такого сертификата как доверенного не всегда представляет опасность. Большинство крупных компаний (например, банки) используют сертификаты, подписанные TRCA. Если установлен флажок **Запрашивать действительность сертификата** (по умолчанию), пользователю будет предложено выбрать действие, которое следует предпринять во время установки зашифрованного соединения. Можно выбрать вариант **Блокировать соединения, использующие сертификат**, чтобы всегда разрывать зашифрованные соединения с сайтом, использующим непроверенный сертификат.

Если сертификат недействителен или поврежден: это значит, что истек срок действия сертификата или же используется недопустимая подпись. В этом случае рекомендуется выбрать **Блокировать соединения, использующие сертификат**.

4.2.3.4.1 Сертификаты

Для нормальной работы SSL-подключений в браузерах и почтовых клиентах необходимо добавить корневой сертификат ESET в список известных корневых сертификатов (издателей). Параметр **Добавить корневой сертификат к известным браузерам** должен быть активирован. Выберите этот параметр, чтобы автоматически добавить корневой сертификат ESET в известные браузеры (например, Opera, Firefox). Для браузеров, использующих системное хранилище сертификатов (например, Internet Explorer), сертификат добавляется автоматически. Для установки сертификата в неподдерживаемые браузеры выберите **Просмотреть сертификат** > **Дополнительно** > **Копировать в файл...**, а затем вручную импортируйте его в браузер.

В некоторых случаях сертификат невозможно проверить с помощью хранилища доверенных корневых сертификатов сертифицирующих органов (например, VeriSign). Это значит, что у сертификата существует собственная подпись какого-либо другого субъекта (например, администратора веб-сервера или небольшой компании) и принятие решения о выборе такого сертификата как доверенного не всегда представляет опасность. Большинство крупных компаний (например, банки) используют сертификаты, подписанные TRCA. Если установлен флажок **Запрашивать действительность сертификата** (по умолчанию), пользователю будет предложено выбрать действие, которое следует предпринять во время установки зашифрованного соединения. На экране отобразится диалоговое окно для выбора действия, в котором можно принять решение о том, что следует сделать: пометить сертификат как доверенный или как исключенный. Если сертификат отсутствует в списке хранилища доверенных корневых сертификатов сертифицирующих органов, для оформления окна используется красный цвет. Если же сертификат есть в этом списке, окно будет оформлено зеленым цветом.

Можно выбрать вариант **Блокировать соединения, использующие сертификат**, чтобы всегда разрывать зашифрованные соединения с сайтом, использующим непроверенный сертификат.

Если этот сертификат недействителен или поврежден, это значит, что истек срок действия сертификата или же используется неверное собственное заверение. В этом случае рекомендуется блокировать соединения, использующие данный сертификат.

4.2.3.4.2 Список известных сертификатов

Список известных сертификатов позволяет настроить поведение ESET NOD32 Antivirus в отношении конкретных сертификатов SSL, а также настроить запоминание действий пользователя, если в режиме **Фильтрация протоколов SSL/TLS** выбран **Интерактивный режим**. Список можно просмотреть и отредактировать, последовательно выбрав элементы **Дополнительные настройки** (F5) > **Интернет и электронная почта** > **SSL/TLS** > **Список известных сертификатов**.

В окне **Список известных сертификатов** имеются перечисленные ниже элементы.

Столбцы

Имя: имя сертификата.

Издатель сертификата: имя создателя сертификата.

Субъект сертификата: в этом поле указывается субъект, которому принадлежит открытый ключ, содержащийся в поле открытого ключа субъекта.

Доступ: в качестве значения параметра **Действие доступа** выберите установку **Разрешить** или **Заблокировать**, чтобы разрешить или заблокировать обмен данными, защищенный этим сертификатом, вне зависимости от его надежности. Выберите установку **Автоматически**, чтобы разрешать доверенные сертификаты и предлагать варианты действий для ненадежных. Выберите **Запрашивать**, чтобы всегда запрашивать действия пользователя.

Сканировать: чтобы сканировать или игнорировать соединение, защищенное сертификатом, выберите значение **Сканировать** или **Пропустить** для параметра **Действие сканирования**. Выберите установку **Автоматически**, чтобы сканирование выполнялось в автоматическом режиме, а запрос действия — в интерактивном. Чтобы программа всегда запрашивала у пользователя, какое действие следует выполнить, выберите установку **Запрашивать**.

Элементы управления

Изменить: выберите сертификат, который нужно настроить, и нажмите кнопку **Изменить**.

Удалить: выберите сертификат, который нужно удалить, и нажмите кнопку **Удалить**.

ОК/Отмена : нажмите кнопку **ОК** для сохранения изменений или **Отмена** для их отмены.

4.2.3.4.3 Список приложений, отфильтрованных с помощью SSL

Список приложений, отфильтрованных с помощью SSL может использоваться для настройки ESET NOD32 Antivirus поведения в отношении конкретных приложений, а также запоминания действий пользователя, если в режиме **Фильтрация протокола SSL** выбран **Интерактивный режим**. Список можно просмотреть и отредактировать, последовательно выбрав элементы **Дополнительные настройки** (F5) > **Интернет и электронная почта** > **SSL/TLS** > **Список приложений, отфильтрованных с помощью SSL**.

В окне **Список приложений, отфильтрованных с помощью SSL** имеются перечисленные ниже элементы.

Столбцы

Приложение: имя приложения.

Действие сканирования: Выберите **Сканировать** или **Пропустить**, чтобы сканировать или игнорировать обмен данными. Выберите установку **Автоматически**, чтобы сканирование выполнялось в автоматическом режиме, а запрос действия — в интерактивном. Чтобы программа всегда запрашивала у пользователя, какое действие следует выполнить, выберите установку **Запрашивать**.

Элементы управления

Добавить: добавление фильтрованных приложений.

Изменить: выберите сертификат, который нужно настроить, и нажмите кнопку **Изменить**.

Удалить: выберите сертификат, который нужно удалить, и нажмите кнопку **Удалить**.

ОК/Отмена : нажмите кнопку **ОК** для сохранения изменений или **Отмена** для их отмены.

4.2.4 Защита от фишинга

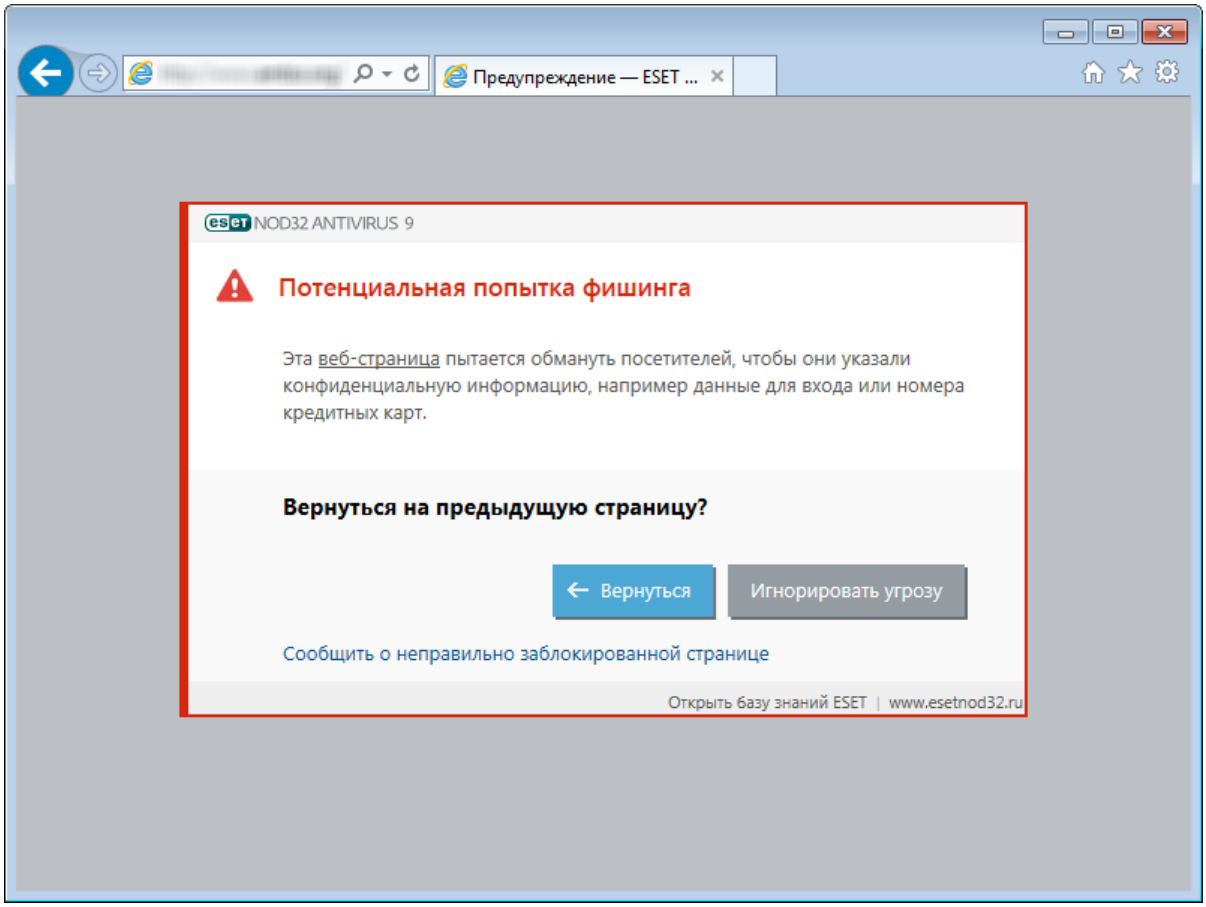
Термин «фишинг» обозначает преступную деятельность, в рамках которой используется социальная инженерия (манипулирование пользователями, направленное на получение конфиденциальной информации). Фишинг часто используется для получения доступа к конфиденциальным сведениям, таким как номера банковских счетов, PIN-коды и т. п. Дополнительные сведения об этом типе защиты см. в глоссарии. ESET NOD32 Antivirus обеспечивает защиту от фишинга: блокирование веб-страниц, которые заведомо распространяют содержимое такого типа.

Настоятельно рекомендуется включить защиту от фишинга в программе ESET NOD32 Antivirus. Для этого нужно в окне **Дополнительные настройки** (F5) последовательно щелкнуть элементы **Интернет и электронная почта** > **Защита от фишинга**.

В статье нашей базы знаний приведены дополнительные сведения о защите от фишинга в программе ESET NOD32 Antivirus.

Доступ к фишинговому веб-сайту

Когда открывается фишинговый веб-сайт, в веб-браузере отображается следующее диалоговое окно. Если вы все равно хотите открыть этот веб-сайт, щелкните элемент **Игнорировать угрозу** (не рекомендуется).



ПРИМЕЧАНИЕ. Время, в течение которого можно получить доступ к потенциальному фишинговому веб-сайту, занесенному в «белый» список, по умолчанию истекает через несколько часов. Чтобы разрешить доступ к веб-сайту на постоянной основе, используйте инструмент Управление URL-адресами. В разделе **Дополнительные настройки** (F5) последовательно щелкните элементы **Интернет и электронная почта** > **Защита доступа в Интернет** > **Управление URL-адресами** > **Список адресов**, выберите команду **Изменить** и добавьте необходимый веб-сайт в список.

Сообщение о фишинговом сайте

Ссылка Сообщить позволяет сообщить о фишинговом или вредоносном веб-сайте в компанию ESET с целью проведения его анализа.

ПРИМЕЧАНИЕ. Прежде чем отправлять адрес веб-сайта в компанию ESET, убедитесь в том, что он соответствует одному или нескольким из следующих критериев:

- веб-сайт совсем не обнаруживается;
- веб-сайт неправильно обнаруживается как угроза. В таком случае можно сообщить о ложной метке фишингового сайта.

Или же адрес веб-сайта можно отправить по электронной почте. Отправьте письмо на адрес samples@eset.com. Помните, что тема письма должна описывать проблему, а в тексте письма следует указать максимально полную информацию о веб-сайте (например, веб-сайт, с которого вы попали на этот сайт, как вы узнали об этом сайте и т. д.).

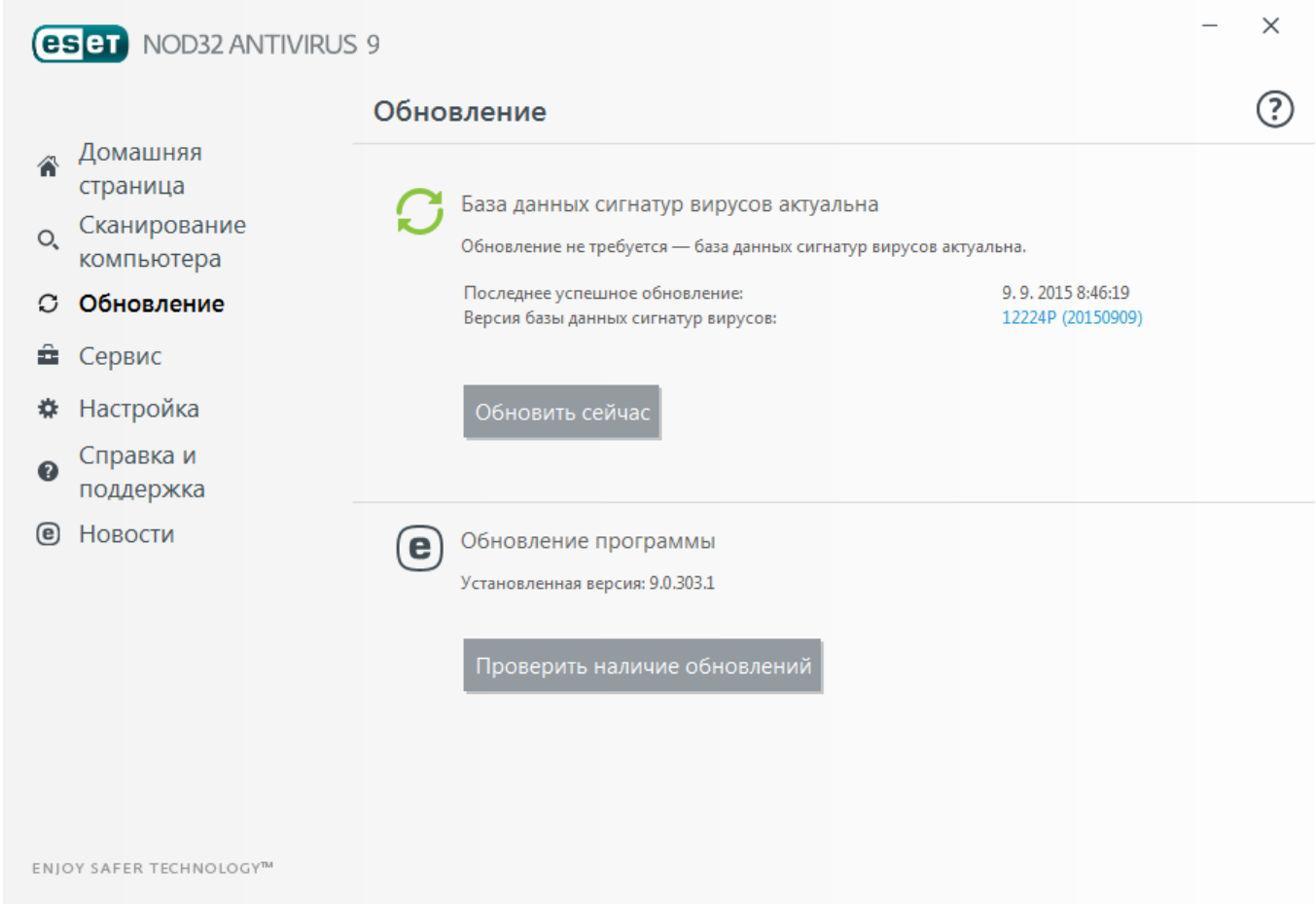
4.3 Обновление программы

Регулярное обновление ESET NOD32 Antivirus — лучший способ обеспечить максимальный уровень безопасности компьютера. Модуль обновления поддерживает актуальность программы двумя способами: путем обновления базы данных сигнатур вирусов и путем обновления компонентов системы.

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

Также можно выполнить обновление вручную, нажав кнопку **Обновить сейчас**. Обновление базы данных сигнатур вирусов и компонентов программы является важнейшей частью обеспечения полной защиты компьютера от злонамеренного кода. Уделите особое внимание изучению конфигурирования и работы этого процесса. Для получения обновлений необходимо активировать продукт с помощью вашего лицензионного ключа. Если лицензионный ключ не был указан в процессе установки, это можно сделать для активации программы при обновлении, чтобы получить доступ к серверам обновлений ESET.

ПРИМЕЧАНИЕ: Лицензионный ключ предоставляется по электронной почте компанией ESET после приобретения ESET NOD32 Antivirus.



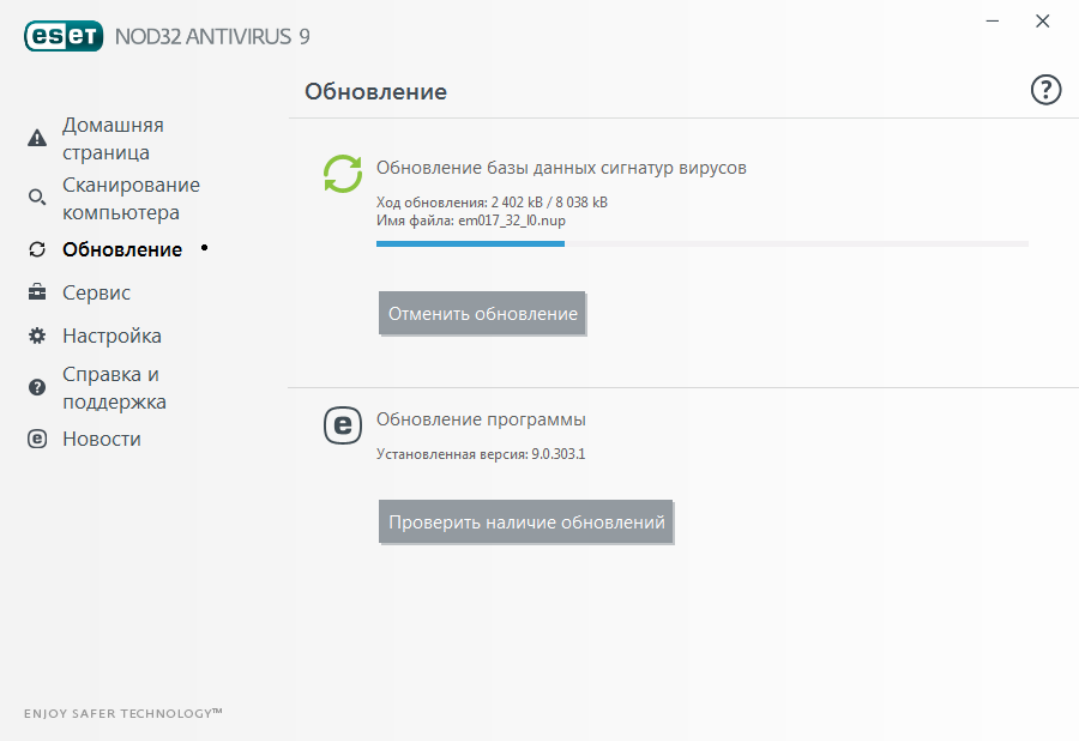
Последнее успешное обновление — дата последнего обновления. Если не отображается недавняя дата, возможно, база данных сигнатур вирусов неактуальна.

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

Нажмите **Проверить наличие обновлений**, чтобы найти последнюю доступную версию ESET NOD32 Antivirus.

Процесс обновления

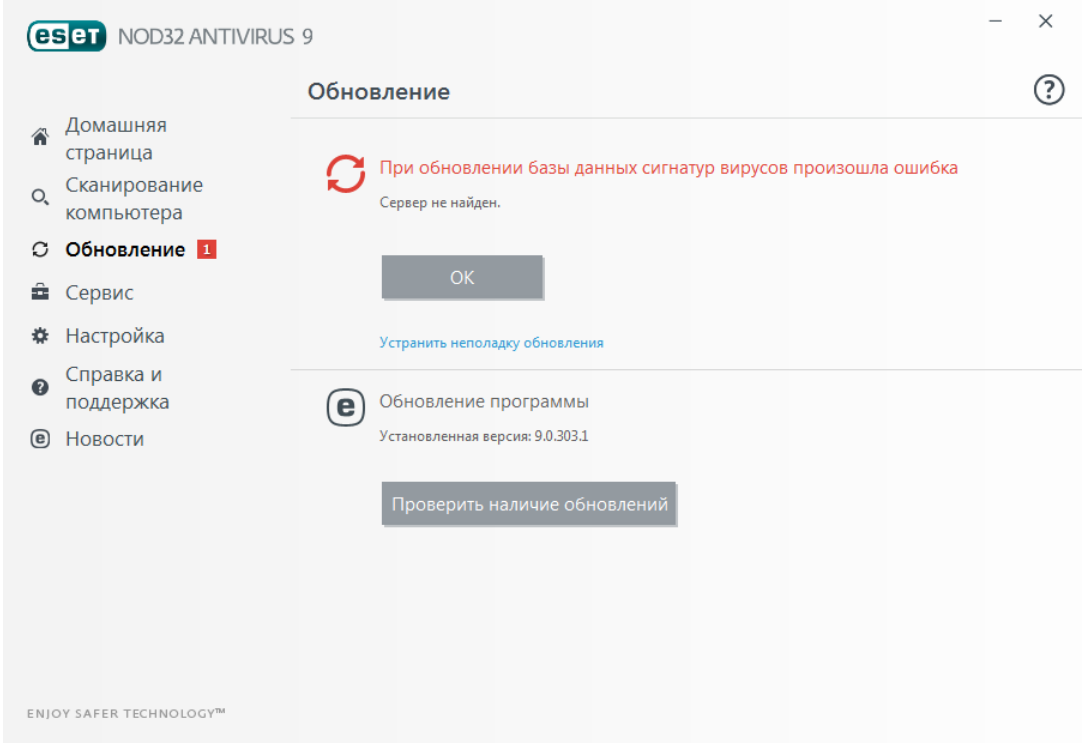
После нажатия кнопки **Обновить** начинается загрузка. На экран будут выведены индикатор выполнения загрузки и время до ее окончания. Чтобы прервать процесс обновления, нажмите **Отменить обновление**.



Внимание! В обычных обстоятельствах в окне **Обновление** отображается сообщение **Обновление не требуется, поскольку установленная база данных сигнатур вирусов является актуальной.**. Если этого сообщения нет, программа устарела. При этом повышается риск заражения. Необходимо обновить базу данных сигнатур вирусов как можно скорее. В противном случае на экран будет выведено одно из следующих сообщений.

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

1. **Недействительная лицензия**: в разделе параметров обновления введен неправильный лицензионный ключ. Рекомендуется проверить данные аутентификации. В окне «Дополнительные настройки» (в главном меню выберите пункт **Настройка**, после чего щелкните **Дополнительные настройки** или нажмите клавишу F5) содержатся расширенные параметры обновления. В главном меню последовательно щелкните элементы **Справка и поддержка** > **Изменить лицензию** и введите новый лицензионный ключ.
2. **Произошла ошибка при загрузке файлов обновлений**: возможная причина этой ошибки — неправильные параметры подключения к Интернету. Рекомендуется проверить наличие подключения к Интернету (например, попробуйте открыть любой веб-сайт в браузере). Если веб-сайт не открывается, возможно, не установлено подключение к Интернету или на компьютере возникли какие-либо проблемы с подключением к сети. Обратитесь к своему поставщику услуг Интернета, чтобы выяснить, есть ли у вас активное подключение к Интернету.



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

4.3.1 Параметры обновления

Параметры обновления доступны в дереве **Дополнительные настройки** (F5) в разделе **Обновление** > **Обычная**. В этом разделе приводится информация об источниках обновлений, таких как серверы обновлений, а также требуемые для них данные аутентификации.

Общие

Используемый в данный момент профиль обновления отображается в раскрывающемся списке **Выбранный профиль**. Чтобы создать профиль, рядом с элементом **Список профилей** нажмите кнопку **Изменить**, введите **Имя профиля** и нажмите кнопку **Добавить**.

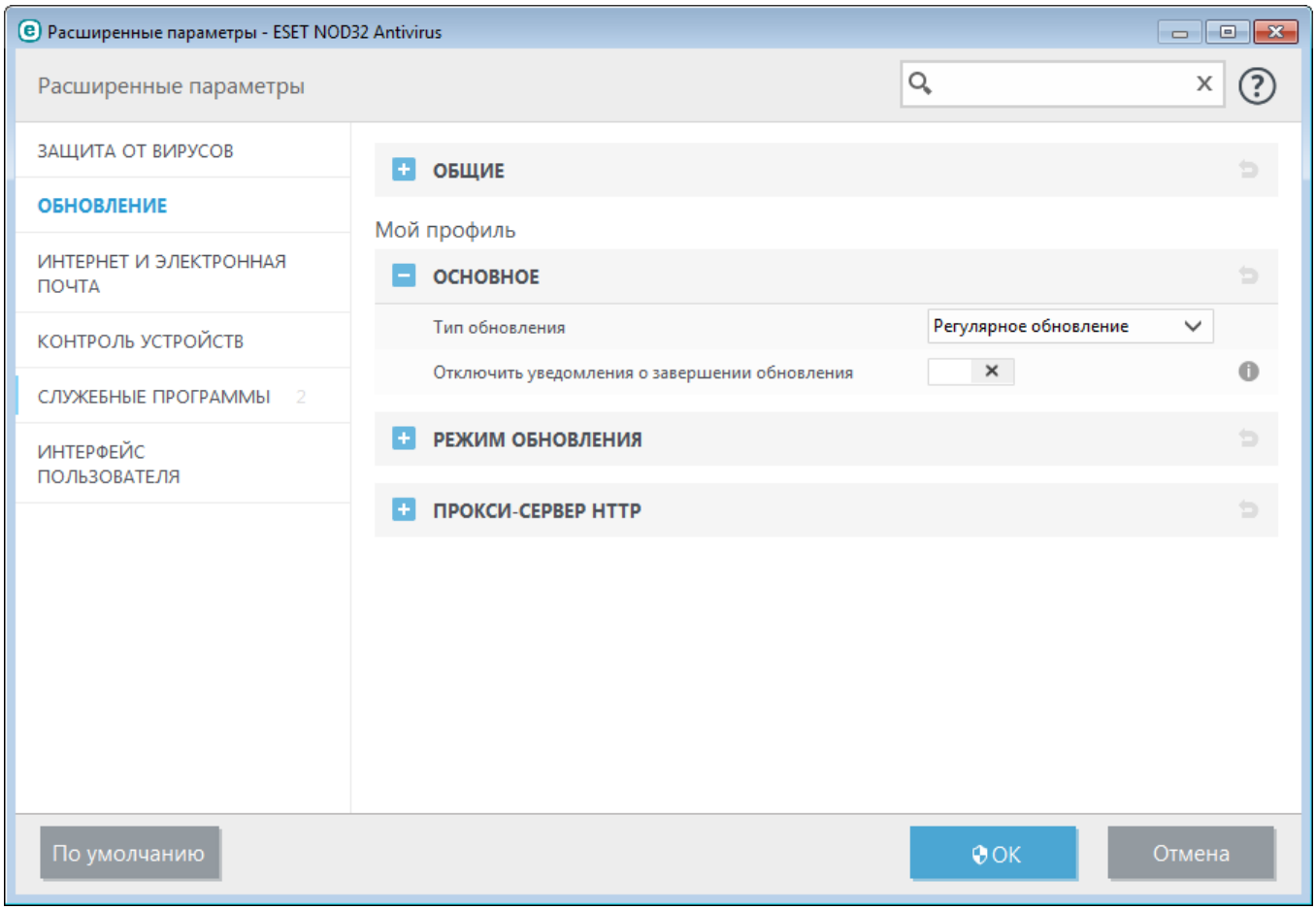
Если во время загрузки обновлений базы данных сигнатур вирусов возникли проблемы, щелкните **Очистить**, чтобы удалить временные файлы обновлений (очистить кэш).

Откат

Если вы подозреваете, что последнее обновление базы данных сигнатур вирусов и (или) модулей программы повреждено либо работает нестабильно, можно выполнить откат к предыдущей версии и отключить обновления на установленный период времени. Или можно включить ранее отключенные обновления, если они отложены на неопределенный период времени.

ESET NOD32 Antivirus создает снимки базы данных сигнатур вирусов и модулей программы для использования с функцией *отката*. Чтобы создавались снимки базы данных сигнатур вирусов, оставьте флажок **Создать снимки файлов обновлений установленным**. В поле **Количество снимков, хранящихся локально** указывается количество хранящихся снимков предыдущих состояний базы данных сигнатур вирусов.

После нажатия кнопки **Откат** (**Дополнительные настройки** (F5) > **Обновление** > **Общие**) нужно выбрать в раскрывающемся списке период времени, на который будет приостановлено обновление базы данных сигнатур вирусов и модулей программы.



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

Основное

По умолчанию для параметра **Тип обновлений** задано значение **Регулярное обновление**. Это означает, что файлы обновлений будут автоматически загружаться с сервера ESET с минимальным расходом трафика. Тестовые обновления (параметр **Тестовое обновление**) — это обновления, которые уже прошли полное внутреннее тестирование и в ближайшее время будут доступны всем пользователям. Преимущество их использования заключается в том, что у вас появляется доступ к новейшим методам обнаружения и исправлениям. Однако такие обновления иногда могут быть недостаточно стабильны и НЕ ДОЛЖНЫ использоваться на производственных серверах и рабочих станциях, где необходимы максимальные работоспособность и стабильность.

Отключить уведомления о завершении обновления: отключает уведомления на панели задач, отображаемые в правом нижнем углу экрана. Этот параметр удобно использовать, если какое-либо приложение или игра работает в полноэкранном режиме. Обратите внимание, что в режиме презентаций все уведомления отключены.

4.3.1.1 Профили обновления

Профили обновления можно создавать для различных конфигураций и задач обновления. Создание профилей обновления особенно полезно для пользователей мобильных устройств, которым необходимо создать вспомогательный профиль для регулярно меняющихся свойств подключения к Интернету.

В раскрывающемся меню **Выбранный профиль** отображается текущий профиль. По умолчанию это **Мой профиль**. Для создания нового профиля щелкните **Профили...**, затем **Добавить...** и введите нужное **имя профиля**. При создании нового профиля можно скопировать параметры из уже существующего профиля, выбрав его в раскрывающемся меню **Копировать настройки профиля**.

4.3.1.2 Дополнительные настройки обновления

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

4.3.1.2.1 Режим обновления

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

При обновлении компонентов программы активируются новые функции или вносятся изменения в уже существующие. После установки обновлений компонентов программы может потребоваться перезагрузка компьютера.

Обновление приложения: когда этот параметр включен, обновление каждого из компонентов программы будет выполняться автоматически, без запросов и уведомлений.

Если установлен флажок **Запрашивать подтверждение перед загрузкой обновления**, при появлении нового обновления будет отображаться уведомление.

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

4.3.1.2.2 Прокси-сервер HTTP

Для доступа к параметрам настройки прокси-сервера для конкретного профиля обновлений щелкните элемент **Обновление** в дереве **Дополнительные настройки** (F5), а затем **Прокси-сервер HTTP**. Выберите в раскрывающемся списке **Режим прокси-сервера** один из трех перечисленных ниже вариантов.

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

Если выбрать вариант **Использовать общие параметры прокси-сервера**, будут использоваться параметры конфигурации прокси-сервера, уже заданные в разделе **Служебные программы** > **Прокси-сервер** дерева расширенных параметров.

Выберите вариант **Не использовать прокси-сервер**, чтобы указать, что прокси-сервер не будет использоваться для обновления ESET NOD32 Antivirus.

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

- Для обновления ESET NOD32 Antivirus должен использоваться прокси-сервер, отличный от указанного в глобальных параметрах (**Служебные программы** > **Прокси-сервер**). В этом случае нужно указать параметры: **Прокси-сервер** (адрес прокси-сервера), **Порт** связи (по умолчанию 3128), а также **Имя пользователя** и **Пароль** для прокси-сервера (если они требуются).
- Не были заданы общие параметры прокси-сервера, однако ESET NOD32 Antivirus будет подключаться к прокси-серверу для получения обновлений.
- Компьютер подключается к Интернету через прокси-сервер. Параметры берутся из Internet Explorer в

процессе установки программы, но при их изменении впоследствии (например, при смене поставщика услуг Интернета) нужно убедиться в том, что указанные в этом окне параметры прокси HTTP верны. Если этого не сделать, программа не сможет подключаться к серверам обновлений.

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

ПРИМЕЧАНИЕ. Данные для аутентификации, такие как **имя пользователя** и **пароль**, предназначены для доступа к прокси-серверу. Заполнять эти поля необходимо только в том случае, если требуются имя пользователя и пароль. Обратите внимание, что эти поля не имеют отношения к имени пользователя и паролю для программы ESET NOD32 Antivirus и должны быть заполнены только в том случае, если подключение к Интернету осуществляется через защищенный паролем прокси-сервер.

4.3.1.2.3 Подключаться к локальной сети как

При обновлении с локального сервера под управлением ОС Windows NT по умолчанию требуется аутентификация всех сетевых подключений.

Чтобы настроить такую учетную запись, выберите в раскрывающемся списке **Тип локального пользователя** один из указанных ниже вариантов:

- **Системная учетная запись (по умолчанию)**;
- **Текущий пользователь**;
- **Указанный пользователь**.

Выберите вариант **Учетная запись системы (по умолчанию)**, чтобы использовать для аутентификации учетную запись системы. Если данные аутентификации в главном разделе параметров обновлений не указаны, как правило, процесса аутентификации не происходит.

Для того чтобы программа использовала для аутентификации учетную запись, под которой в данный момент выполнен вход в систему, выберите вариант **Текущий пользователь**. Недостаток этого варианта заключается в том, что программа не может подключиться к серверу обновлений, если в данный момент ни один пользователь не выполнил вход в систему.

Выберите **Указанный пользователь**, если нужно указать учетную запись пользователя для аутентификации. Этот метод следует использовать в тех случаях, когда невозможно установить соединение с помощью учетной записи системы. Обратите внимание на то, что указанная учетная запись должна обладать правами на доступ к каталогу на локальном сервере, в котором хранятся файлы обновлений. В противном случае программа не сможет установить соединение и загрузить обновления.

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

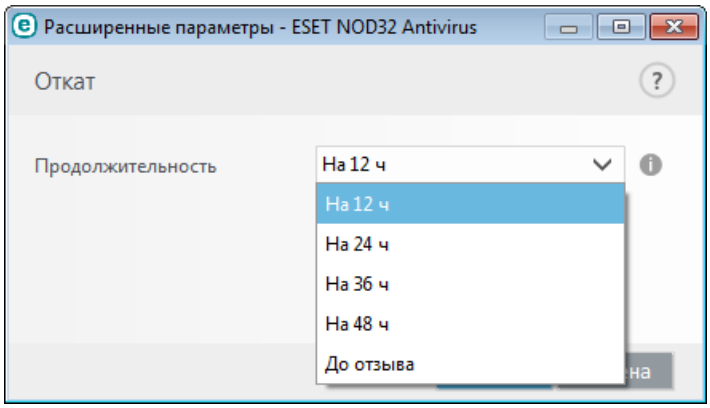
Выберите параметр **Отключиться от сервера после завершения обновления** для принудительного отключения, если подключение к серверу остается активным после загрузки обновлений.

4.3.2 Откат обновления

Если вы подозреваете, что последнее обновление базы данных сигнатур вирусов и/или модулей программы нестабильно или повреждено, вы можете выполнить откат к предыдущей версии и отключить обновления на установленный период времени. Или можно включить ранее отключенные обновления, если они отложены на неопределенный период времени.

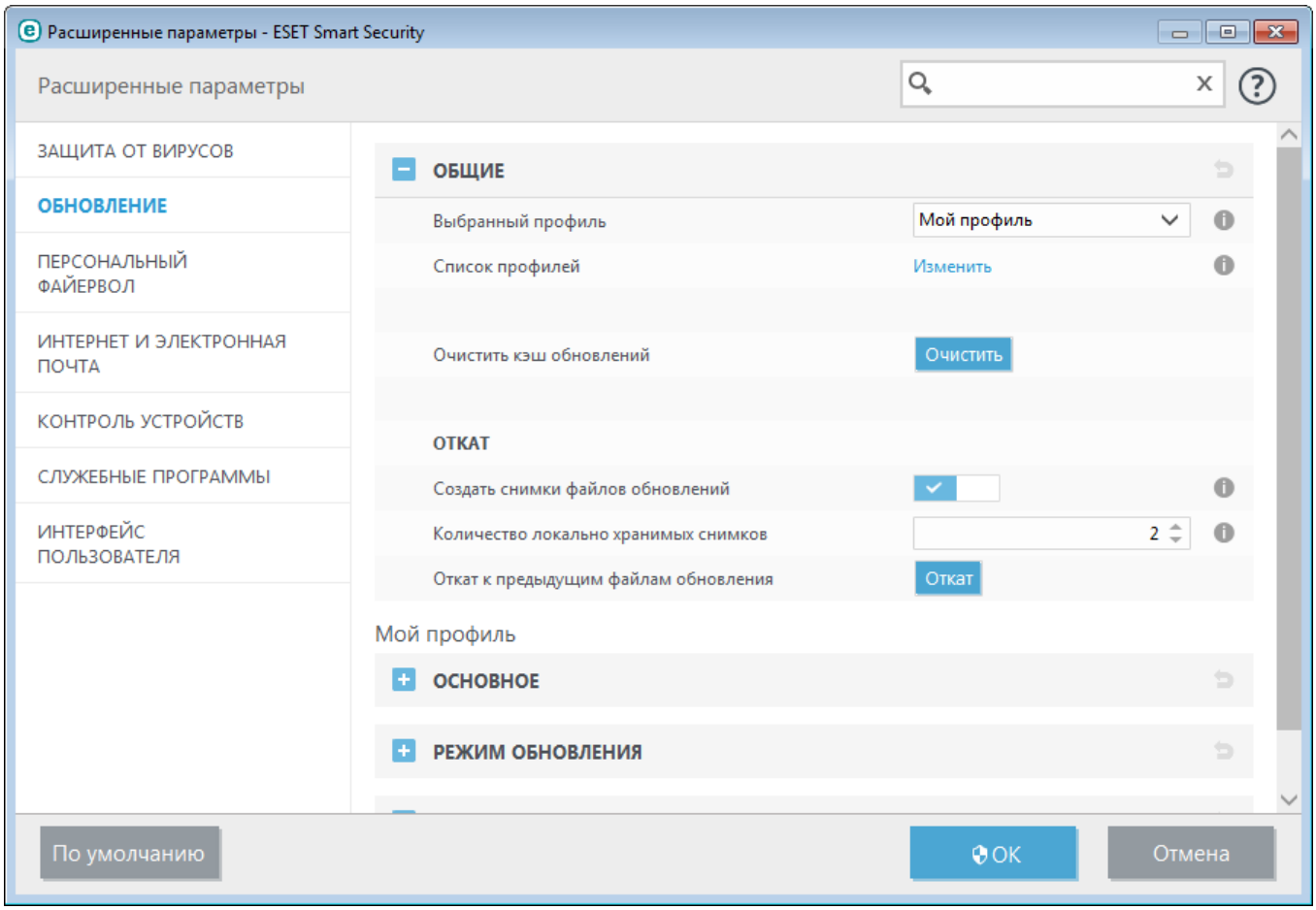
ESET NOD32 Antivirus делает снимки базы данных сигнатур вирусов и модулей программы для использования с функцией *отката*. Чтобы создать снимки базы данных вирусов, установите флажок **Создать снимки файлов обновлений**. В поле **Количество снимков, хранящихся локально** указывается количество хранящихся снимков предыдущих баз данных сигнатур вирусов.

После выбора **Откат** (**Дополнительные настройки** (F5) > **Обновление** > **Дополнительно**) в раскрывающемся меню **Приостановить обновления** выберите промежуток времени, на который будет приостановлено обновление базы данных сигнатур вирусов и модулей программы.



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

После отката кнопка **Откат** заменяется на **Разрешить обновления**. На протяжении периода времени, выбранного в раскрывающемся меню **Приостановить обновления**, обновления не производятся. Программа возвращается к самой старой версии базы данных сигнатур вирусов, которая хранится в качестве снимка в файловой системе локального компьютера.



Пример. Предположим, последней версии базы данных сигнатур вирусов присвоен номер 6871. Версии 6870 и 6868 хранятся в качестве снимков. Обратите внимание, что версия 6869 недоступна, поскольку, например, компьютер был выключен и более новая версия обновления стала доступна до того, как была загружена версия 6869. Если в поле **Количество снимков, хранящихся локально** установить значение 2 и нажать кнопку **Откат**, программа вернется к версии 6868 базы данных сигнатур вирусов (включая модули программы). Это может занять некоторое время. Чтобы проверить, произведен ли откат к предыдущей версии, в главном окне ESET NOD32 Antivirus откройте раздел Обновление.

4.3.3 Создание задач обновления

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

Обновления также можно выполнять как запланированную задачу. Для конфигурирования запланированной задачи перейдите в раздел **Служебные программы** > **Планировщик**. По умолчанию в ESET NOD32 Antivirus активированы указанные ниже задачи.

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

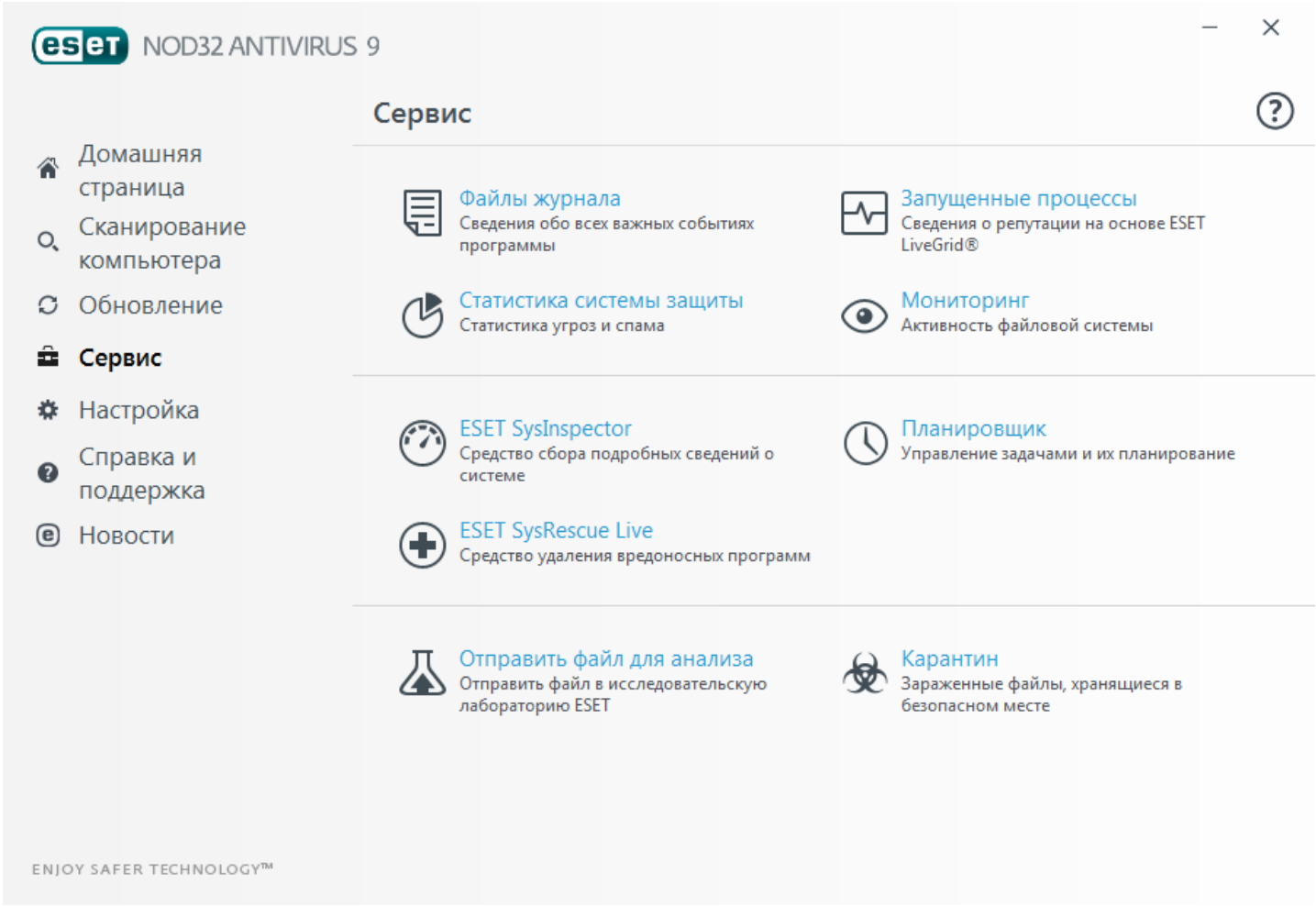
Каждую задачу обновления можно изменить в соответствии с конкретными требованиями. Кроме задач по умолчанию можно создать другие задачи обновления с пользовательскими настройками. Дополнительную информацию о создании и настройке задач обновления см. в разделе Планировщик.

4.4 Служебные программы

В меню **Сервис** перечислены модули, которые позволяют упростить процесс администрирования программы, и также содержит дополнительные возможности администрирования для опытных пользователей.

4.4.1 Служебные программы в ESET NOD32 Antivirus

День **Служебные программы** : в этом меню представлены модули, которые помогают упростить процесс администрирования программы, а также содержатся дополнительные возможности администрирования для опытных пользователей.



В этом меню представлены следующие служебные программы.

 Файлы журналов

 Статистика защиты

 Наблюдение

 Запущенные процессы (если модульThreatSense включен в программе ESET NOD32 Antivirus)

 ESET SysInspector

 ESET SysRescue Live: перенаправляет на страницу ESET SysRescue Live, с которой можно загрузить образ ESET SysRescue Live или Live CD/USB Creator для операционной системы Microsoft Windows.

 Планировщик

 Отправка образца на анализ: возможность отправить подозрительный файл на анализ в исследовательскую лабораторию ESET. Диалоговое окно, открывающееся при использовании этой функции, описано в данном разделе.

 Карантин

ПРИМЕЧАНИЕ. Компонент ESET SysRescue может быть недоступен для ОС Windows 8 в более ранних версиях продуктов ESET. В таком случае рекомендуется обновить соответствующий продукт или создать диск ESET SysRescue в другой версии Microsoft Windows.

4.4.1.1 Файлы журнала

Файлы журнала содержат информацию о важных программных событиях и предоставляют сводные сведения об обнаруженных угрозах. Ведение журнала является важнейшим элементом анализа системы, обнаружения угроз и устранения проблем. Оно выполняется в фоновом режиме без вмешательства пользователя. Данные сохраняются в соответствии с текущими параметрами степени детализации журнала. Просматривать текстовые сообщения и файлы журнала, а также архивировать их можно непосредственно в среде ESET NOD32 Antivirus.

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

- **Обнаруженные угрозы**: журнал угроз содержит подробную информацию о заражениях, обнаруженных программой ESET NOD32 Antivirus. В журнале сохраняется информация о времени обнаружения, названии угрозы, месте обнаружения, выполненных действиях и имени пользователя, который находился в системе при обнаружении заражения. Дважды щелкните запись журнала для просмотра подробного содержимого в отдельном окне.
- **События**: в журнале событий регистрируются все важные действия, выполняемые программой ESET NOD32 Antivirus. Он содержит информацию о событиях и ошибках, которые произошли во время работы программы. Он должен помогать системным администраторам и пользователям решать проблемы. Зачастую информация, которая содержится в этом журнале, оказывается весьма полезной при решении проблем, возникающих в работе программы.
- **Сканирование компьютера**: в этом окне отображаются результаты всех выполненных вручную или запланированных операций сканирования. Каждая строка соответствует одной проверке компьютера. Чтобы получить подробную информацию о той или иной операции сканирования, дважды щелкните соответствующую запись.
- **HIPS**: здесь содержатся записи о конкретных правилах системы предотвращения вторжений на узел, которые помечены для регистрации. Протокол показывает приложение, которое вызвало операцию, результат (разрешение или запрещение правила) и имя созданного правила.
- **Отфильтрованные веб-сайты**: этот список используется для просмотра списка веб-сайтов, заблокированных при помощи защиты доступа в Интернет. В этих журналах отображается время, URL-адрес, пользователь и

приложение, с помощью которого установлено подключение к конкретному веб-сайту.

- **Контроль устройств**: содержит список подключенных к компьютеру съемных носителей и устройств. В журнале регистрируются только те устройства, которые соответствуют правилу контроля. В противном случае в журнале не создаются записи о них. Также здесь отображаются такие сведения, как тип устройства, серийный номер, имя поставщика и размер носителя (при его наличии).

Чтобы скопировать в буфер обмена информацию из любого раздела журнала, выделите нужную запись и нажмите сочетание клавиш **Ctrl+C**. Для выделения нескольких записей можно использовать клавиши **Ctrl** и **Shift**.

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

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

- **Показать**: просмотр в новом окне более подробной информации о выбранном журнале.
- **Фильтрация одинаковых записей**: после активации этого фильтра будут показаны только записи одного типа (диагностика, предупреждения и т. д.).
- **Фильтровать.../Найти...**: при выборе этого параметра на экран выводится окно Поиск в журнале, в котором можно задать критерии фильтрации для определенных записей журнала.
- **Включить фильтр**: активация настроек фильтра.
- **Отключить фильтр**: удаляются все параметры фильтра (созданные, как описано выше).
- **Копировать/копировать все**: копируется информация обо всех записях в окне.
- **Удалить/Удалить все**: удаляются выделенные записи или все записи в окне; для этого действия нужны права администратора.
- **Экспорт...**: экспорт информации о записях в файл формата XML.
- **Экспортировать все...**: экспорт информации о всех записях в файл формата XML.
- **Прокрутить журнал**: установите этот флажок, чтобы выполнялась автоматическая прокрутка старых журналов, а на экран в окне **Файлы журнала** выводились активные журналы.

4.4.1.1.1 Файлы журналов

Настройку ведения журнала ESET NOD32 Antivirus можно открыть из главного окна программы. Нажмите **Настройка** > **Перейти к дополнительным настройкам...** > **Служебные программы** > **Файлы журнала**. Этот раздел используется для настройки управления журналами. Программа автоматически удаляет старые файлы журналов, чтобы сэкономить дисковое пространство. Для файлов журнала можно задать параметры, указанные ниже.

Минимальная степень детализации журнала: определяет минимальный уровень детализации записей о событиях.

- **Диагностика**: регистрируется информация, необходимая для тщательной настройки программы, а также все перечисленные выше записи.
- **Информационные**: записываются информационные сообщения, в том числе сообщения об успешном выполнении обновления, а также все перечисленные выше записи.
- **Предупреждения**: записывается информация обо всех критических ошибках и предупреждениях.
- **Ошибки**: регистрируется информация об *ошибках загрузки файлов* и критических ошибках.
- **Критические**: регистрируются только критические ошибки (ошибки запуска защиты от вирусови т. п.).

Записи в журнале, созданные раньше, чем указано в поле **Автоматически удалять записи старше, чем X дн.**, будут автоматически удаляться.

Оптимизировать файлы журналов автоматически: если этот флажок установлен, файлы журналов будут автоматически дефрагментироваться в тех случаях, когда процент фрагментации превышает значение, указанное в параметре **Если количество неиспользуемых записей превышает (%)**.

Нажмите кнопку **Оптимизировать**, чтобы начать дефрагментацию файлов журналов. При этом удаляются все пустые записи журналов, что улучшает производительность и скорость обработки журналов. Такое улучшение особенно заметно, если в журналах содержится большое количество записей.

Выберите Включить текстовый протокол, чтобы разрешить хранение журналов в другом формате отдельно от файлов журналов.

- **Целевой каталог**: каталог, в котором будут храниться файлы журналов (только для текстового формата и формата CSV). Каждый раздел журнала сохраняется в отдельный файл с предварительно заданным именем (например, в файл *virlog.txt* записывается раздел **Обнаруженные угрозы** файла журнала, если для хранения файлов журнала вами выбран формат обычного текста).
- **Тип**: если выбрать формат **Текст**, журналы будут сохраняться в текстовый файл с символами табуляции в качестве разделителей данных. То же касается формата **CSV**. Если выбрать установку **Событие**, журналы будут сохраняться не в файл, а в журнал событий Windows (его можно просмотреть на панели управления в средстве просмотра событий).

Удалить все файлы журнала: будут удалены все сохраненные журналы, выбранные в раскрывающемся списке **Тип**. После удаления журналов появится уведомление о завершении процесса удаления.

ПРИМЕЧАНИЕ. Для ускорения разрешения проблем специалисты ESET иногда могут запрашивать у пользователей журналы с их компьютеров. ESET Log Collector облегчает сбор необходимой информации. Дополнительные сведения об ESET Log Collector см. в статье базы знаний ESET.

4.4.1.1.2 Защита доступа к сети Microsoft

Защита доступа к сети — это технология Microsoft, предназначенная для контроля доступа компьютера к сети на основе работоспособности системы узла. Используя эту технологию, системные администраторы компьютерной сети организации могут формировать политики в соответствии с требованиями работоспособности системы.

Защита доступа к сети позволяет администраторам поддерживать работоспособность компьютеров сети, что в свою очередь помогает сохранять целостность сети. Она не предназначена для защиты сети от злонамеренных действий пользователей. Например, если программное обеспечение и конфигурация компьютера отвечают политике доступа к сети, компьютер считается работоспособным или совместимым, и ему будет предоставлен соответствующий доступ в сеть. Защита доступа к сети не предотвращает действия по загрузке в сеть вредоносных программ неавторизованным пользователем с совместимым компьютером или другое неприемлемое поведение.

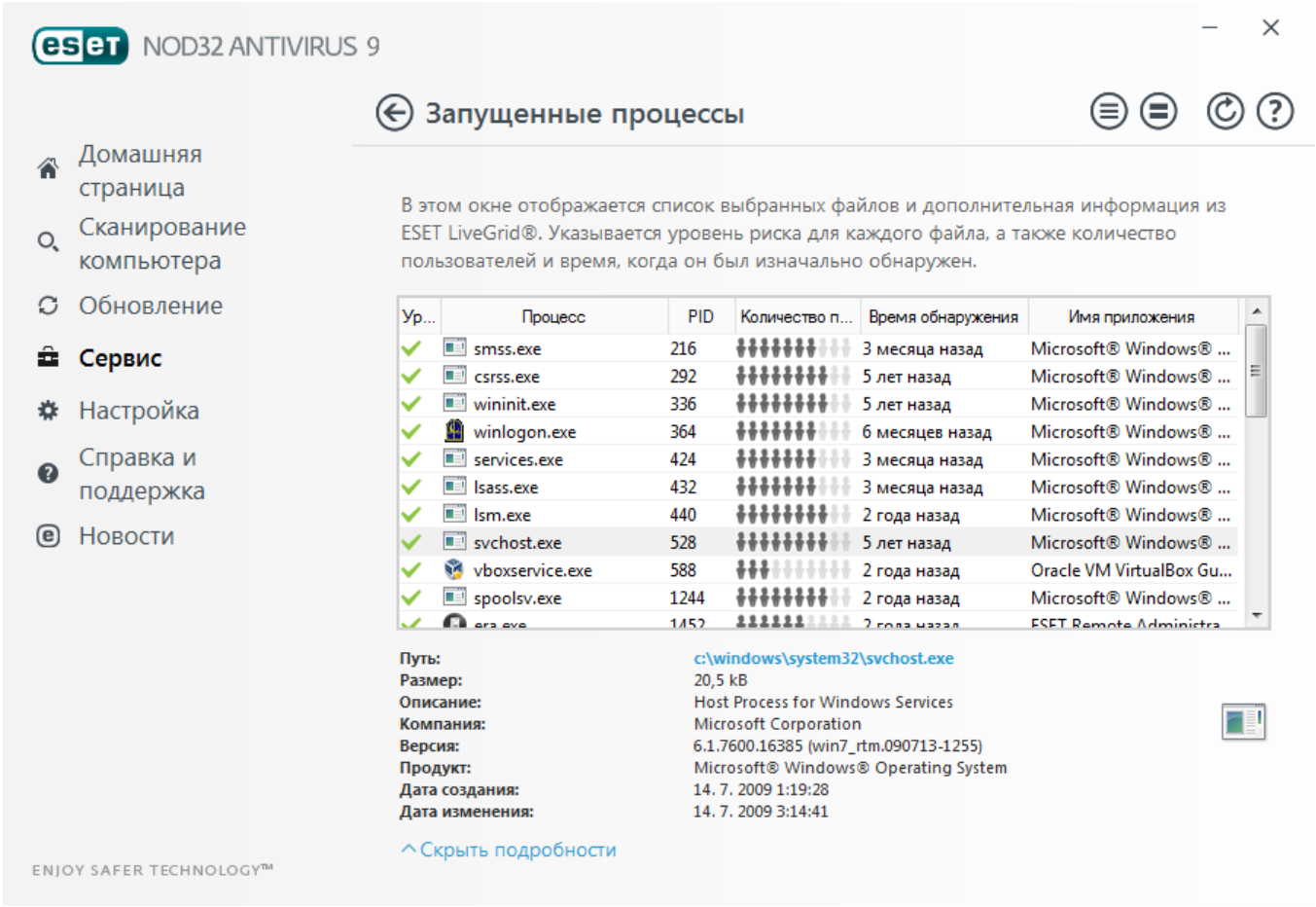
Защита доступа к сети позволяет администраторам создавать и применять политики работоспособности для компьютеров, подключенных к корпоративной сети. Политики определяют требования как к компонентам установленного программного обеспечения, так и к конфигурациям системы. Подсоединенные к сети компьютеры, такие как ноутбуки, рабочие станции и другие устройства, оцениваются в соответствии со сконфигурированными требованиями к работоспособности.

Требования к работоспособности включают:

• включенный файервол;
• наличие антивирусной программы;
• актуальная версия антивирусной программы;
• автоматическое обновление Windows должно быть включено и т. д.

4.4.1.2 Запущенные процессы

В разделе «Запущенные процессы» отображаются выполняемые на компьютере программы или процессы. Кроме того, он позволяет оперативно и непрерывно уведомлять компанию ESET о новых заражениях. ESET NOD32 Antivirus предоставляет подробные сведения о запущенных процессах для защиты пользователей с помощью технологии ThreatSense.



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

Уровень риска: в большинстве случаев ESET NOD32 Antivirus и технология ThreatSense присваивают объектам (файлам, процессам, разделам реестра и т. п.) уровни риска на основе наборов эвристических правил, которые изучают характеристики каждого объекта и затем оценивают вероятность их вредоносной деятельности. На основе такого эвристического анализа объектам присваивается уровень риска от 1 — безопасно (зеленый) до 9 — опасно (красный).

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

Количество пользователей: количество пользователей данного приложения. Эта информация собирается технологией ThreatSense.

Время обнаружения: время, прошедшее с момента обнаружения приложения технологией ThreatSense.

ПРИМЕЧАНИЕ.Если для приложения выбран уровень безопасности неизвестно (оранжевый), оно не обязательно является вредоносной программой. Обычно это просто новое приложение. Если вы не уверены в безопасности файла, его можно отправить на анализ в исследовательскую лабораторию ESET. Если файл окажется вредоносным приложением, необходимая для его обнаружения информация будет включена в последующие обновления.

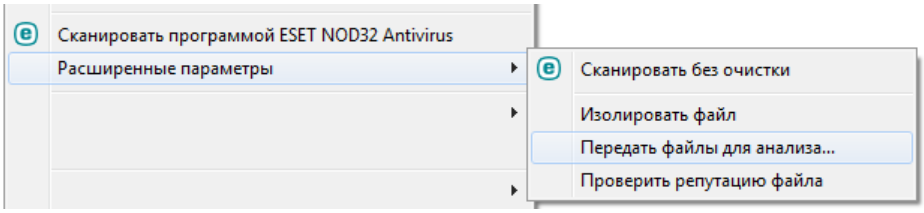
Имя приложения: конкретное имя программы или процесса.

Открыть новое окно: сведения о запущенных процессах будут открыты в новом окне.

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

- **Файл**: расположение приложения на компьютере.
- **Размер файла**: размер файла в байтах (Б).
- **Описание файла**: характеристики файла на основе его описания в операционной системе.
- **Название компании**: название поставщика или процесса приложения.
- **Версия файла**: информация, предоставленная издателем приложения.
- **Имя продукта**: имя приложения и/или наименование компании.

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



4.4.1.3 Статистика защиты

Для просмотра диаграммы статистических данных, связанных с модулями защиты ESET NOD32 Antivirus, нажмите **Служебные программы** > **Статистика защиты**. Выберите интересующий вас модуль защиты в раскрывающемся меню **Статистика**, в результате чего на экран будет выведена соответствующая диаграмма и легенда. Если навести указатель мыши на элемент в легенде, на диаграмме отобразятся данные только для этого элемента.

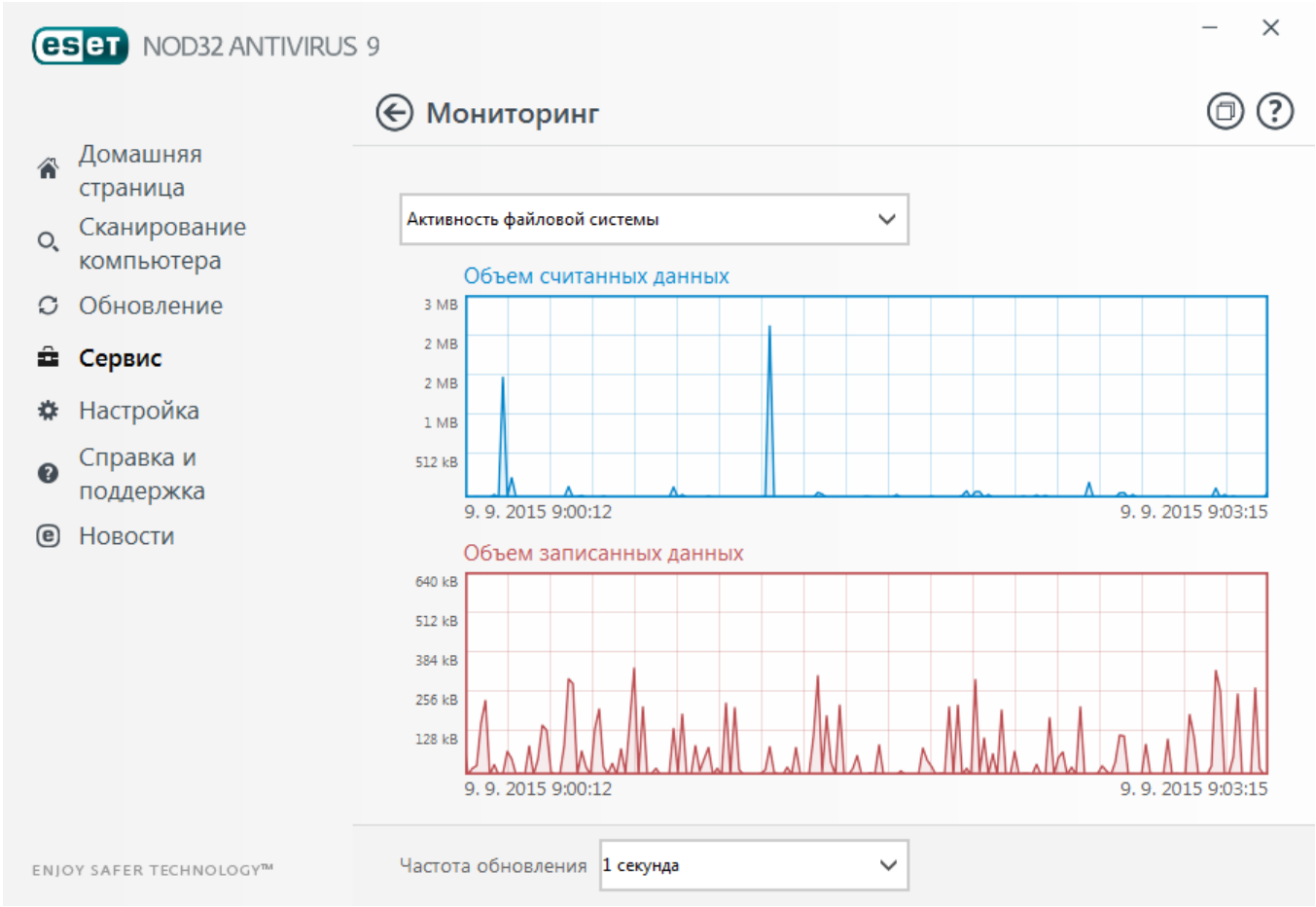
Доступны следующие статистические диаграммы.

- **Защита от вирусов и шпионских программ**: отображение количества зараженных и очищенных объектов.
- **Защита файловой системы**: отображение только объектов, считанных из файловой системы и записанных в нее.
- **Защита почтового клиента**: отображение только объектов, отправленных или полученных почтовыми клиентами.
- **Защита доступа в Интернет и защита от фишинга**: отображение только объектов, загруженных веб-браузерами.

Под статистическими диаграммами показано общее количество просканированных объектов, последний просканированный объект и метка времени статистики. Нажмите **Сброс**, чтобы удалить всю статистическую информацию.

4.4.1.4 Наблюдение

Чтобы просмотреть текущую **активность файловой системы** в виде графика, щелкните **Служебные программы** > **Наблюдение**. В нижней части диаграммы находится временная шкала, на которой отображается активность файловой системы в режиме реального времени за выбранный временной интервал. Чтобы изменить временной интервал, выберите необходимое значение в раскрывающемся меню **Частота обновления**.



Доступны указанные ниже варианты.

- **Шаг: 1 секунда**: график обновляется каждую секунду, временная шкала охватывает последние 10 минут.
- **Шаг: 1 минута (последние 24 часа)**: график обновляется каждую минуту, временная шкала охватывает последние 24 часа.
- **Шаг: 1 час (последний месяц)**: график обновляется каждый час, временная шкала охватывает последний месяц.
- **Шаг: 1 час (выбранный месяц)**: график обновляется каждый час, временная шкала охватывает последние выбранные месяцы в количестве X.

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

4.4.1.5 ESET SysInspector

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

В окне SysInspector отображаются такие данные о созданных журналах.

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

Доступны перечисленные далее действия.

- **Открыть**: открытие созданного журнала. Вы также можете щелкнуть файл журнала правой кнопкой мыши и выбрать в контекстном меню пункт **Показать**.
- **Сравнить**: сравнение двух существующих журналов.
- **Создать...**: создание журнала. Прежде чем открывать журнал, подождите, пока программа ESET SysInspector завершит работу (отобразится состояние журнала «Создано»).
- **Удалить**: удаление выделенных журналов из списка.

Если выбран один или несколько файлов журнала, в контекстном меню доступны следующие элементы.

- **Показать**: открытие выделенного журнала в ESET SysInspector (аналогично двойному щелчку).
- **Сравнить**: сравнение двух существующих журналов.
- **Создать...**: создание журнала. Прежде чем открывать журнал, подождите, пока программа ESET SysInspector завершит работу (отобразится состояние журнала «Создано»).
- **Удалить все**: удаление всех журналов.
- **Экспорт...**: экспорт журнала в файл или архив в формате *XML*.

4.4.1.6 Планировщик

Планировщик управляет запланированными задачами и запускает их с предварительно заданными параметрами и свойствами.

Перейти к планировщику можно из главного окна программы ESET NOD32 Antivirus, открыв раздел меню **Служебные программы** > **Планировщик**. **Планировщик** содержит полный список всех запланированных задач и свойства конфигурации, такие как предварительно заданные дата, время и используемый профиль сканирования.

Планировщик предназначен для планирования выполнения следующих задач: обновление базы данных сигнатур вирусов, сканирование, проверка файлов, исполняемых при запуске системы, и обслуживание журнала. Добавлять и удалять задачи можно непосредственно в главном окне планировщика (кнопки **Добавить...** и **Удалить** в нижней части окна). С помощью контекстного меню окна планировщика можно выполнить следующие действия: отображение подробной информации, выполнение задачи немедленно, добавление новой задачи и удаление существующей задачи. Используйте флажки в начале каждой записи, чтобы активировать или отключить соответствующие задачи.

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

- **Обслуживание журнала**
- **Регулярное автоматическое обновление**
- **Автоматическое обновление после установки модемного соединения**
- **Автоматическое обновление после входа пользователя в систему**
- **Регулярная проверка последней версии программы** (см. раздел Режим обновления)
- **Автоматическая проверка файлов при запуске системы** (после входа пользователя в систему)
- **Автоматическая проверка файлов при запуске системы** (после успешного обновления базы данных сигнатур вирусов)
- **Автоматическое первое сканирование**

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

Добавление новой задачи

1. Щелкните **Добавить задачу** в нижней части окна.
2. Введите имя задачи.
3. Выберите нужную задачу в раскрывающемся меню.

- **Запуск внешнего приложения**: планирование исполнения внешнего приложения.
- **Обслуживание журнала**: в файлах журнала также содержатся остатки удаленных записей. Эта задача регулярно оптимизирует записи в файлах журнала для эффективной работы.
- **Проверка файлов при загрузке системы**: проверка файлов, исполнение которых разрешено при запуске или входе пользователя в систему.
- **Создать сканирование компьютера**: создание снимка состояния компьютера в ESET SysInspector. При этом собираются подробные сведения о компонентах системы (например, драйверах, приложениях) и оценивается уровень риска для каждого их них.
- **Сканирование компьютера по требованию**: сканирование файлов и папок на компьютере.
- **Первое сканирование**: по умолчанию через 20 минут после установки или перезагрузки выполняется сканирование компьютера как задание с низким приоритетом.
- **Обновление**: планирование задачи обновления, в рамках которой обновляется база данных сигнатур вирусов и программные модули.

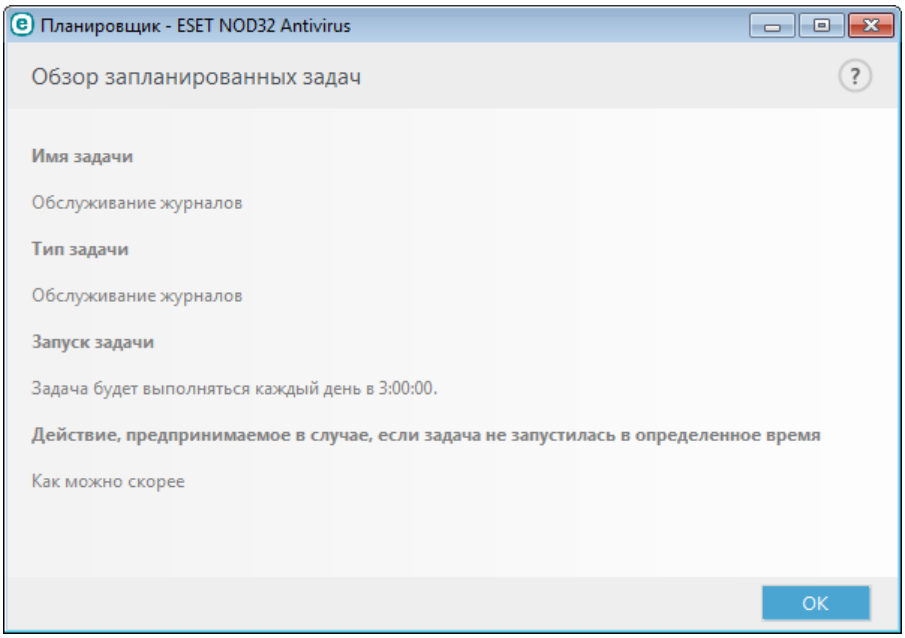
4. Чтобы активировать задачу, установите переключатель в положение **Включено** (это можно сделать позже, установив/сняв флажок в списке запланированных задач), нажмите кнопку **Далее** и выберите один из режимов времени выполнения:

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

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

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

Можно просмотреть запланированную задачу, щелкнув правой кнопкой мыши и выбрав **Показать информацию о задаче**.



4.4.1.7 ESET SysRescue

ESET SysRescue — это утилита для создания загрузочного диска, содержащего одно из решений ESET Security: ESET NOD32 Antivirus, ESET Smart Security или какой-либо серверный продукт. Главным преимуществом ESET SysRescue является то, что решение ESET Security работает независимо от операционной системы компьютера, имея непосредственный доступ к жесткому диску и файловой системе. Это позволяет удалять такие заражения, которые в обычной ситуации (например, при запущенной операционной системе и т. п.) удалить невозможно.

4.4.1.8 ESET LiveGrid®

ESET LiveGrid® (основанная на передовой системе своевременного обнаружения ESET ThreatSense.Net) использует данные от пользователей ESET со всего мира и отправляет их в вирусную лабораторию ESET. Сеть ESET LiveGrid® позволяет получать подозрительные образцы и метаданные из реальных условий, поэтому мы можем незамедлительно реагировать на потребности пользователей и обеспечить готовность ESET к обезвреживанию новейших угроз. Дополнительную информацию о ESET LiveGrid® см. в глоссарии.

Пользователь может проверять репутацию запущенных процессов и файлов непосредственно в интерфейсе программы или в контекстном меню, благодаря чему становится доступна дополнительная информация из ESET LiveGrid®. Существует два варианта работы.

1. Можно принять решение не включать ESET LiveGrid®. Функциональность программного обеспечения при этом не ограничивается, но в некоторых случаях система ESET NOD32 Antivirus может быстрее обрабатывать новые угрозы, чем обновление базы данных сигнатур вирусов.
2. Можно сконфигурировать ESET LiveGrid® так, чтобы отправлялась анонимная информация о новых угрозах и файлах, содержащих неизвестный пока опасный код. Файл может быть отправлен в ESET для тщательного анализа. Изучение этих угроз поможет компании ESET обновить средства обнаружения угроз.

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

По умолчанию программа ESET NOD32 Antivirus отправляет подозрительные файлы в вирусную лабораторию ESET для тщательного анализа. Всегда исключаются файлы с определенными расширениями, такими как *.doc* и *.xls*. Также можно добавить другие расширения, если политика вашей организации предписывает исключение из отправки.

Меню настройки ESET LiveGrid®содержит несколько параметров для включения и отключения системы ESET LiveGrid®, предназначенной для отправки подозрительных файлов и анонимной статистической информации в лабораторию ESET. Эти параметры доступны через дерево расширенных параметров в разделе **Служебные программы** > **ESET LiveGrid®**.

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

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

Отправить файлы: компании ESET на анализ отправляются подозрительные файлы, похожие на угрозы, и файлы с необычными характеристиками или поведением.

Установите флажок **Вести журнал**, чтобы создать журнал событий для регистрации фактов отправки файлов и статистической информации. При каждой отправке файлов или статистики в журнал событий будут вноситься записи.

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

Исключение: фильтр исключений дает возможность указать папки и файлы, которые не нужно отправлять на анализ (например, может быть полезно исключить файлы, в которых может присутствовать конфиденциальная информация, такие как документы и электронные таблицы). Перечисленные в этом списке файлы никогда не будут передаваться в ESET на анализ, даже если они содержат подозрительный код. Файлы наиболее распространенных типов (.doc и т. п.) исключаются по умолчанию. При желании можно дополнять список исключенных файлов.

Если система ESET LiveGrid® использовалась ранее, но была отключена, могут существовать пакеты данных, предназначенные для отправки. Эти пакеты будут отправлены в ESET даже после выключения системы. После отправки всей текущей информации новые пакеты создаваться не будут.

4.4.1.8.1 Подозрительные файлы

На вкладке **Файлы** в области расширенных параметров ESET LiveGrid® можно настроить способ отправки сведений об угрозах в исследовательскую лабораторию ESET для анализа.

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

Фильтр исключения: этот вариант позволяет исключить из отправки определенные файлы или папки. Перечисленные в этом списке файлы никогда не будут передаваться в исследовательскую лабораторию ESET для анализа, даже если они содержат подозрительный код. Например, может быть полезно исключить файлы, в которых может присутствовать конфиденциальная информация, такие как документы и электронные таблицы. Файлы наиболее распространенных типов (.doc и т. п.) исключаются по умолчанию. При желании можно дополнять список исключенных файлов.

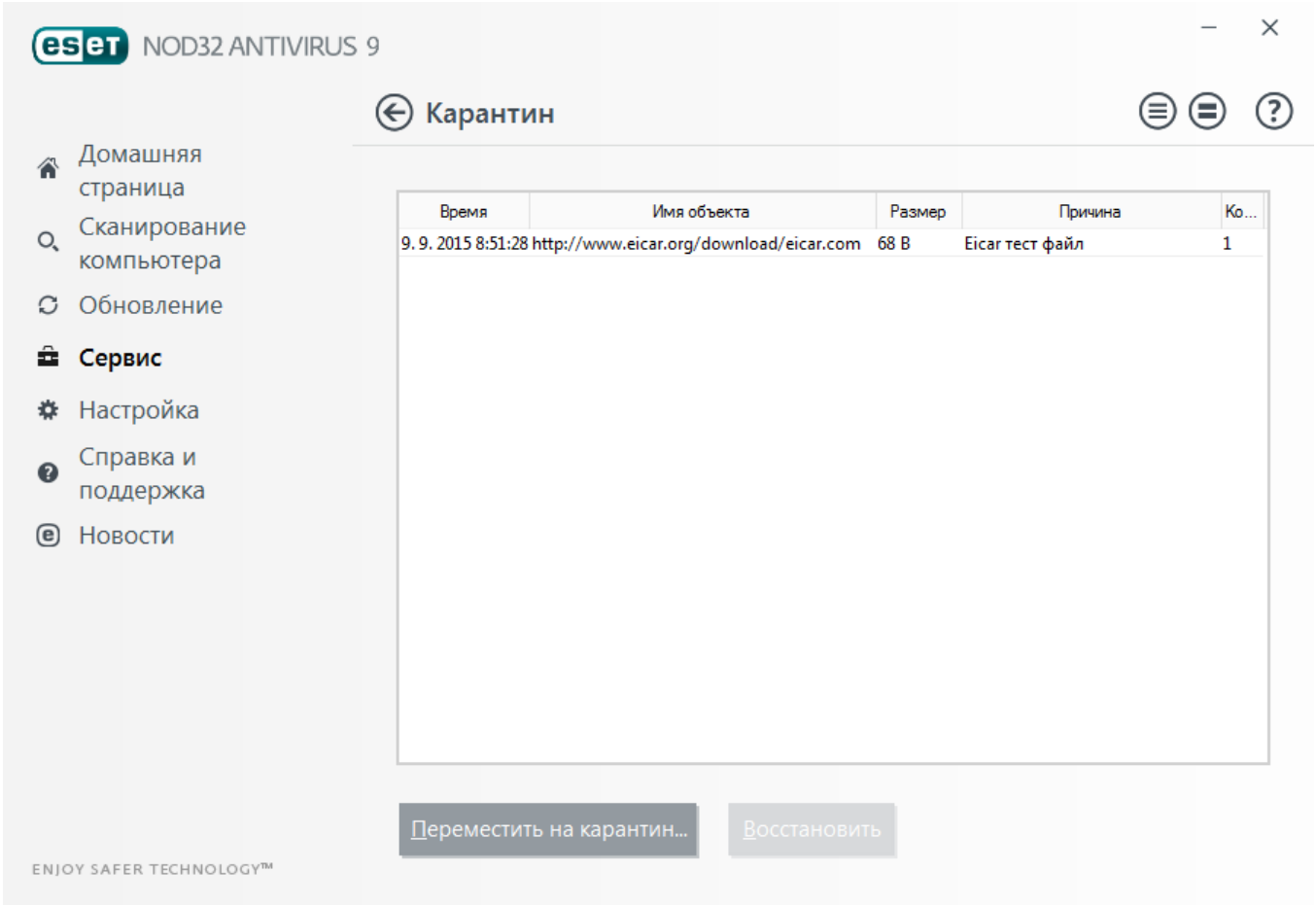
Ваш адрес электронной почты (необязательно): можно отправить адрес электронной почты вместе с подозрительными файлами, чтобы специалисты ESET могли обратиться к вам, если для анализа потребуется дополнительная информация. Имейте в виду, что компания ESET не отправляет ответы пользователям без необходимости.

Установите флажок **Вести журнал**, чтобы создать журнал событий для регистрации фактов отправки файлов и статистической информации. В журнал событий будут вноситься записи при каждой отправке файлов или статистики.

4.4.1.9 Карантин

Карантин предназначен в первую очередь для изоляции и безопасного хранения зараженных файлов. Файлы следует помещать на карантин, если их нельзя вылечить или безопасно удалить либо если они отнесены программой ESET NOD32 Antivirus к зараженным по ошибке.

Поместить на карантин можно любой файл. Рекомендуется помещать на карантин файлы с подозрительной активностью, которые, тем не менее, не обнаруживаются модулем сканирования защиты от вирусов. Файлы на карантине можно отправить в исследовательскую лабораторию ESET на анализ.



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

Помещение файлов на карантин

Программа ESET NOD32 Antivirus автоматически помещает удаленные файлы на карантин (если этот параметр не был отменен пользователем в окне предупреждения). При желании любой подозрительный файл можно поместить на карантин вручную с помощью кнопки **Карантин...**. При этом исходная копия файла не удаляется. Для этого также можно воспользоваться контекстным меню, щелкнув правой кнопкой мыши окно **Карантин** и выбрав пункт **Карантин...**.

Восстановление из карантина

Файлы, находящиеся на карантине, можно восстановить в исходном месте. Для этого предназначена функция **Восстановить**, доступная в контекстном меню определенного файла, отображающегося в окне карантина. Если файл помечен как потенциально нежелательная программа, включается параметр **Восстановить и исключить из сканирования**. Дополнительную информацию об этом типе приложения см. в глоссарии. Контекстное меню содержит также функцию **Восстановить в...**, которая позволяет восстановить файл в месте, отличном от исходного.

ПРИМЕЧАНИЕ: Если программа поместила незараженный файл на карантин по ошибке, исключите этот файл

из сканирования после восстановления и отправьте его в службу поддержки клиентов ESET.

Отправка файла из карантина

Если на карантин помещен файл, который не распознан программой, или файл неверно квалифицирован как зараженный (например, в результате ошибки эвристического метода) и изолирован, передайте файл в вирусную лабораторию ESET. Чтобы отправить файл из карантина, щелкните его правой кнопкой мыши и выберите пункт **Передать на анализ**.

4.4.1.10 Прокси-сервер

В больших локальных сетях подключение компьютеров к Интернету может осуществляться через прокси-сервер. Ориентируясь на эту конфигурацию, нужно задать описанные ниже параметры. Если этого не сделать, программа не сможет обновляться автоматически. В программе ESET NOD32 Antivirus настройку прокси-сервера можно выполнить в двух разных разделах дерева расширенных настроек.

Во-первых, параметры прокси-сервера можно конфигурировать в разделе **Дополнительные настройки**, доступном через **Служебные программы** > **Прокси-сервер**. Настройка прокси-сервера на этом уровне позволяет задать его параметры для программы ESET NOD32 Antivirus в целом. Они используются всеми модулями программы, которым требуется подключение к Интернету.

Для настройки параметров прокси-сервера на этом уровне установите флажок **Использовать прокси-сервер**, а затем введите адрес прокси-сервера в поле **Прокси-сервер** и укажите номер его порта в поле **Порт**.

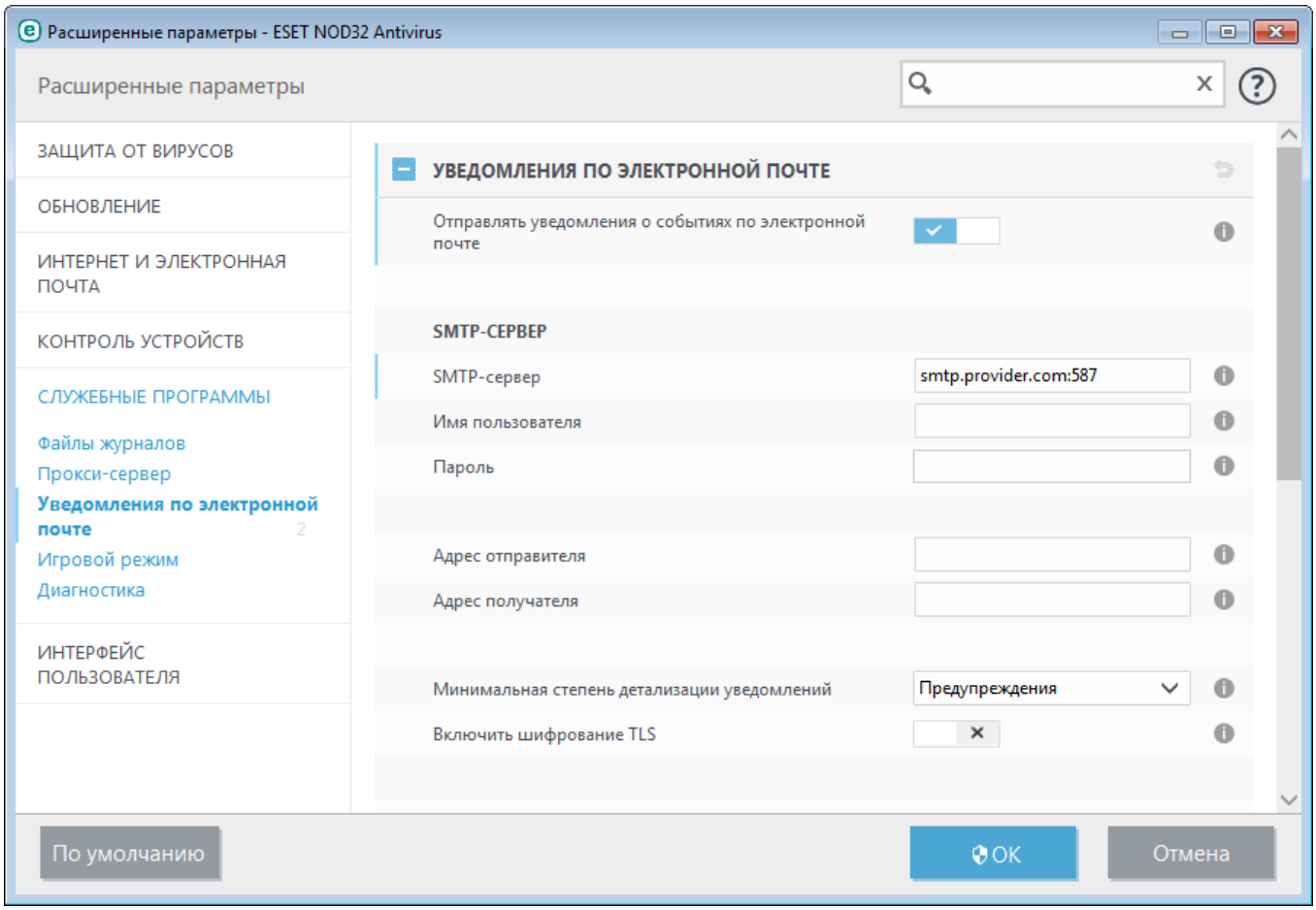
Если требуется аутентификация на прокси-сервере, установите флажок **Прокси-сервер требует аутентификации**, а затем заполните поля **Имя пользователя** и **Пароль**. Нажмите кнопку **Найти**, чтобы автоматически определить параметры прокси-сервера и подставить их. Будут скопированы параметры, указанные в Internet Explorer.

ПРИМЕЧАНИЕ. В настройках в области **Прокси-сервер** имя пользователя и пароль нужно вводить вручную.

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

4.4.1.11 Уведомления по электронной почте

ESET NOD32 Antivirus поддерживает отправку сообщений электронной почты при возникновении событий с заданной степенью детализации. Чтобы включить эту функцию, установите флажок **Отправлять уведомления по электронной почте**.



SMTP-сервер

SMTP-сервер: SMTP-сервер, используемый для отправки оповещений (например, *smtp.provider.com:587*, номер предварительно заданного порта — 25).

ПРИМЕЧАНИЕ. ESET NOD32 Antivirus поддерживает SMTP-серверы, использующие шифрование TLS.

Имя пользователя и **Пароль**: если требуется аутентификация на SMTP-сервере, для получения доступа к нему заполните эти поля.

Адрес отправителя: в этом поле указывается адрес отправителя, который будет отображаться в заголовке писем с уведомлением.

Адрес получателя: в этом поле указывается адрес получателя, который будет отображаться в заголовке писем с уведомлением.

В раскрывающемся списке **Минимальная степень детализации уведомлений** можно выбрать начальный уровень отправляемых уведомлений.

- **Диагностика**: регистрируется информация, необходимая для тщательной настройки программы, а также все перечисленные выше записи.
- **Информационные**: записываются информационные сообщения, такие как нестандартные сетевые события, включая сообщения об успешном выполнении обновления, а также все перечисленные выше записи.
- **Предупреждения**: записываются критические ошибки и предупреждения (например, не удалось выполнить обновление или система Antistealth работает неправильно).
- **Ошибки**: записываются ошибки (не активирована защита документов) и критические ошибки.
- **Критические**: записываются только критические ошибки (ошибки запуска защиты от вирусов или уведомления о наличии вируса в системе).

Включить шифрование TLS: разрешить отправку предупреждений об угрозе и уведомлений с использованием протокола TLS.

Интервал между оправками новых сообщений электронной почты (мин.): время в минутах, спустя которое по электронной почте будут отправляться новые уведомления. Если задать значение 0, уведомления будут отправляться сразу.

Отправлять уведомления в отдельных сообщениях электронной почты: если этот параметр активирован, получатель будет получать каждое уведомление в отдельном сообщении. Это может привести к получению большого количества почты за короткий промежуток времени.

Формат сообщений

Формат сообщений о событиях: формат сообщений о событиях, отображаемых на удаленных компьютерах.

Формат предупреждений об угрозах: предупреждения об угрозе и уведомления по умолчанию имеют предопределенный формат. Изменять этот формат не рекомендуется. Однако в некоторых случаях (например, при наличии системы автоматизированной обработки электронной почты) может понадобиться изменить формат сообщений.

Использовать символы местного алфавита: преобразовывает кодировку сообщения электронной почты в кодировку ANSI на основе региональных параметров Windows (например, Windows-1250). Если не устанавливать этот флажок, сообщение будет преобразовано с использованием 7-битной кодировки ACSII (например, «á» будет преобразовано в «a», а неизвестные символы — в «?»).

Использовать местную кодировку символов: сообщение будет преобразовано в формат Quoted Printable (QP), в котором используются знаки ASCII, что позволяет правильно передавать символы национальных алфавитов по электронной почте в 8-битном формате (áéíóú).

4.4.1.11.1 Формат сообщений

В этом окне можно настроить формат сообщений о событиях, отображающихся на удаленных компьютерах.

Предупреждения об угрозе и уведомления по умолчанию имеют предопределенный формат. Изменять этот формат не рекомендуется. Однако в некоторых случаях (например, при наличии системы автоматизированной обработки электронной почты) может понадобиться изменить формат сообщений.

Ключевые слова (строки, разделенные символом %) в сообщении замещаются реальной информацией о событии. Доступны следующие ключевые слова.

- **%TimeStamp%**: дата и время события.
- **%Scanner%**: задействованный модуль.
- **%ComputerName%**: имя компьютера, на котором произошло событие.
- **%ProgramName%**: программа, создавшая предупреждение.
- **%InfectedObject%**: имя зараженного файла, сообщения и т. п.
- **%VirusName%**: идентифицирующие данные заражения.
- **%ErrorDescription%**: описание события, не имеющего отношения к вирусам.

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

Использовать символы местного алфавита: преобразование сообщений с использованием кодировки ANSI на основе региональных параметров Windows (например, windows-1250). Если не устанавливать этот флажок, сообщение будет преобразовано с использованием 7-битной кодировки ACSII (например, «á» будет преобразовано в «a», а неизвестные символы — в «?»).

Использовать местную кодировку символов: сообщение будет преобразовано в формат Quoted Printable (QP), в котором используются знаки ASCII, что позволяет правильно передавать символы национальных алфавитов по электронной почте в 8-битном формате (áéíóú).

4.4.1.12 Выбор образца для анализа

Диалоговое окно отправки файлов позволяет отправить файл или сайт в ESET для анализа. Чтобы открыть это окно, выберите **Служебные программы** > **Отправка образца на анализ**. При обнаружении на компьютере файла, проявляющего подозрительную активность, или подозрительного сайта в Интернете его можно отправить в исследовательскую лабораторию ESET. Если файл или веб-сайт окажется вредоносным приложением, функция его обнаружения будет включена в последующие обновления.

Другим способом отправки является электронная почта. Если этот способ для вас удобнее, заархивируйте файлы с помощью программы WinRAR или WinZIP, защитите архив паролем «infected» и отправьте его по адресу samples@eset.com. Помните, что тема письма должна описывать проблему, а текст должен содержать как можно более полную информацию о файле (например, адрес веб-сайта, с которого он был загружен).

ПРИМЕЧАНИЕ. Прежде чем отправлять файл в ESET, убедитесь в том, что проблема соответствует одному из следующих критериев:
- файл совсем не обнаруживается;
- файл неправильно обнаруживается как угроза.

Ответ на подобный запрос будет отправлен только в том случае, если потребуется дополнительная информация.

В раскрывающемся меню **Причина отправки файла** выберите наиболее подходящее описание своего сообщения.
- **Подозрительный файл**
- **Подозрительный сайт** (веб-сайт, зараженный вредоносной программой)
- **Ложно обнаруженный файл** (файл обнаружен как зараженный, хотя не является таковым)
- **Ложно обнаруженный сайт**
- **Другое**

Файл/сайт — путь к файлу или веб-сайту, который вы собираетесь отправить.

Адрес электронной почты: адрес отправляется в ESET вместе с подозрительными файлами и может использоваться для запроса дополнительной информации, необходимой для анализа. Указывать адрес электронной почты необязательно. Поскольку каждый день на серверы ESET поступают десятки тысяч файлов, невозможно отправить ответ на каждый запрос. Вам ответят только в том случае, если для анализа потребуется дополнительная информация.

4.4.1.13 Центр обновления Microsoft Windows®

Функция обновления Windows является важной составляющей защиты пользователей от вредоносных программ. По этой причине обновления Microsoft Windows следует устанавливать сразу после их появления. Программное обеспечение ESET NOD32 Antivirus уведомляет пользователя об отсутствующих обновлениях в соответствии с выбранным уровнем. Доступны следующие уровни.

- **Без обновлений**: не будет предлагаться загрузить обновления системы.
- **Необязательные обновления**: будет предлагаться загрузить обновления, помеченные как имеющие низкий и более высокий приоритет.
- **Рекомендованные обновления**: будет предлагаться загрузить обновления, помеченные как имеющие обычный и более высокий приоритет.
- **Важные обновления**: будет предлагаться загрузить обновления, помеченные как важные и имеющие более высокий приоритет.
- **Критические обновления**: пользователю будет предлагаться загрузить только критические обновления.

Для сохранения изменений нажмите кнопку **ОК**. После проверки статуса сервера обновлений на экран будет выведено окно «Обновления системы», поэтому данные об обновлении системы могут быть недоступны непосредственно после сохранения изменений.

4.5 Интерфейс

В разделе **Интерфейс** можно конфигурировать поведение графического интерфейса пользователя программы.

С помощью служебной программы Графика можно изменить внешний вид программы и используемые эффекты.

Путем настройки параметров в разделе Предупреждения и уведомления можно изменить поведение предупреждений об обнаруженных угрозах и системных уведомлений. Их можно настроить в соответствии со своими потребностями.

Если принять решение о том, что некоторые уведомления не должны отображаться, они будут присутствовать в области Скрытые окна уведомлений. Здесь можно проверить их состояние, просмотреть дополнительные сведения или удалить их из данного окна.

Для обеспечения максимального уровня безопасности программного обеспечения можно предотвратить несанкционированное изменение, защитив параметры паролем с помощью служебной программы Параметры доступа.

Если щелкнуть объект правой кнопкой мыши, отобразится контекстное меню. Этот инструмент позволяет интегрировать элементы управления ESET NOD32 Antivirus в контекстное меню.

4.5.1 Элементы интерфейса

Параметры интерфейса пользователя в ESET NOD32 Antivirus позволяют настроить рабочую среду в соответствии с конкретными требованиями. Эти параметры доступны в ветви **Интерфейс** > **Элементы интерфейса дерева расширенных параметров** ESET NOD32 Antivirus.

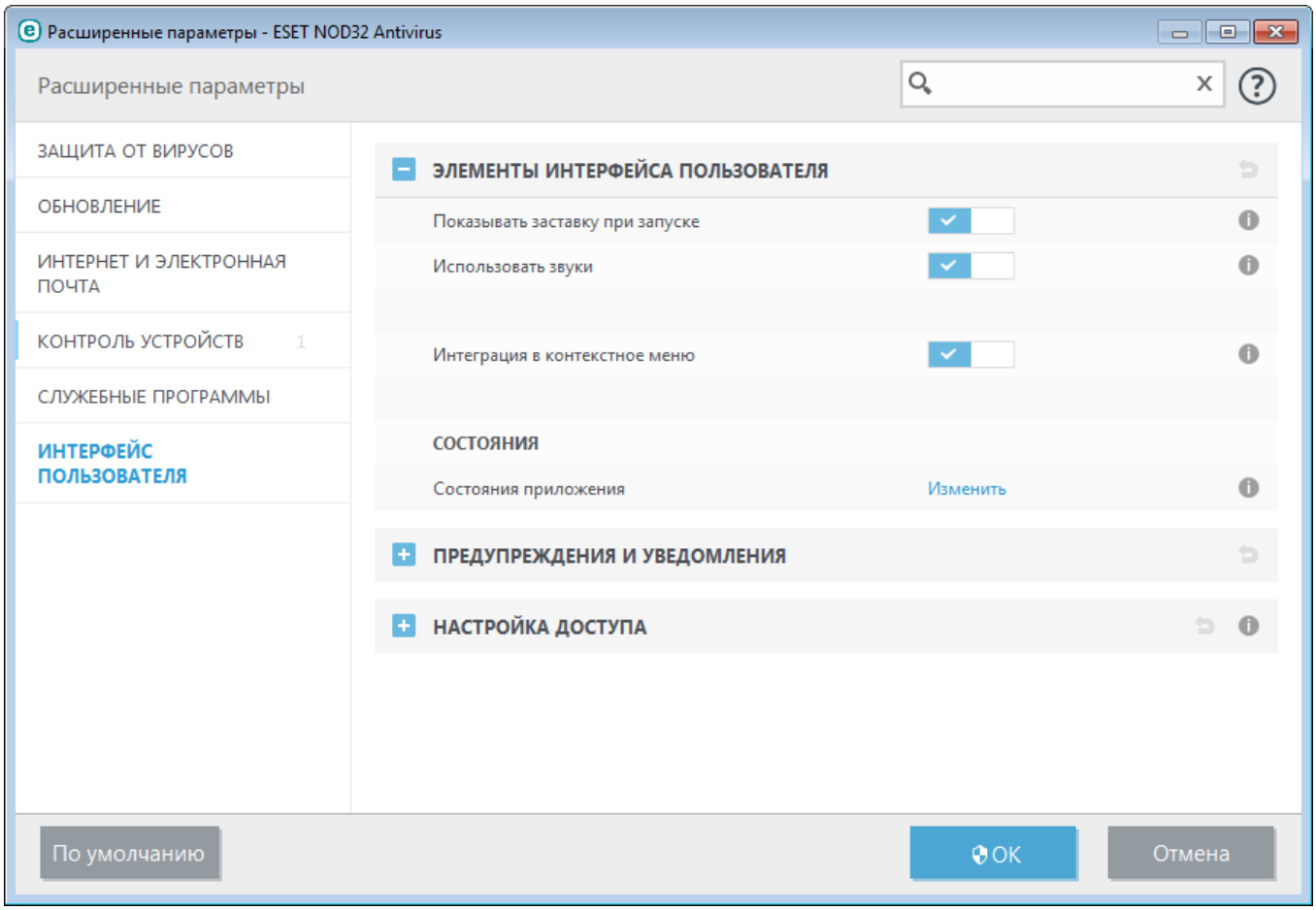
Чтобы отключить заставку ESET NOD32 Antivirus, снимите флажок **Показывать заставку при запуске**.

Если вы хотите, чтобы программа ESET NOD32 Antivirus воспроизводила звуковой сигнал, если во время сканирования происходит важное событие, например обнаружена угроза или сканирование закончено, выберите установку **Использовать звуки**.

Интегрировать с контекстным меню: можно интегрировать элементы управления ESET NOD32 Antivirus в контекстное меню.

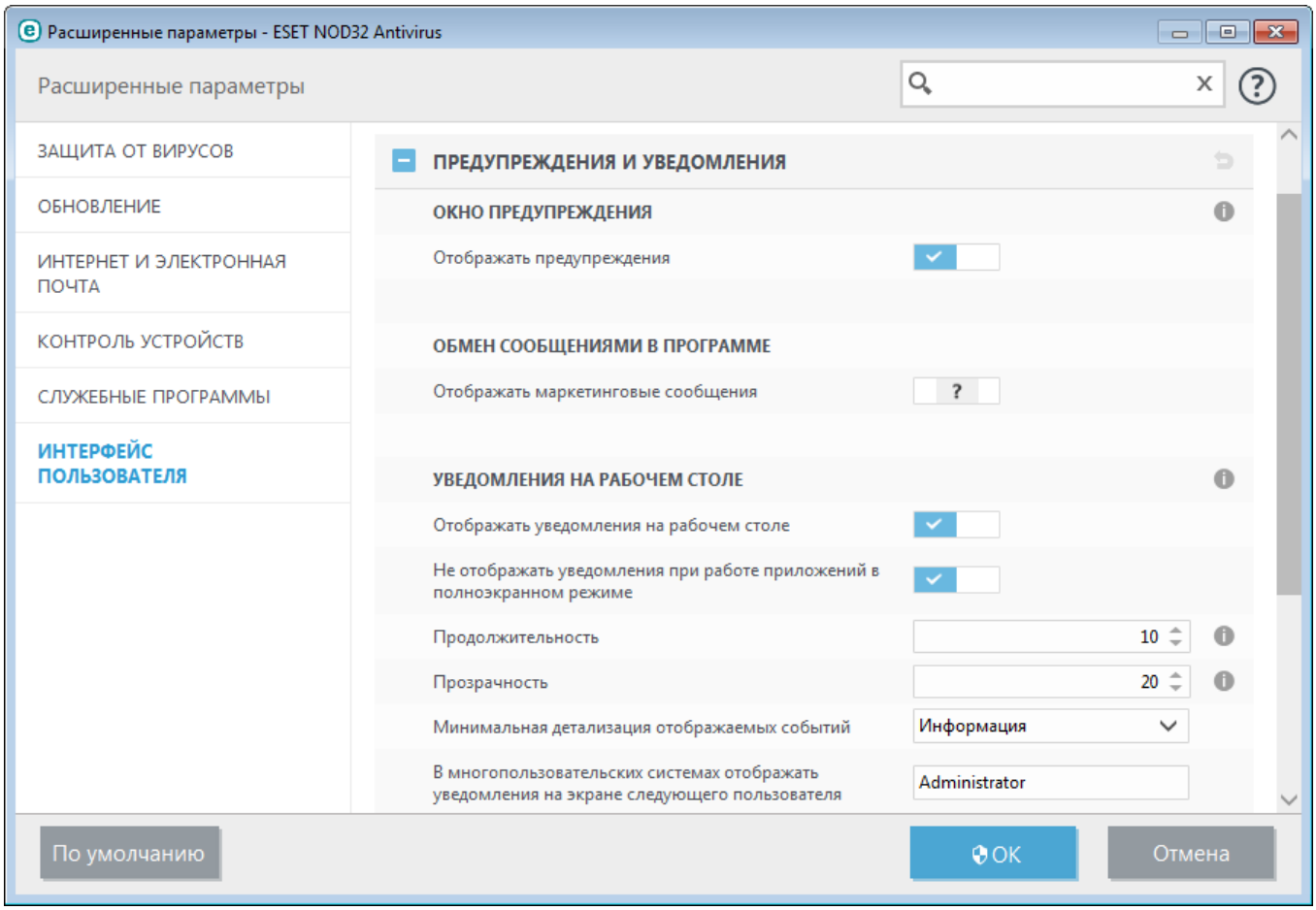
Состояния

Состояния приложения: чтобы включить или выключить отображение состояний в области главного меню **Состояние защиты**, щелкните элемент **Изменить**.


Расширенные параметры - ESET NOD32 Antivirus
Расширенные параметры
ЗАЩИТА ОТ ВИРУСОВ
ОБНОВЛЕНИЕ
ИНТЕРНЕТ И ЭЛЕКТРОННАЯ ПОЧТА
КОНТРОЛЬ УСТРОЙСТВ 1
СЛУЖЕБНЫЕ ПРОГРАММЫ
ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ
ЭЛЕМЕНТЫ ИНТЕРФЕЙСА ПОЛЬЗОВАТЕЛЯ
Показывать заставку при запуске
Использовать звуки
Интеграция в контекстное меню
СОСТОЯНИЯ
Состояния приложения
Изменить
ПРЕДУПРЕЖДЕНИЯ И УВЕДОМЛЕНИЯ
НАСТРОЙКА ДОСТУПА
По умолчанию
OK
Отмена

4.5.2 Предупреждения и уведомления

В разделе **Предупреждения и уведомления** окна **Интерфейс** можно настроить способ обработки предупреждений об угрозах и системных уведомлений (например, сообщений об успешном выполнении обновлений) для программы ESET NOD32 Antivirus. Здесь также можно настроить время отображения и прозрачность уведомлений на панели задач (применяется только к системам, поддерживающим уведомления на панели задач).



Окно предупреждения

Если отключить параметр **Отображать предупреждение**, окна предупреждения не будут выводиться на экран; делать это следует только в некоторых особых ситуациях. В большинстве случаев рекомендуется оставить для этого параметра значение по умолчанию (включен).

Обмен сообщениями в программе

Отображать маркетинговые сообщения: функция внутрипрограммного обмена сообщениями предназначена для информирования пользователей о новостях ESET и для других сообщений. Снимите этот флажок, если не хотите получать маркетинговые сообщения.

Уведомления на рабочем столе

Уведомления на рабочем столе и всплывающие подсказки предназначены только для информирования и не требуют участия пользователя. Они отображаются в области уведомлений в правом нижнем углу экрана. Чтобы активировать уведомления на рабочем столе, установите флажок **Отображать уведомления на рабочем столе**.

Установите флажок **Не отображать уведомления при работе приложений в полноэкранном режиме**, чтобы запретить все неинтерактивные уведомления. Более детальные параметры, такие как время отображения и прозрачность окна уведомлений, можно изменить, выполнив приведенные ниже инструкции.

В раскрывающемся списке **Минимальная детализация отображаемых событий** можно выбрать уровень

серьезности предупреждений и уведомлений, которые следует отображать. Доступны указанные ниже варианты.

- **Диагностика**: регистрируется информация, необходимая для тщательной настройки программы, а также все перечисленные выше записи.
- **Информационные**: записываются информационные сообщения, в том числе сообщения об успешном выполнении обновления, а также все перечисленные выше записи.
- **Предупреждения**: записывается информация обо всех критических ошибках и предупреждениях.
- **Ошибки**: записываются сведения об ошибках загрузки файлов и критических ошибках.
- **Критические**: регистрируются только критические ошибки (ошибки запуска защиты от вирусов,и т. п.).

Последний параметр этого раздела позволяет настроить, кто именно должен получать уведомления в многопользовательской среде. В поле **В многопользовательских системах отображать уведомления для пользователя** указывается пользователь, который будет получать системные и прочие уведомления, что позволяет одновременно подключаться к системе нескольким пользователям. Обычно это системный или сетевой администратор. Эта функция особенно полезна для терминальных серверов при условии, что все системные уведомления отправляются администратору.

Окно сообщения

Чтобы всплывающие окна закрывались автоматически по истечении определенного времени, установите флажок **Автоматически закрывать окна сообщений**. Если окно предупреждения не будет закрыто пользователем, оно закрывается автоматически через указанный промежуток времени.

Подтверждения: отображение списка подтверждений, для которых можно настроить параметры отображения.

4.5.2.1 Дополнительные настройки

В раскрывающемся меню **Минимальная детализация отображаемых событий** можно выбрать начальный уровень серьезности предупреждений и уведомлений, которые следует отображать.

- **Диагностика**: регистрируется информация, необходимая для тщательной настройки программы, а также все перечисленные выше записи.
- **Информационные**: записываются информационные сообщения, в том числе сообщения об успешном выполнении обновления, а также все перечисленные выше записи.
- **Предупреждения**: записывается информация обо всех критических ошибках и предупреждениях.
- **Ошибки**: регистрируется информация об *ошибках загрузки файлов* и критических ошибках.
- **Критические**: регистрируются только критические ошибки (ошибки запуска защиты от вирусови т. п.).

Последний параметр этого раздела позволяет сконфигурировать, кто именно должен получать уведомления в многопользовательской среде. В поле **В многопользовательских системах отображать уведомления для пользователя** указывается пользователь, который будет получать системные и прочие уведомления, если одновременно может быть подключено несколько пользователей. Обычно это системный или сетевой администратор. Эта функция особенно полезна для терминальных серверов при условии, что все системные уведомления отправляются администратору.

4.5.3 Скрытые окна уведомлений

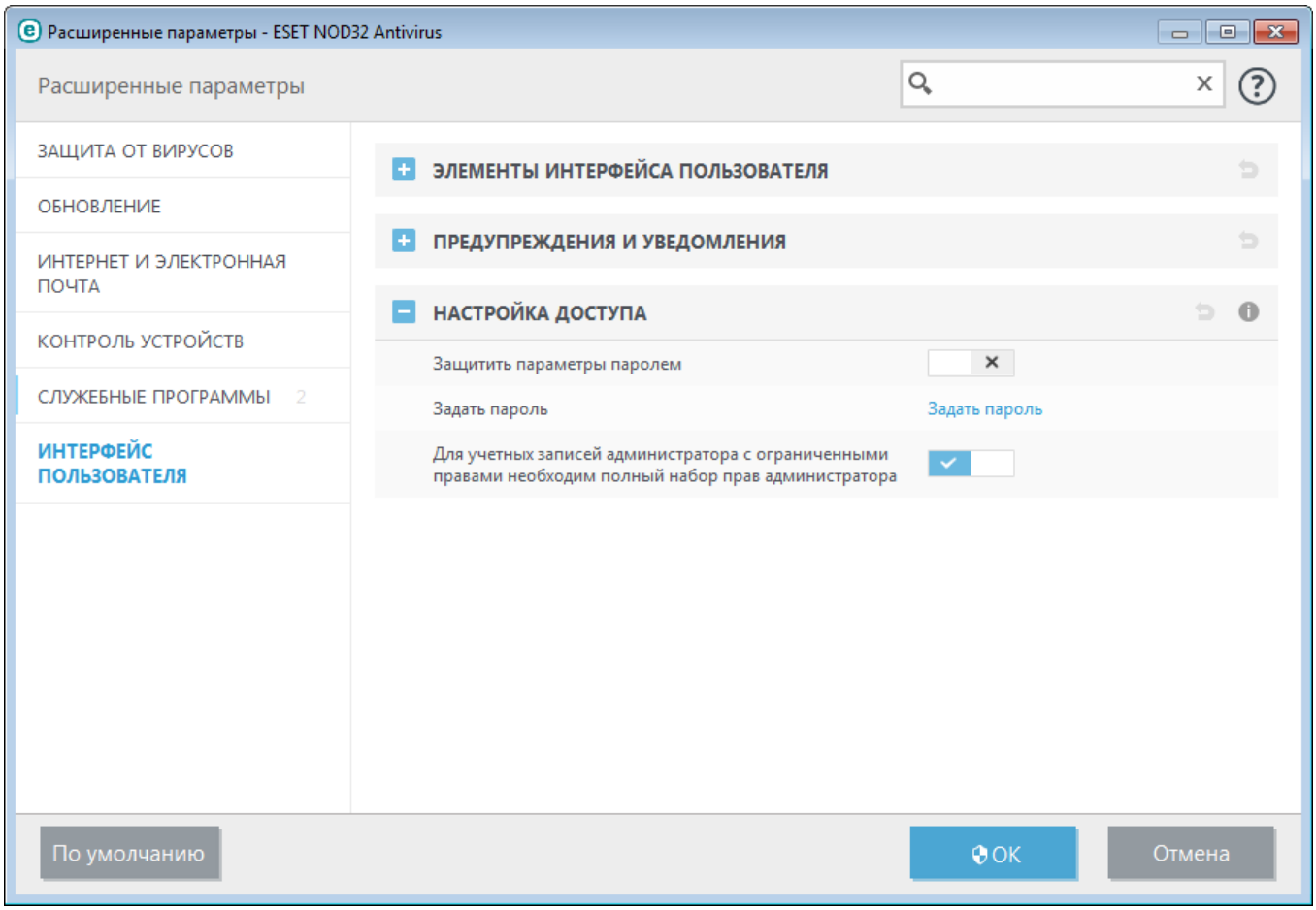
Если для одного из показанных ранее окон уведомлений (предупреждений) выбран параметр **Больше не показывать это сообщение**, данное окно появится в списке скрытых окон уведомлений. Действия, которые в настоящий момент выполняются автоматически, отображаются в столбце **Подтвердить**.

Показать: предварительный просмотр окон уведомлений, которые сейчас не отображаются и для которых сконфигурировано автоматическое действие.

Удалить: удаление элементов из списка **Скрытые диалоговые окна**. Все окна уведомлений, удаленные из списка, снова будут отображаться.

4.5.4 Настройка доступа

Настройки ESET NOD32 Antivirus являются важной составной частью вашей политики безопасности. Несанкционированное изменение параметров может нарушить стабильность работы системы и ослабить ее защиту. Для предотвращения несанкционированного изменения параметры ESET NOD32 Antivirus можно защитить паролем.



Защитить параметры паролем: выбор настроек парольной защиты. Щелкните, чтобы открыть окно настройки пароля.

Чтобы установить или изменить пароль для защиты параметров настройки, щелкните **Настроить**.

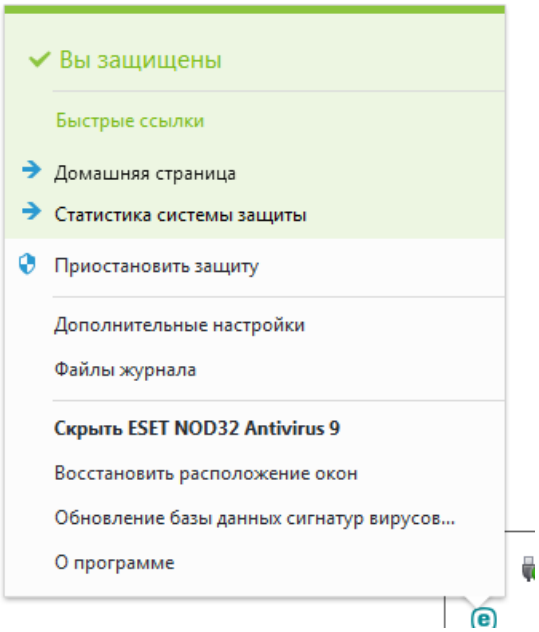
Требуется полный набор прав администратора для ограниченных учетных записей администратора: выберите этот параметр, чтобы при изменении определенных параметров системы для текущего пользователя (если у такого пользователя нет прав администратора) отображался запрос на ввод имени пользователя и пароля администратора (аналогично контролю учетных записей в Windows Vista и Windows 7). К таким изменениям относится отключение модулей защиты. В ОС Windows XP, где нет контроля учетных записей, для пользователей будет доступен параметр **Требуются права администратора (система без поддержки UAC)**.

Только для Windows XP:

Требуются права администратора (система без поддержки UAC): установите этот флажок, чтобы программа ESET NOD32 Antivirus предлагала ввести учетные данные администратора.

4.5.5 Меню программы

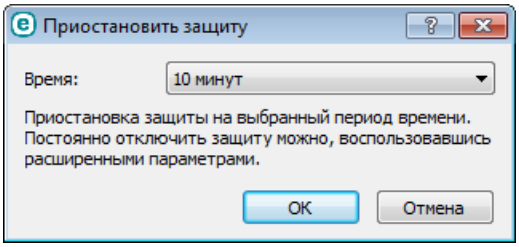
К некоторым наиболее важным функциям и настройкам можно получить доступ, щелкнув правой кнопкой мыши значок на панели задач .



Быстрые ссылки: отображение наиболее часто используемых компонентов ESET NOD32 Antivirus. К ним можно быстро перейти через меню программы.

Приостановить защиту: на экран выводится диалоговое окно для подтверждения. В нем можно отключить защиту от вирусов и шпионских программ, посредством которой, путем контроля обмена файлами и данными через Интернет и электронную почту, предотвращаются атаки на компьютер со стороны злонамеренных систем.

В раскрывающемся меню **Время** указывается период времени, на которое будет полностью отключена защита от вирусов и шпионских программ.



Дополнительные настройки: установите этот флажок, чтобы перейти к дереву **Дополнительные настройки**. Дерево дополнительных настроек можно отобразить и другими способами, например нажать клавишу F5 или использовать меню **Настройка** > **Дополнительные настройки**.

Файлы журнала: файлы журнала содержат информацию о важных программных событиях и предоставляют общие сведения об обнаруженных угрозах.

СкрытьESET NOD32 Antivirus: позволяет скрыть окно ESET NOD32 Antivirus.

Сбросить настройки макета окна: для окна ESET NOD32 Antivirus восстанавливаются размер и положение на экране по умолчанию.

Активируйте программу...: выберите этот параметр, если вы еще не активировали продукт обеспечения безопасности ESET, или повторно введите ученые данные для активации продукта после обновления лицензии.

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

О программе: отображение системной информации, сведений об установленной версии ESET NOD32 Antivirus и модулях программы. Также здесь отображаются дата окончания срока действия лицензии и данные об операционной системе и системных ресурсах.

4.5.6 Контекстное меню

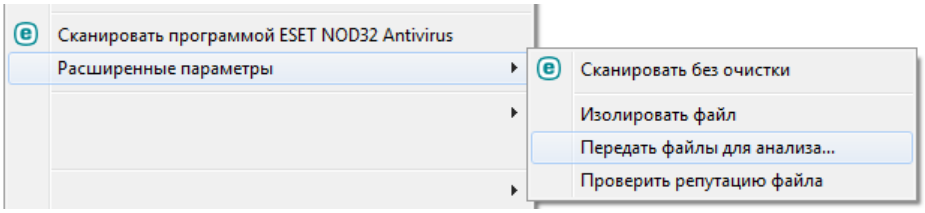
Если щелкнуть объект правой кнопкой мыши, отобразится контекстное меню. В меню указаны все действия, которые можно выполнить по отношению к объекту.

Элементы управления ESET NOD32 Antivirus можно интегрировать в контекстное меню. Более детальная настройка этих функций выполняется в дереве расширенных параметров, в разделах **Интерфейс** > **Контекстное меню**.

Интегрировать с контекстным меню: можно интегрировать элементы управления ESET NOD32 Antivirus в контекстное меню.

В раскрывающемся меню **Тип меню** доступны следующие варианты.

- **Полное (сначала сканирование)**: активация всех функций контекстного меню. В главном меню первым будет отображаться пункт **Сканировать без очистки с помощью ESET NOD32 Antivirus**, а вторым — **Сканировать и очистить**.
- **Полное (сначала очистка)**: активация всех функций контекстного меню. В главном меню первым будет отображаться пункт **Сканировать программой ESET NOD32 Antivirus**, а вторым — **Сканировать без очистки**.



- **Только сканирование**: в контекстном меню будет отображаться только пункт **Сканировать без очистки с помощью ESET NOD32 Antivirus**.
- **Только очистка**: в контекстном меню будет отображаться только пункт **Сканировать программой ESET NOD32 Antivirus**.

5. Для опытных пользователей

5.1 Диспетчер профилей

Диспетчер профилей используется в двух разделах ESET NOD32 Antivirus: в разделе **Сканирование ПК по требованию** и в разделе **Обновление**.

Сканирование компьютера

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

Для создания профиля откройте окно «Дополнительные настройки» (F5) и щелкните **Защита от вирусов** > **Сканирование компьютера по требованию** > **Основное** > **Список профилей**. В окне **Диспетчер профилей** есть раскрывающееся меню **Выбранный профиль**, в котором перечисляются существующие профили сканирования и есть возможность создать новый. Для создания профиля сканирования в соответствии с конкретными потребностями см. раздел Настройка параметров модуля ThreatSense, в котором описывается каждый параметр, используемый для настройки сканирования.

Пример. Предположим, пользователю требуется создать собственный профиль сканирования, причем конфигурация **Сканировать компьютер** частично устраивает его, но не нужно сканировать упаковщики или потенциально опасные приложения, но при этом нужно применить **тщательную очистку**. Введите имя нового профиля в окне **Диспетчер профилей** и нажмите кнопку **Добавить**. Выберите новый профиль в раскрывающемся меню **Выбранный профиль** и настройте остальные параметры в соответствии со своими требованиями, а затем нажмите кнопку **ОК**, чтобы сохранить новый профиль.

Обновление

Редактор профилей, расположенный в разделе «Настройка обновлений», дает пользователям возможность создавать новые профили обновления. Создавать и использовать собственные пользовательские профили (т. е. профили, отличные от профиля по умолчанию **Мой профиль**) следует только в том случае, если компьютер подключается к серверам обновлений разными способами.

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

Выбранный профиль: текущий профиль обновления. Для изменения профиля выберите нужный из раскрывающегося меню.

Добавить...: создание новых профилей обновления.

В нижней части окна находится список существующих профилей.

5.2 Сочетания клавиш

Для более удобной навигации в программе ESET можно использовать следующие сочетания клавиш.

F1	вызов справки
F5	вызов окна расширенных параметров
Вверх/вниз	переход по элементам в программе
-	свертывание узлов дерева расширенных параметров
TAB	перемещение курсора по окну
Esc	закрытие активного диалогового окна

5.3 Диагностика

Функция диагностики формирует аварийные дампы приложения процессов ESET (например, *ekrn*). Если происходит сбой приложения, формируется дамп памяти. Это может помочь разработчикам выполнять отладку и устранять различные проблемы ESET NOD32 Antivirus. Откройте раскрывающийся список рядом с элементом **Тип дампа** и выберите один из трех доступных вариантов.

- Выберите **Отключить** (установлено по умолчанию), чтобы отключить эту функцию.
- **Мини**: регистрируется самый малый объем полезной информации, которая может помочь выявить причину неожиданного сбоя приложения. Подобный файл дампа может пригодиться, если на диске мало места. Однако при анализе ограниченный объем включенной в него информации может не позволить обнаружить ошибки, которые не были вызваны непосредственно потоком, выполнявшимся в момент возникновения проблемы.
- **Полный**: когда неожиданно прекращается работа приложения, регистрируется все содержимое системной памяти. Полный дамп памяти может содержать данные процессов, которые выполнялись в момент создания дампа.

Включить расширенное ведение журнала фильтрации протоколов: запись всех сетевых данных, проходящих через модуль фильтрации протоколов в формате PCAP. Это помогает разработчикам диагностировать и устранять проблемы, связанные с фильтрацией протоколов.

Файлы журналов хранятся в расположении:
C:\ProgramData\ESET\ESET Smart Security\Diagnostics в ОС Windows Vista или более поздних версиях Windows либо по адресу *C:\Documents and Settings\All Users\...* в старых версиях Windows.

Целевой каталог: каталог, в котором будет создаваться дамп при сбое.

Открыть папку диагностики: нажмите кнопку **Показать**, чтобы открыть этот каталог в новом окне *проводника Windows*.

5.4 Импорт и экспорт параметров

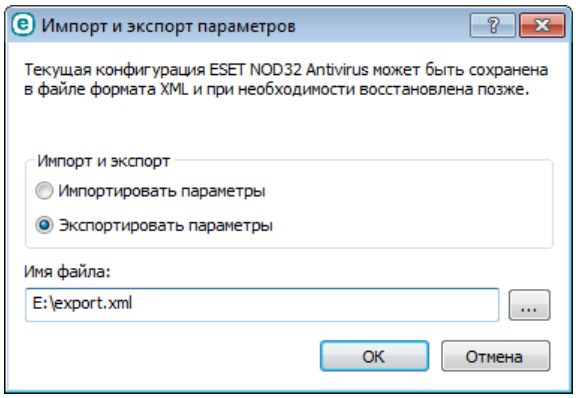
Можно импортировать и экспортировать пользовательский XML-файл конфигурации ESET NOD32 Antivirus с помощью меню **Настройка**.

Импорт и экспорт файлов конфигурации удобны, если нужно создать резервную копию текущей конфигурации программы ESET NOD32 Antivirus для использования в будущем. Экспорт параметров также удобен, если необходимо использовать предпочитаемую конфигурацию на нескольких компьютерах. С этой целью файл *.xml* можно легко импортировать для переноса нужных параметров.

Импортировать конфигурацию несложно. В главном окне программы выберите команду **Настройка** > **Импорт и экспорт параметров...**, а затем — **Импортировать параметры**. Введите имя для файла конфигурации или нажмите кнопку **...**, чтобы выбрать файл конфигурации, который следует импортировать.

Процедура экспорта конфигурации похожа на ее импорт. В главном меню выберите пункт **Настройка** > **Импорт и экспорт параметров...**. Выберите **Экспортировать параметры** и введите имя для файла конфигурации (например, *export.xml*). С помощью проводника выберите место на компьютере для сохранения файла конфигурации.

ПРИМЕЧАНИЕ. При экспорте параметров может возникнуть ошибка, если у вас недостаточно прав для записи экспортируемого файла в указанный каталог.



5.5 Обнаружение в состоянии простоя

Параметры обнаружения в состоянии простоя можно настроить в разделе **Дополнительные настройки**, доступном через **Служебные программы** > **Обнаружение в состоянии простоя**. Данные параметры позволяют указать условие запуска обнаружения в состоянии простоя, например когда:

- запущена заставка;
- компьютер заблокирован;
- пользователь выполняет выход.

Используйте флажки для каждого состояния, чтобы включить или отключить различные условия обнаружения в состоянии простоя.

5.6 ESET SysInspector

5.6.1 Введение в ESET SysInspector

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

Существует два способа воспользоваться приложением ESET SysInspector. Во-первых, можно открыть интегрированную в решения ESET Security версию, а, во-вторых, загрузить самостоятельную версию (SysInspector.exe) бесплатно с веб-сайта ESET. Обе версии аналогичны по своим функциям и имеют одинаковые элементы управления программой. Единственное отличие заключается в том, как осуществляется управление результатами. И самостоятельная, и интегрированная версии позволяют экспортировать снимки системы в файл в формате *.xml* и сохранять его на диске. Однако интегрированная версия также дает возможность сохранить снимки системы непосредственно из меню **Служебные программы** > **ESET SysInspector** (кроме решения ESET Remote Administrator). Дополнительные сведения см. в разделе ESET SysInspector как часть ESET NOD32 Antivirus.

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

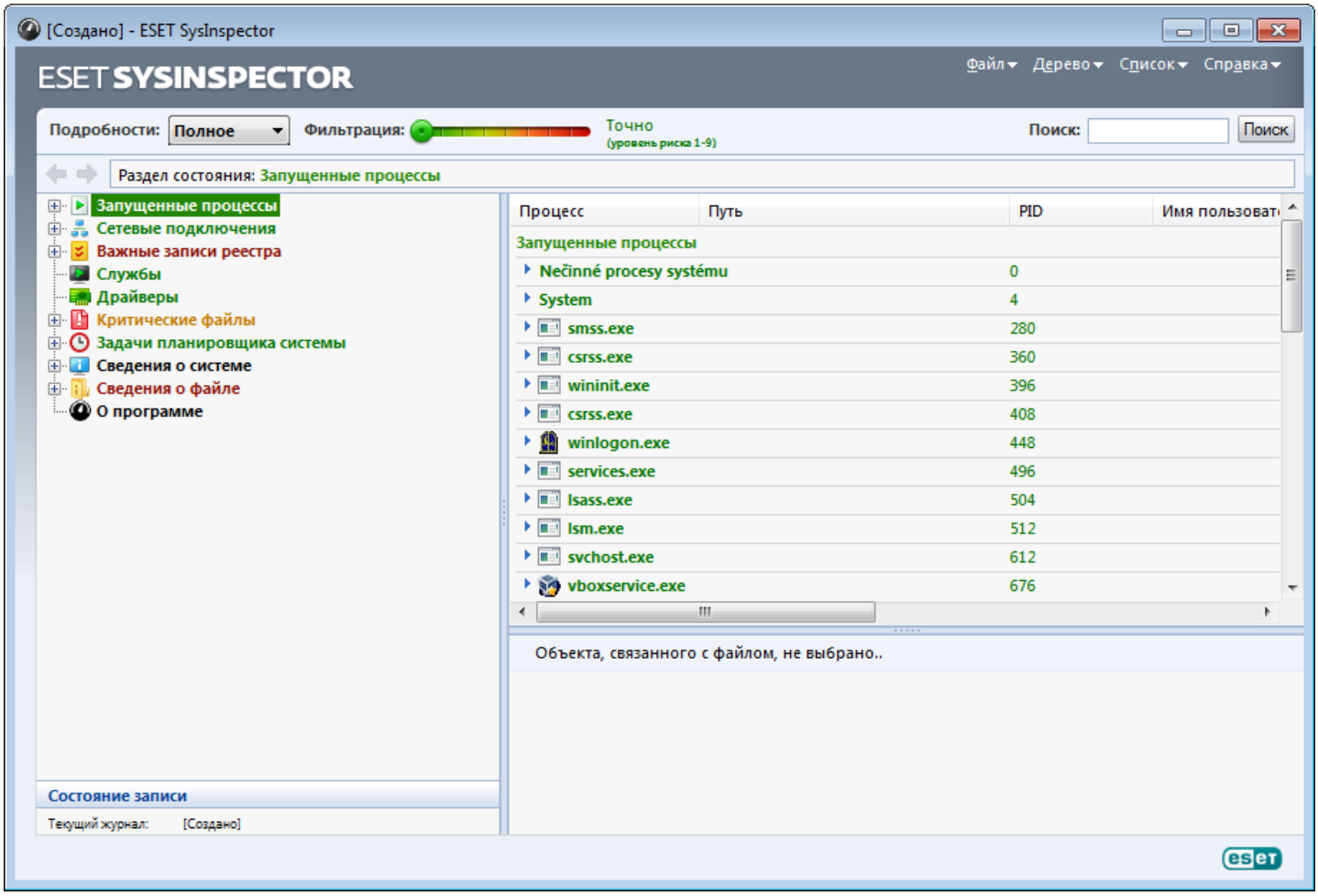
5.6.1.1 Запуск ESET SysInspector

Для запуска ESET SysInspector достаточно выполнить файл *SysInspector.exe*, загруженный с веб-сайта ESET. Если у вас уже установлено одно из решений ESET Security, можно запустить ESET SysInspector непосредственно из меню «Пуск» (**Программы** > **ESET** > **ESET NOD32 Antivirus**).

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

5.6.2 Интерфейс пользователя и работа в приложении

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



5.6.2.1 Элементы управления программой

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

Файл

Элемент **Файл** позволяет сохранить данные о текущем состоянии системы для их последующего изучения или открыть ранее сохраненный журнал. Если планируется опубликовать журнал, для его создания рекомендуется использовать пункт меню **Подходит для отправки**. В этом случае из него исключается конфиденциальная информация (например, имя текущего пользователя, имена компьютера и домена, права текущего пользователя, переменные окружения и т. п.).

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

Дерево

Позволяет развернуть или свернуть все узлы, а также экспортировать выделенные разделы в сценарий службы.

Список

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

Справка

Содержит сведения о приложении и его функциях.

Подробности

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

Фильтрация

Фильтрация элементов очень удобна для поиска подозрительных файлов или записей реестра, существующие в системе. С помощью ползунка можно фильтровать элементы по их уровню риска. Если ползунок установлен в крайнее левое положение (уровень риска 1), отображаются все элементы. При перемещении ползунка вправо программа будет отфильтровывать все элементы с уровнем риска, меньшим текущего уровня, и выводить на экран только те элементы, уровень подозрительности которых выше данного уровня. Если ползунок находится в крайнем правом положении, программа отображает только определенно вредоносные элементы.

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

ПРИМЕЧАНИЕ. Уровень риска элемента легко определяется путем сравнения цвета элемента с цветом на ползунке уровней рисков.

Сравнить

При сравнении двух журналов можно выбрать, какие элементы следует отображать: все элементы, только добавленные элементы, только удаленные элементы или только замененные элементы.

Найти

Поиск можно использовать для быстрого нахождения определенного элемента по его названию или части названия. Результаты поиска отображаются в окне описания.

Возврат

С помощью стрелок назад и вперед можно вернуться в окне описания к ранее отображенной информации. Вместо стрелок перехода назад и вперед можно использовать клавиши Backspace и пробел.

Раздел состояния

Отображает текущий узел в окне навигации.

Внимание! Элементы, выделенные красным цветом, являются неизвестными, поэтому программа помечает их как потенциально опасные. Если элемент выделен красным, это не означает, что соответствующий файл можно удалить. Перед удалением убедитесь, что файлы действительно опасны или не являются необходимыми.

5.6.2.2 Навигация в ESET SysInspector

ESET SysInspector распределяет информацию разных типов по нескольким основным разделам, называемым узлами. Для того чтобы получить дополнительные сведения о каком-либо из разделов, разверните вложенные узлы соответствующего узла. Чтобы открыть или свернуть узел, дважды щелкните имя узла либо рядом с именем щелкните значок + или −. При перемещении по древовидной структуре узлов и вложенных узлов в окне навигации различные сведения о каждом узле отображаются в окне описания. При переходе к конкретному элементу в окне подробной информации отображаются дополнительные сведения о нем.

Ниже описаны основные узлы, отображаемые в окне навигации, и относящаяся к ним информация, доступная в окнах описания и подробных сведений.

Запущенные процессы

Этот узел содержит сведения о приложениях и процессах, выполняемых в момент создания журнала. В окне описания могут находиться дополнительные сведения о каждом из процессов, например названия динамических библиотек, используемых процессом, и их местонахождение в системе, название поставщика приложения и уровень риска файла.

Окно подробных сведений содержит дополнительную информацию об элементах, выделенных в окне описания, такую как размер файла или его хэш.

ПРИМЕЧАНИЕ. Любая операционная система состоит из нескольких важных компонентов ядра, которые постоянно работают и обеспечивают работу базовых крайне важных функций для других пользовательских приложений. В определенных случаях путь к файлам таких процессов отображается в ESET SysInspector с символами «\??\» в начале. Эти символы обеспечивают оптимизацию до запуска таких процессов и с точки зрения системы являются безопасными.

Сетевые подключения

В окне описания перечислены процессы и приложения, которые обмениваются данными через сеть по протоколу, выбранному в окне навигации (TCP или UDP), а также удаленные адреса, с которыми эти приложения устанавливают соединения. Также можно проверить IP-адреса DNS-серверов.

Окно подробных сведений содержит дополнительную информацию об элементах, выделенных в окне описания, такую как размер файла или его хэш.

Важные записи реестра

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

В окне описания также может отображаться, какие файлы связаны с конкретными записями реестра. В окне подробных сведений может быть представлена дополнительная информация.

Службы

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

Драйверы

Список драйверов, установленных в системе.

Критические файлы

В окне описания отображается содержимое критических файлов, относящихся к операционной системе Microsoft Windows.

Задачи системного планировщика

Список задач, запускаемых планировщиком заданий Windows в указанное время или интервал времени.

Информация о системе

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

Сведения о файле

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

О программе

Информация о версии ESET SysInspector и список программных модулей.

5.6.2.2.1 Сочетания клавиш

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

Файл

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

Создать

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

Фильтрация элементов

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

Просмотр

Ctrl + 5	просмотр по производителям, все производители
Ctrl + 6	просмотр по производителям, только Microsoft
Ctrl + 7	просмотр по производителям, все другие производители
Ctrl + 3	отображение полных сведений
Ctrl + 2	отображение сведений средней степени подробности
Ctrl + 1	основной вид
BackSpace	переход на один шаг назад
Пробел	переход на один шаг вперед
Ctrl + W	разворачивание дерева
Ctrl + Q	сворачивание дерева

Прочие элементы управления

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

Ctrl + A	отображение всех сведений об элементе
Ctrl + C	копирование дерева текущего элемента
Ctrl + X	копирование элементов
Ctrl + B	поиск сведений о выбранных файлах в Интернете
Ctrl + L	открытие папки, в которой находится выделенный файл
Ctrl + R	открытие соответствующей записи в редакторе реестра
Ctrl + Z	копирование пути к файлу (если элемент связан с файлом)
Ctrl + F	переход в поле поиска
Ctrl + D	закрытие результатов поиска
Ctrl + E	запуск сценария службы

Сравнение

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

Разное

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

5.6.2.3 Сравнение

С помощью функции сравнения пользователь может сравнить два существующих журнала. Результатом выполнения этой команды является набор элементов, не совпадающих в этих журналах. Это позволяет отслеживать изменения в системе, что удобно для обнаружения вредоносного кода.

После запуска приложение создает новый журнал, который выводится на экран в новом окне. Чтобы сохранить журнал в файл, в меню **Файл** выберите пункт **Сохранить журнал**. Сохраненные файлы журналов можно впоследствии открывать и просматривать. Чтобы открыть существующий журнал, в меню **Файл** выберите пункт **Открыть журнал**. В главном окне программы ESET SysInspector в каждый момент времени отображается только один журнал.

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

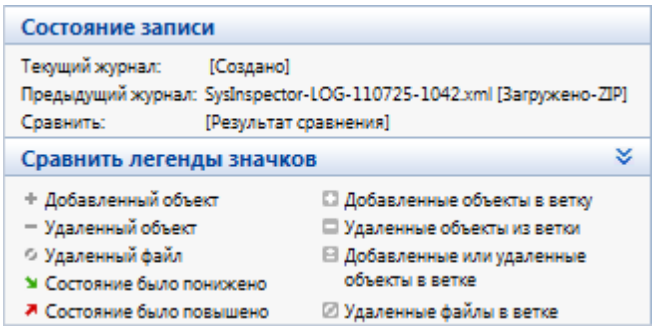
ПРИМЕЧАНИЕ. При сравнении двух файлов журнала в меню **Файл** выберите пункт **Сохранить журнал** и сохраните журнал как файл в формате ZIP. В результате будут сохранены оба файла. Если позже открыть такой файл, содержащиеся в нем журналы будут автоматически сравниваться.

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

Описание всех символов, которые могут отображаться напротив элементов

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

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



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

Пример

Создайте и сохраните журнал, содержащий исходную информацию о системе, в файл с названием «предыдущий.xml». После внесения изменений в систему откройте ESET SysInspector и разрешите приложению создать новый журнал. Сохраните его в файл с названием *текущий.xml*.

Чтобы отследить различия между этими двумя журналами, в меню **Файл** выберите пункт **Сравнить журналы**. Программа создаст сравнительный журнал, содержащий различиями между сравниваемыми.

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

SysIsnpector.exe текущий.xml предыдущий.xml

5.6.3 Параметры командной строки

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

/gen	создание журнала из командной строки без запуска графического интерфейса
/privacy	создание журнала без конфиденциальной информации
/zip	сохранение созданного журнала в ZIP-архиве
/silent	скрытие окна выполнения при создании журнала из командной строки
/blank	запуск ESET SysInspector без создания или загрузки журнала

Примеры

Использование:
```
Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]
```

Чтобы открыть определенный журнал непосредственно в браузере, воспользуйтесь следующей командой: *SysInspector.exe .\клиентский_журнал.xml*
Чтобы создать журнал из командной строки, воспользуйтесь следующей командой: *SysInspector.exe /gen=.\мой_новый_журнал.xml*
Чтобы создать журнал, из которого исключена конфиденциальная информация, непосредственно в сжатом файле, воспользуйтесь следующей командой: *SysInspector.exe /gen=.\мой_новый_журнал.zip /privacy /zip*
Чтобы сравнить два журнала и просмотреть различия, воспользуйтесь следующей командой: *SysInspector.exe*

новый.xml старый.xml

ПРИМЕЧАНИЕ. Если название файла или папки содержит пробел, это название необходимо заключить в кавычки.

5.6.4 Сценарий службы

Сценарий службы — это специальное средство, помогающее пользователям ESET SysInspector с легкостью удалять нежелательные объекты с компьютера.

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

Сценарий службы предназначен для пользователей, имеющих опыт в диагностике компьютерных систем. Неквалифицированные действия могут привести к повреждению операционной системы.

Пример

При наличии подозрения о заражении компьютера вирусом, который не обнаруживается программой защиты от вирусов, выполните приведенные ниже пошаговые инструкции.

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

5.6.4.1 Создание сценариев службы

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

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

5.6.4.2 Структура сценария службы

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

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

01) Running processes (Запущенные процессы)

В этом разделе содержится список процессов, запущенных в системе. Каждый процесс идентифицируется по UNC-пути, а также по хэш-коду CRC16, заключенному в символы звездочки (*).

Пример.

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

В данном примере выделен (помечен символом «+») процесс module32.exe. При выполнении сценария этот процесс будет завершен.

02) Loaded modules (Загруженные модули)

В этом разделе перечислены используемые в данный момент системные модули.

Пример.

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

В данном примере модуль khbekhb.dll помечен символом «+». При выполнении сценария процессы, использующие данный модуль, распознаются и завершаются.

03) TCP connections (Подключения по TCP)

Этот раздел содержит данные о существующих подключениях по TCP.

Пример.

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

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

04) UDP endpoints (Конечные точки UDP)

Этот раздел содержит информацию о существующих конечных точках UDP.

Пример.

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

При выполнении сценария определяется владелец сокета помеченных конечных точек UDP, после чего сокет останавливается.

05) DNS server entries (Записи DNS-сервера)

Этот раздел содержит информацию о текущей конфигурации DNS-сервера.

Пример.

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

При выполнении сценария помеченные записи DNS-сервера удаляются.

06) Important registry entries (Важные записи реестра)

Этот раздел содержит информацию о важных записях реестра.

Пример.

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

При выполнении сценария помеченные записи будут удалены, сведены к 0-разрядным значениям или же будут восстановлены их значения по умолчанию. Действия, применяемые к конкретным записям, зависят от категории и значения записи реестра.

07) Services (Службы)

Этот раздел содержит список служб, зарегистрированных в системе.

Пример.

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

При выполнении сценария помеченные службы, а также все зависящие от них службы будут остановлены и удалены.

08) Drivers (Драйверы)

В этом разделе перечислены установленные драйверы.

Пример.

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

При выполнении сценария выбранные драйверы будут остановлены. Обратите внимание, что некоторые драйверы не удастся остановить.

09) Critical files (Критические файлы)

Этот раздел содержит информацию о файлах, критически необходимых для правильной работы операционной системы.

Пример.

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

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

10) Запланированные задачи

Этот раздел содержит информацию о запланированных задачах.

Пример.

```
10) Scheduled tasks
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe /c
- c:\users\admin\appdata\local\google\update\googleupdate.exe /ua /installsource
- %windir%\system32\appidpolicyconverter.exe
- %windir%\system32\appidcertstorecheck.exe
- aitagent
[...]
```

5.6.4.3 Выполнение сценариев службы

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

В диалоговом окне появится подтверждение выполнения сценария.

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

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

5.6.5 Часто задаваемые вопросы

Требуются ли для запуска ESET SysInspector права администратора?

Хотя для запуска ESET SysInspector права администратора не требуются, некоторые из собираемых этим приложением данных доступны только для учетной записи администратора. Запуск под учетной записью обычного пользователя или пользователя с ограниченным доступом приведет к сбору меньшего объема данных о системе.

Создает ли ESET SysInspector файл журнала?

ESET SysInspector может создать файл журнала с конфигурацией системы. Для сохранения такого журнала в главном окне программы выберите **Файл** > **Сохранить журнал**. Журналы сохраняются в формате XML. По умолчанию файлы сохраняются в папке *%ПРОФИЛЬ_ПОЛЬЗОВАТЕЛЯ%\Мои документы* в файл с именем SysInpsector-%ИМЯ_КОМПЬЮТЕРА%-ГГММДД-ЧЧММ.XML. Перед сохранением файла журнала можно изменить его местоположение и название.

Как просмотреть файл журнала ESET SysInspector?

Для просмотра файла журнала, созданного в ESET SysInspector, запустите программу и в главном окне выберите **Файл** > **Открыть журнал**. Файлы журнала также можно перетаскивать в окно приложения ESET SysInspector. Если вы часто просматриваете файлы журнала ESET SysInspector, рекомендуется создать на рабочем столе ярлык для файла SYSINSPECTOR.EXE. После этого просматриваемые файлы можно просто перетаскивать на этот ярлык. Из соображений безопасности в ОС Windows Vista/7 может быть запрещено перетаскивать элементы между окнами, имеющими разные параметры безопасности.

Доступна ли спецификация для формата файлов журнала? Существует ли пакет SDK?

В настоящее время ни спецификация файла журнала, ни пакет SDK недоступны, поскольку программа все еще находится на стадии разработки. Возможно, мы выпустим их после выхода конечной версии программы в зависимости от отзывов пользователей и наличия интереса.

Как ESET SysInspector оценивает риск определенного объекта?

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

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

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

Зачем ESET SysInspector в ходе работы подключается к Интернету?

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

Что такое технология Anti-Stealth?

Технология Anti-Stealth обеспечивает эффективное обнаружение руткитов.

Если система подвергается атаке вредоносного кода, который ведет себя как руткит, пользователь может подвергаться риску потери или кражи данных. Без специального инструмента для борьбы с руткитами

обнаружить их практически невозможно.

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

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

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

Пример.

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

5.6.6 ESET SysInspector как часть ESET NOD32 Antivirus

Чтобы открыть раздел ESET SysInspector в ESET NOD32 Antivirus, выберите **Служебные программы** > **ESET SysInspector**. Система управления в окне ESET SysInspector похожа на ту, которая применяется в окнах журналов сканирования компьютера или запланированных задач. Для выполнения всех операций со снимками системы (создание, просмотр, сравнение, удаление и экспорт) достаточно одного или двух щелчков мыши.

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

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

Ниже приведено подробное описание доступных функций.

- **Сравнить**: сравнение двух существующих журналов. Эта функция удобна, если нужно найти различия между текущим и более старым журналом. Для использования этой функции нужно выбрать два снимка, которые следует сравнить.
- **Создать...**: создание новой записи. Перед созданием записи нужно ввести краткий комментарий к ней. Ход создания (формируемого в данный момент снимка) отображается в столбце **Состояние**. Все уже созданные снимки помечены надписью **Создано**.
- **Удалить/Удалить все**: удаление записей из списка.
- **Экспорт...**: сохранение выбранной записи в XML-файле с возможностью упаковки в архив.

5.7 Командная строка

Модуль защиты от вирусов ESET NOD32 Antivirus может быть запущен из командной строки вручную (с помощью команды «ecls») или в пакетном режиме (с помощью файла BAT-файла). Использование модуля сканирования командной строки ESET:

```
ecls [ПАРАМЕТРЫ..] ФАЙЛЫ..
```

Следующие параметры и аргументы могут использоваться при запуске сканера по требованию из командной строки.

Параметры

/base-dir=ПАПКА	загрузить модули из ПАПКИ
/quar-dir=ПАПКА	ПАПКА карантина
/exclude=МАСКА	исключить из сканирования файлы, соответствующие МАСКЕ
/subdir	сканировать вложенные папки (по умолчанию)
/no-subdir	не сканировать вложенные папки
/max-subdir-level=УРОВЕНЬ	максимальная степень вложенности папок для сканирования
/symlink	следовать по символическим ссылкам (по умолчанию)
/no-symlink	пропускать символические ссылки
/ads	сканировать ADS (по умолчанию)
/no-ads	не сканировать ADS
/log-file=ФАЙЛ	вывод журнала в ФАЙЛ
/log-rewrite	перезаписывать выходной файл (по умолчанию добавлять)
/log-console	вывод журнала в окно консоли (по умолчанию)
/no-log-console	не выводить журнал в консоль
/log-all	регистрировать также незараженные файлы
/no-log-all	не регистрировать незараженные файлы (по умолчанию)
/aind	показывать индикатор работы
/auto	сканирование и автоматическая очистка всех локальных дисков

Параметры модуля сканирования

/files	сканировать файлы (по умолчанию)
/no-files	не сканировать файлы
/memory	сканировать память
/boots	сканировать загрузочные секторы
/no-boots	не сканировать загрузочные секторы (по умолчанию)
/arch	сканировать архивы (по умолчанию)
/no-arch	не сканировать архивы
/max-obj-size=РАЗМЕР	сканировать файлы, только если их размер не превышает РАЗМЕР в мегабайтах (по умолчанию 0 = без ограничений)
/max-arch-level=УРОВЕНЬ	максимальная степень вложенности архивов для сканирования
/scan-timeout=ОГРАНИЧЕНИЕ	сканировать архивы не более указанного в ОГРАНИЧЕНИИ количества секунд
/max-arch-size=РАЗМЕР	сканировать файлы в архивах, только если их размер не превышает РАЗМЕР (по умолчанию 0 = без ограничений)
/max-sfx-size=РАЗМЕР	сканировать файлы в самораспаковывающихся архивах, только если их размер не превышает РАЗМЕР в мегабайтах (по умолчанию 0 = без ограничений)
/mail	сканировать файлы электронной почты (по умолчанию)
/no-mail	не сканировать файлы электронной почты
/mailbox	сканировать почтовые ящики (по умолчанию)
/no-mailbox	не сканировать почтовые ящики
/sfx	сканировать самораспаковывающиеся архивы (по умолчанию)
/no-sfx	не сканировать самораспаковывающиеся архивы
/rtp	сканировать упаковщики (по умолчанию)
/no-rtp	не сканировать упаковщики
/unsafe	сканировать на наличие потенциально опасных приложений

/no-unsafe	не сканировать на наличие потенциально опасных приложений (по умолчанию)
/unwanted	сканировать на наличие потенциально нежелательных приложений
/no-unwanted	не сканировать на наличие потенциально нежелательных приложений (по умолчанию)
/suspicious	сканировать на наличие подозрительных приложений (по умолчанию)
/no-suspicious	не сканировать на наличие подозрительных приложений
/pattern	использовать сигнатуры (по умолчанию)
/no-pattern	не использовать сигнатуры
/heur	включить эвристический анализ (по умолчанию)
/no-heur	отключить эвристический анализ
/adv-heur	включить расширенную эвристику (по умолчанию)
/no-adv-heur	отключить расширенную эвристику
/ext=РАСШИРЕНИЯ	сканировать только файлы с РАСШИРЕНИЯМИ, указанными через двоеточие
/ext-exclude=РАСШИРЕНИЯ	исключить из сканирования файлы с РАСШИРЕНИЯМИ, указанными через двоеточие
/clean-mode=РЕЖИМ	использовать РЕЖИМ очистки для зараженных объектов. Доступны указанные ниже варианты. • **нет**: автоматическая очистка не выполняется. • **стандартная** (по умолчанию): ecls.exe попытается автоматически очистить или удалить зараженные файлы. • **тщательная**: ecls.exe попытается автоматически очистить или удалить зараженные файлы без вмешательства пользователя (вам не будет предложено подтвердить удаление файлов). • **наиболее тщательная**: ecls.exe удалит все файлы без проведения очистки независимо от их типа. • **удаление**: ecls.exe удалит все файлы без проведения очистки, кроме важных, таких как системные файлы Windows.
/quarantine	копировать зараженные файлы, если они очищены, в карантин (дополнительно к действию, выполняемому при очистке)
/no-quarantine	не копировать зараженные файлы в карантин

Общие параметры

/help	показать справку и выйти
/version	показать сведения о версии и выйти
/preserve-time	сохранить последнюю отметку о времени доступа

Коды завершения

0	угроз не обнаружено
1	угроза обнаружена и очищена
10	некоторые файлы не удалось просканировать (могут быть угрозами)
50	угроза найдена
100	ошибка

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

6. Глоссарий

6.1 Типы заражений

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

6.1.1 Вирусы

Компьютерный вирус — это фрагмент злонамеренного кода, который добавляется в начало или конец файлов на компьютере. Название было выбрано из-за сходства с биологическими вирусами, так как они используют похожие методы для распространения с компьютера на компьютер. Часто термином «вирус» неверно обозначают любые типы угроз. Однако постепенно он выводится из употребления, и на смену ему приходит более точный термин «вредоносная программа».

Компьютерные вирусы атакуют в основном исполняемые файлы и документы. Компьютерный вирус функционирует следующим способом: после запуска зараженного файла вызывается и выполняется злонамеренный код. Это происходит до выполнения исходного приложения. Вирус способен заразить все файлы, на запись в которые у пользователя есть права.

Компьютерные вирусы могут быть разными по целям и степени опасности. Некоторые из вирусов особо опасны, так как могут целенаправленно удалять файлы с жесткого диска. С другой стороны, некоторые вирусы не причиняют никакого вреда. Они просто раздражают пользователя и демонстрируют возможности своих авторов.

Если ваш компьютер заражен вирусом, который не удается очистить, отправьте соответствующие файлы в исследовательскую лабораторию ESET для изучения. В ряде случаев зараженные файлы изменяются настолько, что их невозможно очистить. В таком случае их нужно заменять чистыми копиями.

6.1.2 Черви

Компьютерные черви — это содержащие злонамеренный код программы, которые атакуют главные компьютеры и распространяются через сеть. Основное различие между вирусами и червями заключается в том, что черви могут распространяться самостоятельно, так как они не зависят от зараженных файлов или загрузочных секторов. Черви распространяются, используя адресную книгу пользователя или уязвимости в системе безопасности сетевых приложений.

Поэтому черви намного более подвижны, чем компьютерные вирусы. Благодаря широкой популярности Интернета они могут распространяться по всему земному шару за считаные часы или даже минуты после запуска. Эта способность быстро самостоятельно реплицироваться делает черви более опасными, чем другие типы вредоносных программ.

Действующий в системе червь может доставить множество неудобств пользователю: он может удалять файлы, снижать производительность системы или даже отключать другие программы. По сути компьютерный червь может служить в качестве «транспортного средства» для других типов заражений.

Если компьютер заражен червем, рекомендуется удалить зараженные файлы, поскольку они с большой вероятностью содержат злонамеренный код.

6.1.3 Троянские программы

Исторически троянскими программами называли такой класс угроз, которые пытаются маскироваться под полезные программы, тем самым заставляя пользователя запускать их.

Так как эта категория весьма широка, ее часто разбивают на несколько подкатегорий.

- **Загрузчик**— вредоносная программа, способная загружать другие угрозы из Интернета.
- **Dropper**— вредоносная программа, которая предназначена для заражения компьютеров другими вредоносными программами.
- **Backdoor**— вредоносная программа, которая обменивается данными со злоумышленниками, позволяя им получить доступ к компьютеру и контроль над ним.
- **Клавиатурный шпион** — программа, которая регистрирует все, что пользователь набирает на клавиатуре, и отправляет эту информацию злоумышленникам.
- **Программа дозвона** — вредоносная программа, которая предназначена для подключения к номерам с высокими тарифными планами, а не к поставщику интернет-услуг пользователя. При этом пользователь практически не может заметить, что создано новое подключение. Программы дозвона могут нанести вред только пользователям модемов. К счастью, модемы уже не распространены столь широко, как раньше.

Если на компьютере обнаружен файл, классифицированный как троянская программа, рекомендуется удалить его, так как он с большой вероятностью содержит злонамеренный код.

6.1.4 Руткиты

Руткитом называется вредоносная программа, которая предоставляет злоумышленникам полный доступ к компьютеру, не проявляя при этом своего присутствия в системе. После получения доступа к системе (обычно путем использования ее уязвимостей) руткиты используют функции операционной системы, чтобы избежать обнаружения программным обеспечением защиты от вирусов: используются механизмы маскировки процессов, файлов и данных системного реестра. По этой причине их активность невозможно обнаружить стандартными методами проверки.

Существует два уровня обнаружения, направленных на борьбу с руткитами.

1. Обнаружение при попытке доступа к системе. Их еще нет в системе, то есть они не активны. Многие системы защиты от вирусов способны устранить руткиты на этом уровне (при условии, что они действительно обнаруживают такие файлы как зараженные).
2. Обнаружение при попытке скрыться во время обычной проверки. Пользователям ESET NOD32 Antivirus доступны преимущества технологии Anti-Stealth, которая также позволяет обнаруживать и устранять активные руткиты.

6.1.5 Рекламные программы

Под рекламной программой понимается программное обеспечение, существующее за счет рекламы. Программы, демонстрирующие пользователю рекламные материалы, относятся к этой категории. Рекламные приложения часто автоматически открывают всплывающие окна с рекламой в веб-браузере или изменяют домашнюю страницу. Рекламные программы часто распространяются в комплекте с бесплатными программами. Это позволяет их создателям покрывать расходы на разработку полезных (как правило) программ.

Сами по себе рекламные программы не опасны, но они раздражают пользователей. Опасность заключается в том, что в рекламных программах могут быть реализованы дополнительные функции слежения, подобно шпионским программам.

Если пользователь решает использовать бесплатный программный продукт, ему стоить уделить особое внимание установке программы. Чаще всего программа установки предупреждает об установке дополнительной рекламной программы. Зачастую пользователь имеет возможность отказаться от его установки и установить необходимую программу без рекламной.

Некоторые программы нельзя установить без рекламных модулей либо их функциональность будет ограничена. Это приводит к тому, что рекламная программа часто получает доступ к системе на «законных»

основаниях, так как пользователь дал согласие на ее установку. В этом случае лучше перестраховаться. В случае обнаружения на компьютере файла, классифицированного как рекламная программа, рекомендуется удалить его, так как он с большой вероятностью содержит злонамеренный код.

6.1.6 Шпионские программы

К этой категории относятся все приложения, которые отправляют личную информацию без ведома и согласия владельца. Шпионские программы используют функции слежения для отправки различной статистической информации, такой как список посещенных веб-сайтов, адреса электронной почты из адресных книг пользователя или набираемый на клавиатуре текст.

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

Примерами хорошо известного бесплатного программного обеспечения, вместе с которым поставляется шпионское, могут служить клиенты пиринговых (P2P) сетей. Программы Spyfalcon и Spy Sheriff (и многие другие) относятся к особой подкатегории шпионских программ. Утверждается, что они предназначены для защиты от шпионских программ, но на самом деле они сами являются таковыми.

В случае обнаружения на компьютере файла, классифицированного как шпионская программа, рекомендуется удалить его, так как с высокой вероятностью он содержит злонамеренный код.

6.1.7 Упаковщики

Упаковщик — это самораспаковывающийся исполняемый файл, в котором содержится несколько видов вредоносных программ.

Наиболее распространенными упаковщиками являются UPX, PE_Compact, PKLite и ASPack. Одни и те же вредоносные программы могут быть обнаружены разными способами, если их сжатие выполнено при помощи разных упаковщиков. Кроме того, упаковщики обладают свойством, благодаря которому их сигнатуры со временем изменяются, что усложняет задачу обнаружения и удаления вредоносных программ.

6.1.8 Потенциально опасные приложения

Существует множество нормальных программ, предназначенных для упрощения администрирования подключенных к сети компьютеров. Однако злоумышленники могут использовать их для причинения вреда. Программное обеспечение ESET NOD32 Antivirus позволяет обнаруживать такие угрозы.

В качестве **потенциально опасных приложений** выступает нормальное коммерческое программное обеспечение. В эту категорию входят такие программы, как средства удаленного доступа, приложения для взлома паролей и клавиатурные шпионы (программы, записывающие нажатия клавиш на клавиатуре).

Если потенциально опасное приложение обнаружено и работает на компьютере (но пользователь не устанавливал его), следует обратиться к администратору сети или удалить приложение.

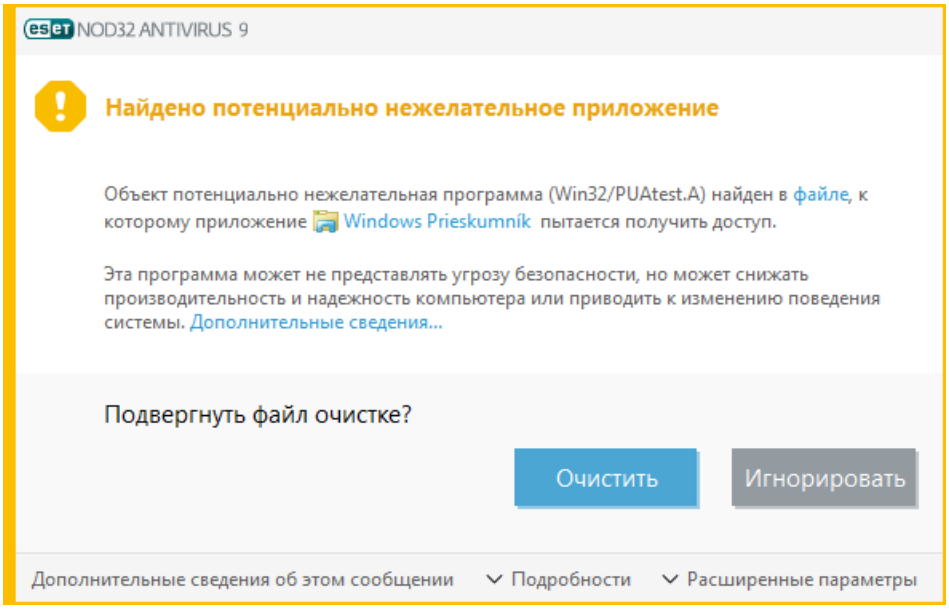
6.1.9 Потенциально нежелательные приложения

Потенциально нежелательное приложение — это программа, которая содержит рекламу, устанавливает панели инструментов или выполняет другие неясные функции. В некоторых ситуациях может показаться, что преимущества такого потенциально нежелательного приложения перевешивают риски. Поэтому компания ESET помещает эти приложения в категорию незначительного риска, в отличие от других вредоносных программ, например троянских программ или червей.

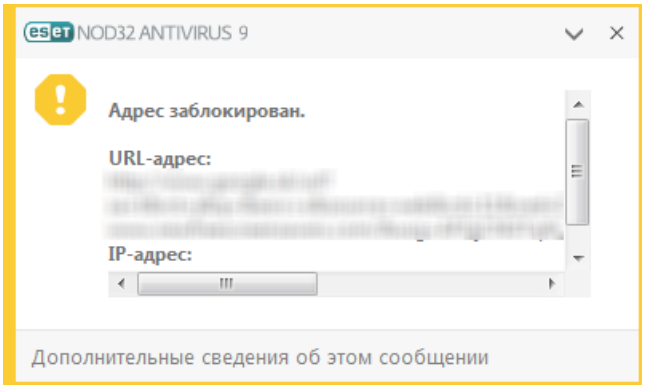
Предупреждение — обнаружена потенциальная угроза

Когда обнаруживается потенциально нежелательное приложение, вы можете самостоятельно решить, какое действие нужно выполнить.

1. **Очистить/отключить**: действие прекращается, и потенциальная угроза не попадает в систему.
2. **Пропустить**: эта функция позволяет потенциальной угрозе проникнуть на компьютер.
3. Чтобы разрешить приложению и впредь работать на компьютере без прерываний, щелкните элемент **Расширенные параметры** и установите флажок **Исключить из обнаружения**.

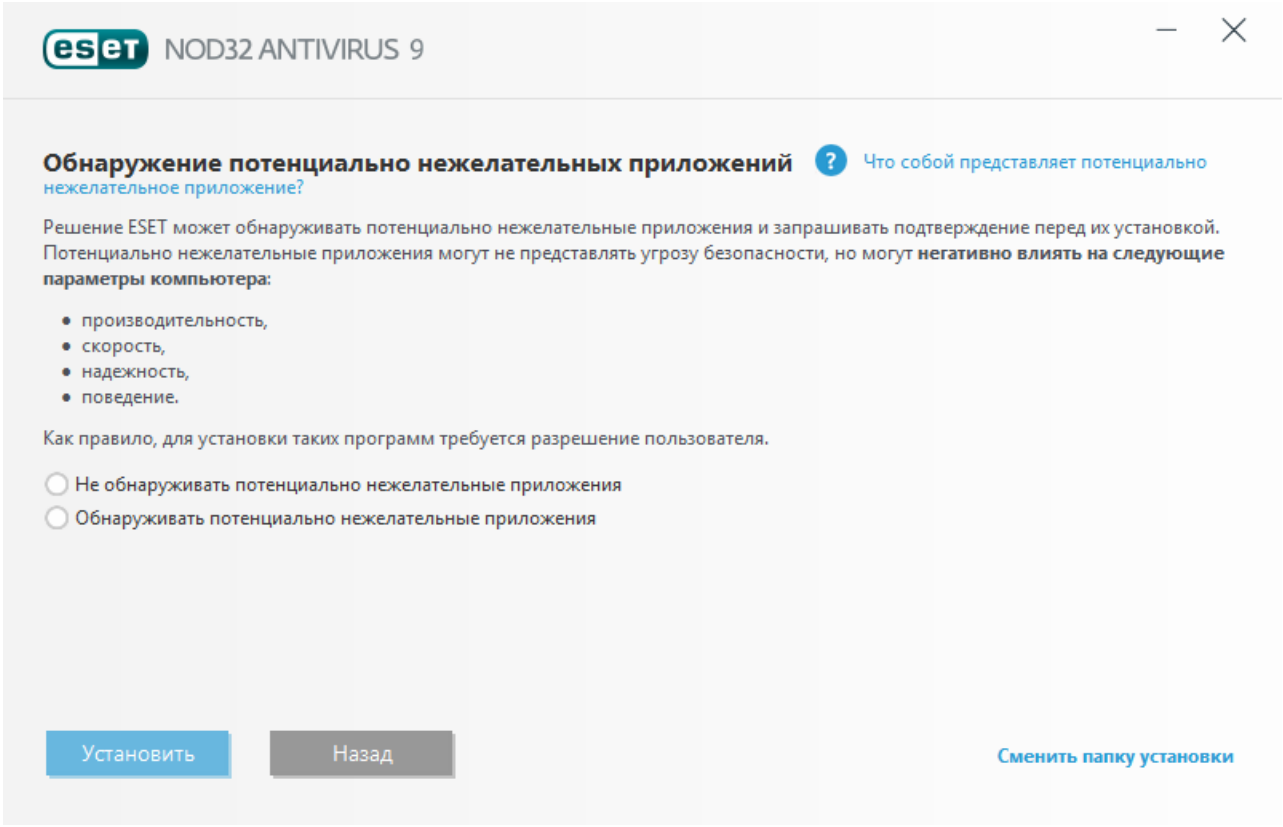


Если обнаружено потенциально нежелательное приложение и его невозможно очистить, в правом нижнем углу экрана отобразится окно уведомлений **Адрес заблокирован**. Для получения дополнительных сведений об этом событии перейдите из главного меню в раздел **Служебные программы** > **Файлы журналов** > **Отфильтрованные веб-сайты**.



Потенциально нежелательные приложения — параметры

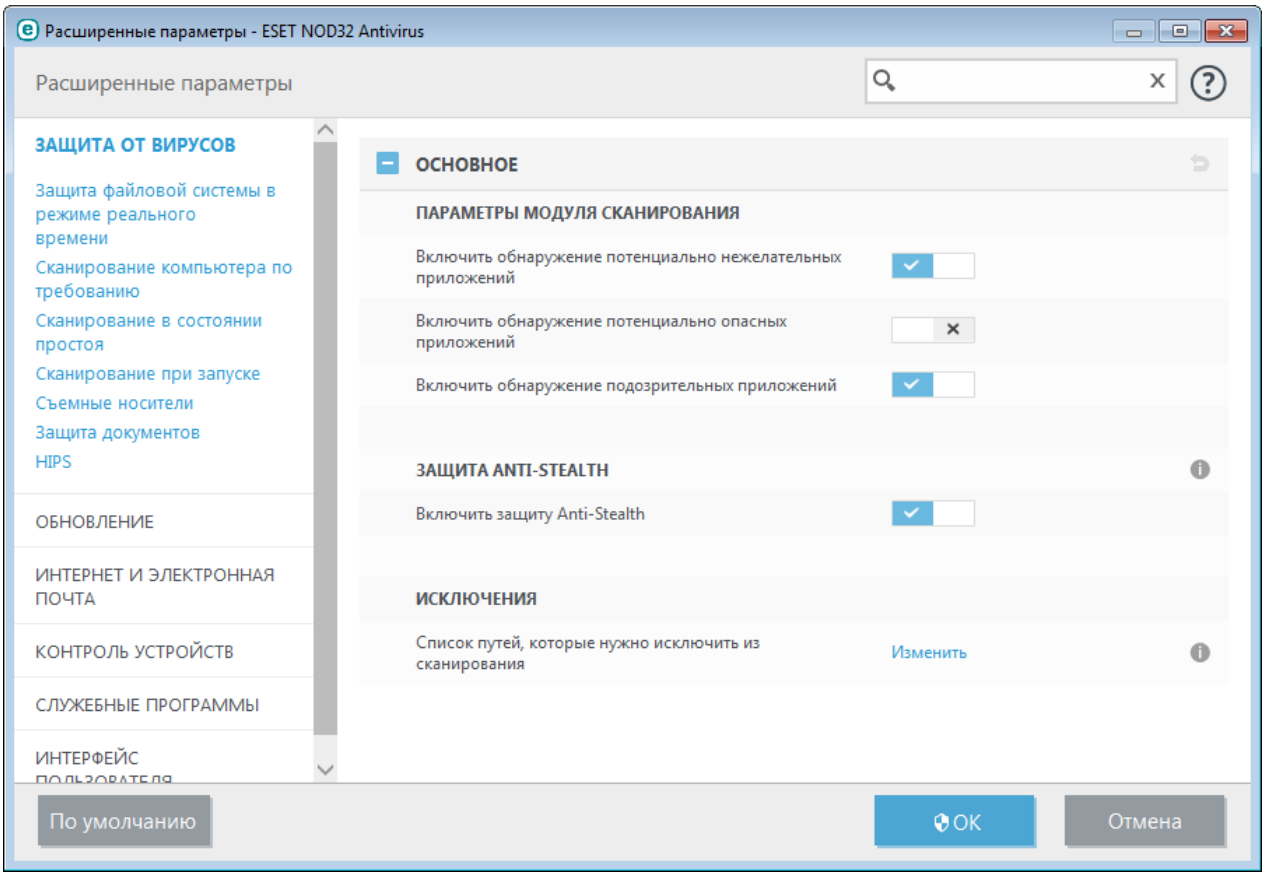
При установке программы ESET можно включить обнаружение потенциально нежелательных приложений (см. изображение ниже).



Потенциально нежелательные приложения могут устанавливать рекламные программы и панели инструментов или содержать рекламу и другие нежелательные и небезопасные программные компоненты.

Эти параметры можно в любое время изменить в разделе параметров программы. Чтобы включить или отключить обнаружение потенциально нежелательных, небезопасных или подозрительных приложений, следуйте приведенным ниже инструкциям.

1. Откройте программу ESET. Как открыть программу ESET на моем компьютере?
2. Нажмите клавишу **F5**, чтобы перейти к разделу **Дополнительные настройки**.
3. Щелкните элемент **Антивирус** и на свое усмотрение включите или отключите параметры **Включить обнаружение потенциально нежелательных приложений**, **Включить обнаружение потенциально опасных приложений** и **Включить обнаружение подозрительных приложений**. Чтобы сохранить настройки, нажмите кнопку **ОК**.



Потенциально нежелательные приложения — оболочки

Оболочка — специальное приложение, используемое на некоторых файлообменных ресурсах. Это стороннее средство, устанавливающее программу, которую нужно загрузить, в комплекте с другим программным обеспечением, например панелью инструментов или рекламной программой, которые могут изменить домашнюю страницу браузера или параметры поиска. При этом файлообменные ресурсы часто не уведомляют поставщиков программного обеспечения или получателей загруженных файлов о внесенных изменениях, а отказаться от этих изменений непросто. Именно поэтому компания ESET считает оболочки потенциально нежелательными приложениями и дает пользователям возможность отказаться от их загрузки.

Обновленную версию данной страницы справки см. в этой статье базы знаний ESET.

6.2 Технологии ESET

6.2.1 Блокировщик эксплойтов

Блокировщик эксплойтов предназначен для защиты приложений, которые обычно уязвимы для эксплойтов, например браузеров, программ для чтения PDF-файлов, почтовых клиентов и компонентов MS Office. Он осуществляет мониторинг работы процессов для выявления подозрительных действий, которые могли бы означать использование эксплойта.

Когда блокировщик эксплойтов обнаруживает подозрительный процесс, он может сразу же остановить его работу и записать данные об угрозе, которые затем отправляются в облачную систему ThreatSense. Эти данные затем обрабатываются в исследовательской лаборатории ESET и используются для улучшения защиты всех пользователей от неизвестных угроз и атак «нулевого дня» (новые вредоносные программы, для которых еще нет предварительно настроенных средств защиты).

6.2.2 Расширенный модуль сканирования памяти

Расширенный модуль сканирования памяти работает в сочетании с блокировщиком эксплойтов для усиления защиты от вредоносных программ, которые могут избегать обнаружения обычными продуктами для защиты от вредоносных программ за счет использования умышленного запутывания и/или шифрования. В случаях, когда угроза может быть не обнаружена с помощью обычной эмуляции или эвристики, расширенный модуль сканирования памяти может определять подозрительные действия и сканировать угрозы, когда они появляются в системной памяти. Это решение эффективно даже против вредоносных программ с высокой степенью умышленного запутывания.

В отличие от блокировщика эксплойтов, расширенный модуль сканирования памяти — это метод, применяемый после выполнения, поэтому существует риск того, что некоторые вредоносные действия могли быть выполнены до обнаружения угрозы. Однако если применение других методов обнаружения не дало результатов, такое решение обеспечивает дополнительный уровень безопасности.

6.2.3 ThreatSense

Сеть ESET LiveGrid®, основанная на передовой системе раннего обнаружения ThreatSense.Net®, использует данные, предоставленные пользователями ESET со всего мира, и отправляет их в исследовательскую лабораторию ESET. Сеть ESET LiveGrid® позволяет получать подозрительные образцы и метаданные из реальных условий, поэтому мы можем незамедлительно реагировать на потребности пользователей и обеспечить готовность ESET к обезвреживанию новейших угроз. Исследователи вредоносных программ ESET используют эту информацию для получения точного представления о природе и масштабах глобальных угроз, что позволяет нам направлять усилия на решение правильных задач. Данные системы ESET LiveGrid® играют важную роль при определении приоритетов в наших автоматизированных системах.

Кроме того, применяется система репутации, помогающая улучшить общую эффективность наших решений по борьбе с вредоносными программами. Когда исполняемый файл или архив проверяется на компьютере пользователя, его хэш-тег сначала проверяется по базе элементов, внесенных в «белые» и «черные» списки. Если он находится в «белом» списке, проверяемый файл считается чистым и помечается для исключения из будущих сканирований. Если он находится в «черном» списке, предпринимаются соответствующие действия, исходя из природы угрозы. Если соответствие не найдено, файл тщательно сканируется. На основании результатов сканирования происходит категоризация файлов как угроз или чистых файлов. Такой подход имеет существенное положительное влияние на производительность сканирования.

Система репутации обеспечивает эффективное обнаружение образцов вредоносных программ еще до доставки их сигнатур в обновленную базу данных вирусов на компьютере пользователя (что происходит несколько раз в день).

6.2.4 Блокировщик эксплойтов Java

Блокировщик эксплойтов Java — это расширение существующей защиты блокировщика эксплойтов. Он осуществляет мониторинг Java на предмет поведения, подобного поведению эксплойтов. Заблокированные образцы можно передавать аналитикам вредоносных программ, чтобы они могли создавать сигнатуры для блокировки таких программ на разных уровнях (блокировка URL-адресов, загрузка файлов и т. п.).

6.3 Электронная почта

Электронная почта является современным средством общения, которое применяется во многих областях. Она отличается гибкостью, высокой скоростью и отсутствием посредников и сыграла ключевую роль в распространении Интернета в начале 90-х годов прошлого века.

К сожалению, вследствие высокого уровня анонимности электронная почта и Интернет оставляют пространство для незаконных действий, таких как рассылка спама. К спаму относятся нежелательные рекламные объявления, мистификации и сообщения, предназначенные для распространения вредоносных программ. Доставляемые пользователю неудобства и опасность увеличиваются из-за того, что стоимость рассылки минимальна, а в распоряжении авторов спама есть множество средств для получения новых адресов электронной почты. Кроме того, количество и разнообразие спама сильно затрудняют контроль над ним. Чем дольше используется адрес электронной почты, тем выше вероятность того, что он попадет в базы данных, используемые для рассылки спама. Вот некоторые советы, помогающие избежать этого.

- По возможности не размещайте свой адрес электронной почты в Интернете.
- Давайте свой адрес только тем, кому полностью доверяете.
- Если возможно, не используйте распространенные слова в качестве псевдонимов (чем сложнее псевдоним, тем труднее отследить адрес).
- Не отвечайте на полученный спам.
- Будьте осторожны при заполнении форм на веб-сайтах (особенно если они содержат пункты типа «Да, я хочу получать информацию»).
- Используйте «специализированные» адреса электронной почты (например, заведите один адрес для работы, другой для общения с друзьями и т. д.).
- Время от времени меняйте адрес электронной почты.
- Используйте какое-либо решение для защиты от спама.

6.3.1 Рекламные объявления

Реклама в Интернете является одним из наиболее бурно развивающихся видов рекламы. Ее преимуществами являются минимальные затраты и высокая вероятность непосредственного общения с потребителем. Кроме того, сообщения доставляются практически мгновенно. Многие компании используют электронную почту в качестве маркетингового инструмента для эффективного общения с существующими и потенциальными клиентами.

Этот вид рекламы является нормальным, так как потребители могут быть заинтересованы в получении коммерческой информации о некоторых товарах. Однако многие компании занимаются массовыми рассылками нежелательных коммерческих сообщений. В таких случаях реклама по электронной почте выходит за границы допустимого, и эти сообщения классифицируются как спам.

Количество нежелательных сообщений уже стало проблемой, и при этом никаких признаков его сокращения не наблюдается. Авторы нежелательных сообщений часто пытаются выдать спам за нормальные сообщения.

6.3.2 Мистификации

Мистификацией называется ложная информация, распространяющаяся через Интернет. Обычно мистификации рассылаются по электронной почте или с помощью таких средств общения, как ICQ и Skype. Собственно сообщение часто представляет собой шутку или городскую легенду.

Связанные с компьютерными вирусами мистификации направлены на то, чтобы вызвать в получателях страх, неуверенность и мнительность, побуждая их верить в то, что «не поддающийся обнаружению вирус» удаляет их файлы, крадет пароли или выполняет какие-либо другие крайне нежелательные действия с компьютерами.

Некоторые мистификации работают, предлагая получателям переслать сообщение своим знакомым, за счет чего увеличивается масштаб мистификации. Существуют мистификации, которые передаются через мобильные телефоны, мистификации, представляющие собой просьбы о помощи, предложения получить деньги из-за границы, и прочие. Часто бывает невозможно понять мотивацию создателя мистификации.

Если сообщение содержит просьбу переслать его всем знакомым, это сообщение с большой вероятностью

является мистификацией. Существует большое количество веб-сайтов, которые могут проверить, является ли сообщение нормальным. Прежде чем пересылать сообщение, которое кажется вам мистификацией, попробуйте найти в Интернете информацию о нем.

6.3.3 Фишинг

Термин «фишинг» обозначает преступную деятельность, в рамках которой используются методы социальной инженерии (манипулирование пользователем, направленное на получение конфиденциальной информации). Целью фишинга является получение доступа к таким конфиденциальным данным, как номера банковских счетов, PIN-коды и т. п.

Попытка получения информации обычно представляет собой отправку сообщения якобы от доверенного лица или компании (такой как финансового учреждения или страховой компании). Сообщение может казаться благонадежным и содержать изображения и текст, которые могли изначально быть получены от источника, якобы являющегося отправителем данного сообщения. Под разными предлогами (проверка данных, финансовые операции) предлагается предоставить какую-либо личную информацию, такую как номера банковских счетов, имена пользователя, пароли и т. д. Если такие данные предоставляются, они легко могут быть украдены и использованы в преступных целях.

Банки, страховые компании и другие легитимные организации никогда не запрашивают имена пользователей и пароли в незапрошенных сообщениях электронной почты.

6.3.4 Распознавание мошеннических сообщений

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

- Адрес отправителя отсутствует в адресной книге получателя.
- Предлагается получить большую сумму денег, но сначала нужно оплатить небольшую сумму.
- Под разными предлогами (проверка данных, финансовые операции) предлагается предоставить какие-либо личные данные, такие как номера банковских счетов, имя пользователя, пароль и т. д.
- Сообщение написано на иностранном языке.
- Предлагается покупка продукции, в которой получатель не заинтересован. Однако если получателя заинтересовало предложение, следует проверить, является ли отправитель надежным поставщиком (например, проконсультироваться с представителем производителя продукции).
- Некоторые из слов намеренно написаны с ошибками, чтобы обмануть фильтр спама. Например, «веагро» вместо «виагра» и т. п.

7. Часто задаваемые вопросы

Эта глава содержит ответы на некоторые из наиболее часто задаваемых вопросов и решения проблем пользователей. Нажмите ссылку, описывающую вашу проблему.

Выполнение обновления ESET NOD32 Antivirus
Удаление вируса с компьютера
Создание задачи в планировщике
Планирование задачи сканирования (каждые 24 часа)

Если ваша проблема не включена в список на страницах справки выше, попробуйте найти ее на страницах справки ESET NOD32 Antivirus.

Если решение проблемы не удалось найти с помощью поиска в содержимом справочной системы, перейдите в регулярно обновляемую базе знаний ESET в Интернете. Ссылки на самые популярные статьи базы знаний, которые помогут вам решить распространенные проблемы, перечислены ниже.

Во время установки программы ESET появилось сообщение об ошибке. Что это означает?
Как ввести имя пользователя и пароль в программу ESET Smart Security или ESET NOD32 Antivirus?
Во время установки программы ESET появилось сообщение, что установка преждевременно завершена.
Что делать после обновления лицензии? (пользователи домашней версии)
Что делать, если мой адрес электронной почты изменится?
Запуск Windows в безопасном режиме или в безопасном режиме с поддержкой сети

При необходимости направьте свои вопросы в нашу онлайн-службу технической поддержки. Контактная форма находится на вкладке **Справка и поддержка** программы ESET NOD32 Antivirus.

7.1 Выполнение обновления ESET NOD32 Antivirus

Обновлять ESET NOD32 Antivirus можно вручную или автоматически. Чтобы запустить обновление, выберите команду **Обновить сейчас** в разделе **Обновление**.

При установке программы с параметрами по умолчанию создается задача автоматического обновления. Она запускается каждый час. Чтобы изменить интервал, последовательно выберите **Сервис** > **Планировщик** (дополнительную информацию о планировщике см. здесь).

7.2 Удаление вируса с компьютера

Если компьютер начал работать медленнее, часто зависать и проявлять другие признаки заражения вредоносной программой, рекомендуется выполнить следующие действия.

1. В главном окне программы щелкните **Сканирование ПК**.
2. Щелкните элемент **Сканировать компьютер**, чтобы запустить сканирование компьютера.
3. После завершения сканирования просмотрите журнал на предмет количества проверенных, зараженных и очищенных файлов.
4. Если необходимо проверить только определенную часть диска, щелкните **Выборочное сканирование** и укажите объекты, которые следует сканировать на наличие вирусов.

Дополнительные сведения можно найти в статье нашей регулярно обновляемой базы знаний ESET.

7.3 Создание задачи в планировщике

Для создания задачи выберите **Служебные программы** > **Планировщик**, а затем нажмите кнопку **Добавить** или щелкните правой кнопкой мыши и выберите команду **Добавить...** в контекстном меню. Доступно пять типов задач.

- **Запуск внешнего приложения** - планирование выполнения внешнего приложения.
- **Обслуживание журнала** - в файлах журнала также содержатся остатки удаленных записей. Эта задача регулярно оптимизирует записи в файлах журнала для эффективной работы.
- **Проверка файлов, исполняемых при запуске системы** - проверка файлов, исполнение которых разрешено при запуске или входе пользователя в систему.
- **Создать снимок состояния компьютера** - создание снимка состояния компьютера в ESET SysInspector, для которого собираются подробные сведения о компонентах системы (например, драйверах, приложениях) и оценивается уровень риска для каждого их них.
- **Сканирование ПК по требованию** - выполнение сканирования файлов и папок на компьютере.
- **Первое сканирование** - по умолчанию через 20 минут после установки или перезагрузки выполняется сканирование компьютера как задание с низким приоритетом.
- **Обновление** — планирование задачи обновления, в рамках которой обновляется база данных сигнатур вирусов и программные модули.

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

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

- **В следующее запланированное время**
- **Как можно скорее**
- **Незамедлительно, если с момента последнего запуска прошло больше времени, чем указано** (интервал можно указать в поле **Время с момента последнего запуска (ч)**).

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

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

7.4 Планирование еженедельного сканирования компьютера

Чтобы запланировать регулярную задачу, откройте главное окно программы и выберите **Служебные программы** > **Планировщик**. Ниже приведено краткое описание процедуры планирования задачи, предусматривающей сканирование локальных дисков каждые 24 часа. Подробные инструкции см. в статье нашей базы знаний.

Для того чтобы запланировать задачу сканирования, выполните следующие действия.

1. В главном окне планировщика нажмите **Добавить**.
2. В раскрывающемся меню выберите **Сканирование ПК по требованию**.
3. Введите имя задачи и выберите частоту выполнения задачи **Еженедельно**.

4. Задайте день и время выполнения задачи.
5. Выберите установку **Выполнить задачу как можно скорее**, чтобы выполнить задачу позже в случае, если запланированное выполнение задачи не запустится по какой-либо причине (например, если компьютер будет выключен).
6. Просмотрите сводную информацию о запланированной задаче и нажмите **Готово**.
7. В раскрывающемся меню **Объекты** выберите пункт **Жесткие диски**.
8. Нажмите **Готово** для применения задачи.